PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

EXPOSIÇÃO E VULNERABILIDADES DE ATIVOS NO BRASIL

Victor Alcanfor Concentino

GOIÂNIA
2026

Victor Alcanfor Concentino

EXPOSIÇÃO E VULNERABILIDADES DE ATIVOS NO BRASIL

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.

Orientador(a):
Prof. Me. Fernando Gonçalves Abadia

Banca examinadora:
Prof. Dr. Cristian Patricio Novoa Bustos
Prof. Me. Anibal Santos Jukemura

GOIÂNIA
2026

VICTOR ALCANFOR CONCENTINO

EXPOSIÇÃO E VULNERABILIDADES DE ATIVOS NO BRASIL

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciencia da Computação, em _____/_____/_____.

_____

Orientador(a): Prof. Me. Fernando Gonçalves Abadia

_____

Prof. Dr. Cristian Patricio Novoa Bustos

_____

Prof. Me. Anibal Santos Jukemura

GOIÂNIA

2026

“Se você pensa que a tecnologia pode resolver os seus problemas de segurança, então você não entende os problemas e você não entente a tecnologia”

Bruce Schneier

RESUMO

A rápida digitalização de serviços no Brasil, que se intensificou após 2020, aumentou consideravelmente a superfície de ataque digital no Brasil. Muitos serviços, como servidores web, bancos de dados e protocolos de rede, ficaram expostos à internet, frequentemente com configurações inadequadas ou versões vulneráveis, o que facilita sua exploração, especialmente em sistemas legados que não recebem manutenção. Neste contexto, este estudo avalia o grau de exposição de serviços publicamente acessíveis no país e identifica possíveis vulnerabilidades associadas. Para isso, se utiliza uma pesquisa descritiva e quantitativa, coletando e analisando dados obtidos em plataformas como Shodan e Censys. Esses dados permitem identificar serviços expostos, versões de software e indícios de configurações inseguras. Como resultado, procura-se identificar padrões de exposição, quantificar possíveis vulnerabilidades e debater falhas frequentes, auxiliando na compreensão do contexto nacional e enfatizando a relevância de práticas adequadas de segurança da informação.

Palavras-chave: Superfície de ataque; Serviços expostos; Vulnerabilidades conhecidas; Inteligência de segurança; Cibersegurança; Brasil.

ABSTRACT

The rapid digitization of services in Brazil, which intensified after 2020, has significantly expanded the country's digital attack surface. Many services, such as web servers, databases, and network protocols, have been exposed to the internet, often with inadequate configurations or vulnerable versions, making them easier to exploit—especially in legacy systems that are no longer maintained. In this context, this study assesses the degree of exposure of publicly accessible services in the country and identifies potential associated vulnerabilities. To this end, it employs a descriptive and quantitative research approach, collecting and analyzing data obtained from platforms such as Shodan and Censys. This data enables the identification of exposed services, software versions, and indications of insecure configurations. As a result, the study seeks to identify patterns of exposure, quantify potential vulnerabilities, and discuss common flaws, thereby aiding in the understanding of the national context and emphasizing the importance of proper information security practices.

Keywords: Attack surface; Exposed services; Known vulnerabilities; Security intelligence; Cybersecurity; Brazil.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

OWASP	Open Worldwide Application Security Project
NIST	National Institute of Standards and Technology
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
NVD	National Vulnerability Database
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
P2P	Peer-to-peer
DDoS	Distributed Denial of Service
DoS	Denial of Service
PoLP	Principle of Least Privilege
FIRST	Forum of Incident Response and Security Teams
GAO	United States Government Accountability Office
VPN	Virtual Private Network
ZTNA	Zero Trust Network Access
OSINT	Open Source Inteligence
IDOR	Insecure Direct Object Reference
CORS	Cross-Origin Resource Sharing
ECB	Eletronic Code Book
HSMs	Hardware Security Modules
SEC	United States Securities and Exchange Commission
sFTP	Secure File Transfer Protocol
SSH	Secure Shell
DPC	Data Protection Commission
MFA	Multi-factor authentication
PoC	Proof of Concept
SCAP	Security Content Automation Protocol
SMB	Server Message Block
FTP	File Transfer Protocol
IoT	Internet of Things
ACL	Access Control List

SUMÁRIO

1. INTRODUÇÃO

O crescimento acelerado da digitalização de serviços públicos e privados ampliou significativamente a presença de sistemas conectados à internet. No Brasil, essa expansão ocorreu de forma particularmente intensa nos últimos anos, impulsionada pela adoção de soluções digitais em setores governamentais, empresariais e domésticos. Como consequência, servidores web, bancos de dados, dispositivos IoT e diversos serviços passaram a estar amplamente acessíveis pela rede ou conectados de forma geral, aumentando a superfície de ataque disponível para possíveis ameaças.

A exposição direta desses ativos torna-se um problema relevante de segurança quando sistemas operam com configurações inadequadas ou utilizam versões de software com vulnerabilidades conhecidas. Na maioria dos casos, falhas de manutenção, ou más práticas de configuração são as maiores causas de sistemas vulneráveis, criando oportunidades para exploração de vulnerabilidades por agentes mal intencionados.

Diante disto, torna-se importante compreender o nível de exposição dos serviços e identificar possíveis sinais de vulnerabilidades associadas a esses sistemas. Este trabalho busca analisar a exposição de serviços acessíveis no Brasil e discutir os riscos relacionados à presença de configurações inseguras e softwares potencialmente vulneráveis, contribuindo para a compreensão do panorama de segurança de sistemas expostos no país.

1.1. Objetivo Geral

O objetivo deste trabalho é demonstrar que uma percentagem consideravel dos serviços que utilizam a internet no Brasil está exposta e, em muitos casos, utiliza softwares que apresentam vulnerabilidades conhecidas e que poderiam ser corrigidas por meio de atualizações ou ajustes de configuração. Após demonstrar a situação atual da infraestrutura, será destacada a importância da manutenção dos sistemas e adoção de práticas adequadas de configuração e gerenciamento da segurança.

Para a realização do estudo, a analise será conduzida de maneira ética, utilizando ferramentas amplamente conhecidas e conceituadas de monitoramento passivo e não intrusivo, como Shodan e Censys. Tais plataformas coletam e

disponibilizam informações públicas sobre serviços acessíveis na internet, com ciclos de atualização relativamente curtos, geralmente de até uma semana. Dessa forma, os dados analisados tensem a serem relativamente recentes e refletem com boa precisão o estado dos serviços observados, permitindo identificar possíveis vulnerabilidades presentes nos sistemas expostos.

1.2. Objetivos Específicos

- Levantar os principais tipos de serviços e sistemas acessíveis pela internet estão localizados no Brasil, utilizando plataformas de observação passiva como Shodan e Censys, que permitem visualizar informações públicas sobre serviços expostos.
- Reunir informações técnicas sobre os serviços identificados, como portas abertas, protocolos em uso, banners de identificação e versões de software quando essas informações estiverem disponíveis.
- Organizar os serviços encontrados de acordo com sua natureza, separando-os em categorias como servidores web, bancos de dados, serviços de infraestrutura de rede, dispositivos IoT e outros sistemas semelhantes.
- Verificar se as versões de software identificadas apresentam indícios de vulnerabilidades conhecidas, consultando bases públicas de registro de falhas de segurança.
- Examinar possíveis padrões de exposição e identificar configurações que possam indicar práticas inadequadas de segurança ou falta de manutenção dos sistemas analisados.
- Apresentar uma análise quantitativa da exposição desses serviços no Brasil, discutindo os riscos que essa situação pode representar para a segurança da informação e apontando possíveis medidas que possam contribuir para reduzir esses problemas.

1.3. Justificativa

Devido à crescente digitalização de serviços e ao crescimento do mercado digital, a importância de se reduzir a superfície de ataque o máximo possível é imperativa, caso contrário, o risco de ataques que põe em risco os dados do sistema, ou até mesmo o seu funcionamento se tornam uma ameaça palpável.

Segundo a OWASP (Open Worldwide Application Security Project) uma organização não governamental dedicada a melhorar a segurança de sistemas digitais, várias das 10 maiores vulnerabilidades (OWASP Top 10, 2025) estão relacionadas com o problema abordado por este trabalho, como por exemplo:

- Vulnerabilidade #1 – “Broken Access Control” (Controle de Acesso Quebrado): Ocorre quando não há ou quando não são aplicadas corretamente as políticas de controle de acesso acesso dos usuários, impedindo que possam agir fora das suas permissões, a falta de tais medidas geralmente resulta no acesso não autorizado de informações, na modificação ou destruição de dados, ou na execução de um comando que está acima das permissões do usuário. Não pode ser verificada com muita precisão de forma passiva, mas algumas consequências do problema podem ser observadas quando por exemplo, painéis de gerenciamento e outras ferramentas que deveriam ser exclusivamente de uso interno estão expostas, uma confirmação real da vulnerabilidade requere interação direta (tentativa de acesso, invasiva) com os sistemas e não seria ética, a analise somente irá utilizar dados obtidos de forma passiva que podem demonstrar tais problemas.

- Vulnerabilidade #2 – “Security Misconfiguration” (Configuração Insegura): Ocorre quando a configuração de um sistema, aplicação ou serviço cloud foi configurado de forma errada da perspectiva de segurança, criando vulnerabilidades. É facilmente quantificável com as ferramentas utilizadas, exemplos incluem painéis de administração expostos, listagem de diretórios, HTTP TRACE habilitado, CORS permissivo, serviços de gerenciamento sem autenticação e outros.

- Vulnerabilidade #3 – “Software Supply Chain Failures” (Falhas na Cadeia de Suprimentos de Software): São falhas que geralmente ocorrem no processo de

desenvolvimento, distribuição ou atualização de software, na maioria das vezes ocorrendo por vulnerabilidades ou alterações maliciosas no código de terceiros, em ferramentas ou em outras dependências das quais o sistema utiliza. É identificável com tecnicas de monitoramento passivo devido a versões de software expostos, exemplos: versões de PHP, Apache/Nginx, OpenSSL (casos como Heartbleed), WordPress/Plugins, Drupal e outras dependências ou artefatos de build e distribuição que indicam componentes vulneráveis ou desatualizados.

- Vulnerabilidade #4 – “Cryptographic Failures” (Falhas Criptográficas): São riscos que se manifestam pela ausência de criptografia, criptografia insuficientemente robusta, vazamento de chaves criptográficas e erros relacionados. Pode ser observado passivamente por indicadores como suítes fracas, certificados expirados ou autoassinados, uso de HTTP sem TLS em áreas de login ou administração, e reutilização de chaves.

- Vulnerabilidade #7 – “Authentication Failures” (Falhas de Autenticação): Ocorre quando mecanismos de autenticação são implementados de forma inadequada, permitindo que qualquer usuario seja reconhecido como legítimo, seja por uso de credenciais fracas ou padrão, ausência de proteção contra tentativas automatizadas ou falhas na validação de sessões. Não é totalmente identificável por meios passivos, mas algumas características podem ser identificadas, como a exposição de interfaces de login ou painéis administrativos, uso de autenticação básica sem criptografia, serviços acessíveis sem autenticação adequada ou transmissão de credenciais por meio de HTTP sem TLS.

É importante ressaltar que o presente trabalho somente utilizará dados obtidos de forma ética através de monitoramento passivo e que muitas outras vulnerabilidades ligadas ao tema só poderiam realmente ser diagnosticadas ou confirmadas através de testes invasivos que requerem interação direta com os sistemas.

O assunto abordado é de grande importancia e deve ser tratada com mais seriedade tanto por profissionais da área quanto pelos consumidores e usuarios, uma vez que os dados e a segurança de todos entram em risco devido à má prática da segurança da informação.

1.4. Metodologia

O trabalho será realizada de forma descritiva e quantitativa, utilizando dados provenientes de observação passiva de serviços publicamente acessíveis no Brasil. Durante o período X-Y, as informações serão obtidas em plataformas de inteligência (Shodan e Censys), com coletas regulares e filtro geográfico para o país. Os seguintes atributos serão extraídos por meio de consultas utilizando: IP (anonimizado posteriormente), porta, protocolo, família de serviço, banner/headers, versão quando disponível, indicador de uso de TLS/STARTTLS, ASN e UF. Antes da análise, os registros serão unificados em uma única base, com a normalização de nomes, extração de versões, deduplicação por IP:porta:protocolo e anonimização.

A análise será realizada em duas fases. Na primeira, serão geradas medidas de exposição: totais e percentuais por categoria de serviço, porta e protocolo, distribuição consolidada por UF e ASN, além de listas Top-N por prevalência. Na segunda, serão analisadas vulnerabilidades por meio de sinais visíveis: porcentagem de versões possivelmente desatualizadas por tecnologia e frequência de configurações inseguras identificáveis em banner/protocolo; quando pertinente, haverá mapeamento para catálogos públicos (CVE) e métricas (CVSS/EPSS). Os resultados serão exibidos apenas em nível agregado, utilizando tabelas e visualizações, com validação cruzada entre plataformas e registro completo de consultas, dicionário de dados e scripts no apêndice. Durante todo o processo, serão respeitados os princípios de anonimização, minimização de dados e aderência aos termos de uso das fontes.

1.4.1. Tecnologias utilizadas

- Plataformas de coleta de dados: Shodan, Censys, Netlas.
- Bases de vulnerabilidades e referência: CVE (Common Vulnerabilities and Exposures), NVD (National Vulnerability Database), OWASP Top 10.

- Ferramentas de consulta e exploração de dados: APIs do Shodan e Censys, consultas em linguagem própria das plataformas.
- Ferramentas auxiliares: GitHub

1.5. Organização do trabalho

Este trabalho está estruturado da seguinte forma:

- Capítulo 1: apresenta a introdução, objetivos, justificativa, metodologia e organização geral da monografia.
- Capítulo 2: contém a fundamentação teórica necessária, abordando conceitos relacionados à segurança da informação, serviços expostos na internet, superfície de ataque e vulnerabilidades conhecidas.
- Capítulo 3: descreve os materiais e métodos utilizados no trabalho, e suas origens, explicando as ferramentas empregadas na coleta de dados e a maneira como as informações foram analisadas.
- Capítulo 4: apresenta os resultados obtidos durante a análise, enfatizando os padrões observados, configurações inseguras ou softwares vulneráveis identificados, entrando em detalhes quando necessário para melhor exemplificação.
- Capítulo 5: traz as considerações finais do trabalho, discutindo as principais conclusões do trabalho e suas implicações para a segurança de sistemas conectados à internet.
- Por fim, são apresentadas as Considerações Finais do trabalho, seguidas das Referências utilizadas para fundamentar o trabalho.

Ao final deste capitulo, destaca-se que a análise proposta busca contribuir para uma compreensão melhor e mais detalhada da exposição de serviços no Brasil, evidenciando a importância de práticas adequadas de configuração, manutenção e gestão da segurança em sistemas conectados à rede.

2. FUNDAMENTAÇÃO TEÓRICA

O presente capítulo tem como objetivo apresentar a fundamentação teórica necessária para a compreensão do problema abordado, como os fundamentos de segurança da informação, vetores, superfície de ataque e exposição de serviços. Também são discutidas algumas referências como OWASP Top 10 que é amplamente reconhecida e conceituada na área de cybersegurança, assim como bases públicas de classificação de riscos e vulnerabilidades. Em seguida, são abordados o funcionamento das plataformas utilizadas, como Shodan, Netlas e Censys, bem como os princípios de seu monitoramento passivo, suas implicações éticas e eficácia em determinar ou identificar algumas das vulnerabilidades abordadas. Por fim, são apresentados os conceitos relacionados às vulnerabilidades presentes no ranking OWASP Top 10 2025 que serão analisadas neste trabalho de forma a elucidar as suas respectivas causas, funcionamento e mitigação.

2.1. Vulnerabilidade

Vulnerabilidade, na segurança da informação, é uma falha ou fraqueza presente em um sistema, software ou configuração que pode ser explorada/atacada para comprometer sua segurança. Essa exploração pode permitir acesso não autorizado, alteração de dados, interrupção de serviços ou exposição de informações sensíveis (NIST SP 800-30 Rev. 1).

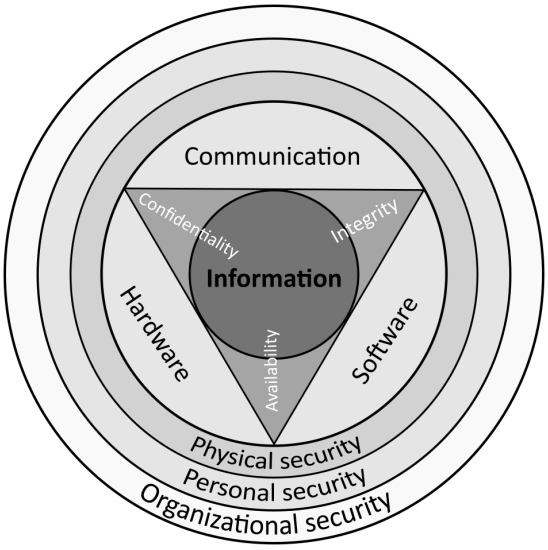
Essas falhas ocorrem por diversos motivos, como erros de desenvolvimento programação, configurações inadequadas ou uso de componentes ou software desatualizados. Em muitos casos, essas vulnerabilidades permanecem nos sistemas por longos períodos de tempo quando os mesmos não recebem manutenção adequada, não são bem administrados ou não recebem atualizações de segurança.

Portanto, a identificação de vulnerabilidades é essencial para a gestão de segurança, em grande parte fazendo uso de bases públicas como o CVE para registrar e acompanhar falhas em sistemas e softwares. Essas bases também costumam utilizar métricas de gradação de riscos e suas severidades (NIST, 2024), como o CVSS, se baseando em diversos fatores, sendo alguns deles: complexidade do ataque, privilégios necessários, escopo, impacto, entre outros (FIRST, 2026).

2.2. Segurança da informação

A segurança da informação é um dos pilares fundamentais para o funcionamento de sistemas digitais. Envolvendo um conjunto de técnicas que visam proteger dados e sistemas contra acessos não autorizados, alterações não autorizadas ou interrupções de funcionamento (NIST, 2020).A segurança da informação é baseada em três princípios centrais conhecido como Tríade CIA (do inglês Confidentiality, Integrity, and Availability) exemplificados pelas figuras 1 e 2.

Figura 1. Atributos da Segurança da informação



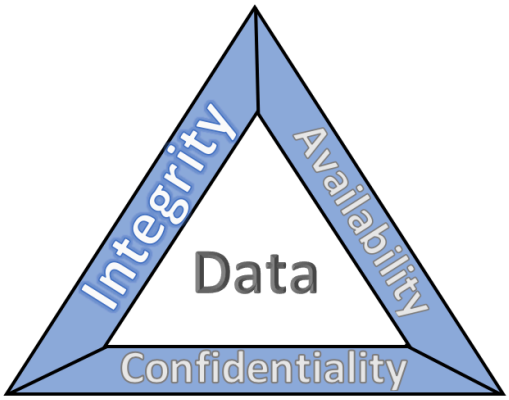
Fonte: https://en.wikipedia.org/wiki/Information_security

- Confidencialidade: É a garantia de que a informação será acessada apenas por pessoas ou sistemas autorizados. Sendo mais associado à privacidade.
    - Aplicação: Através de criptografia de dados, desde o uso de criptografia em protocolos de conexão como HTTPS até a criptografia de arquivos locais ou de mensagens criptografadas P2P assim como diversas outras técnicas.
- Integridade: É a garantia de que a informação se manterá íntegra, sem perdas ou modificações não autorizadas, sejam elas intencionais ou acidentais (Blacksmith InfoSec, 2025)
    - Aplicação: Usando funções de hash, checksum, assinaturas digitais, auditorias de sistema e controles de versão de forma que mesmo

pequenas alterações sejam detectadas ou pelo sistema ou pelo usuário e em alguns casos existe a possibilidade de restauração.

- Disponibilidade: É a garantia de que os dados e sistemas estejam acessíveis e utilizáveis sempre que os usuários autorizados precisarem. (Lumos, 2025)
    - Aplicação: Através de backups regulares, infraestrutura redundante, proteções contra ataques de Negação de Serviço (DDoS), e outras medidas que mantêm um sistema ou dado acessível mesmo sob condições adversas ou mitigando tais condições.

Figura 2. Tríade CIA



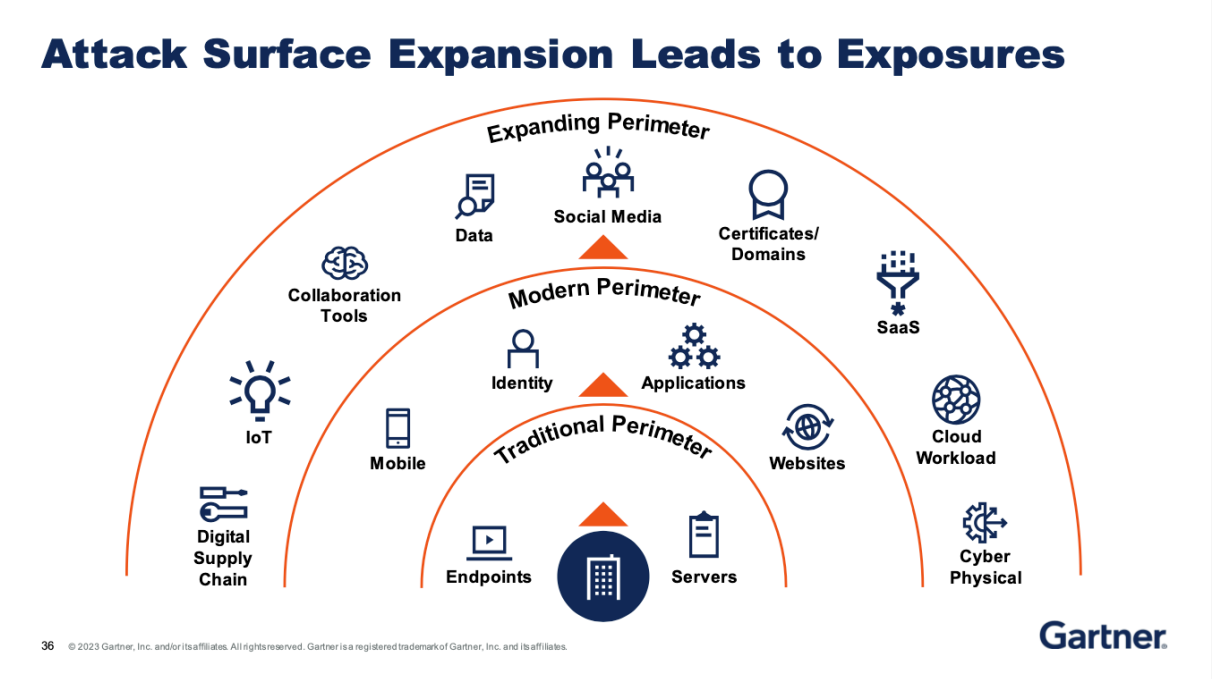
Fonte: NIST SPECIAL PUBLICATION 1800-26A

2.3. Superfície de Ataque

O conceito de superfície de ataque se refere a soma total dos possiveis pontos de entrada (também denominados vetores) que podem ser utilizados para interagir com um sistema (GAO, 2018), de forma autorizada ou não. Em ambientes conectados a internet, essa superfície inclui serviços expostos, portas abertas a rede publica, interfaces administrativas, APIs e outras partes do sistema que são acessíveis remotamente.

Quanto maior a superfície de ataque de um sistema, maior tende a ser o número de possíveis vetores de exploração disponíveis para agentes mal intencionados (NIST, 2020). Entender, monitorar e reduzir a superficie de ataque é essencial para qualquer sistema conectado a internet, principalmente quando há tráfego de informações sensíveis ou serviços essenciais para um negócio.

Figura 3. A expansão da superficie de ataque leva à exposição



Fonte: ©Gartner, Inc., Emerging Cybersecurity Market Trends and Growth Opportunities, June 2023

A superfície de ataque não é um bloco único (figura 3), ela é geralmente dividida em diferentes camadas, onde as vulnerabilidades podem se encontrar.

- Superfície de Rede (Network Attack Surface): Refere-se a tudo que está exposto na infraestrutura, como portas abertas, protocolos inseguros e serviços mal configurados.
    - Exemplo: Ter um banco de dados onde a porta de conexão está mapeada para a rede publica sem a proteção de um firewall ou autenticação.
- Superfície de Software/Aplicação (Software Attack Surface): Envolve o código-fonte, os endpoints de APIs, as interfaces administrativas e todas as dependências de um determinado sistema.
    - Exemplo: Falhas de gerenciamento de memória em aplicações escritas em C ou C++ (como buffer overflows) ou até mesmo um formulário web sem tratamento de input.
- Superfície Humana (Human Attack Surface): Muitas vezes negligenciada na arquitetura de sistemas, refere-se aos usuários, desenvolvedores e administradores do sistema.

- Exemplo: O comprometimento de credenciais válidas através de ataques de engenharia social (phishing), complacência ou falta de treinamento ou consciência de praticas de segurança.

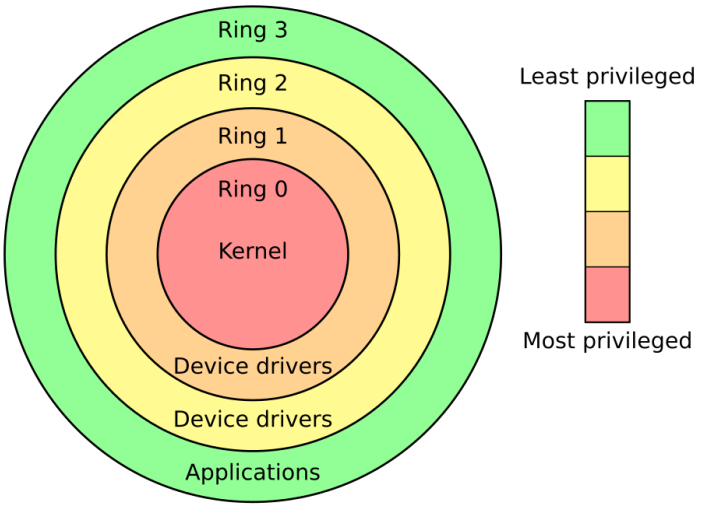
Uma distinção importante deve ser feita entre uma superficie de ataque e um vetor de ataque (OWASP, 2026).

- A Superfície de Ataque é o "onde", são os locais de onde se iniciaria um ataque para ganhar acesso, alguns exemplos sendo, as portas abertas, os formulários de login e as APIs disponíveis.
- O Vetor de Ataque é o "como". É a técnica ou método específico que um agente mal-intencionado utiliza para atravessar a superfície de ataque, como por exemplo ataques de injeção de SQL ou mais recentemente injeção de prompt.

Compreender a superfície de ataque leva diretamente a prática de mitigação da mesma, um processo frequentemente chamado de Hardening. Que em grande parte incluem:

- Princípio do Menor Privilégio (PoLP)**:** Serviços, processos e usuários devem ter apenas o nível mínimo e estrito de acesso necessário para funcionar adequadamente e nunca acessar outras partes do sistema fora da sua área ou competência (figura 4), levando a um controle de acesso bem estabelecido.

Figura 4. Princípio do Menor Privilégio



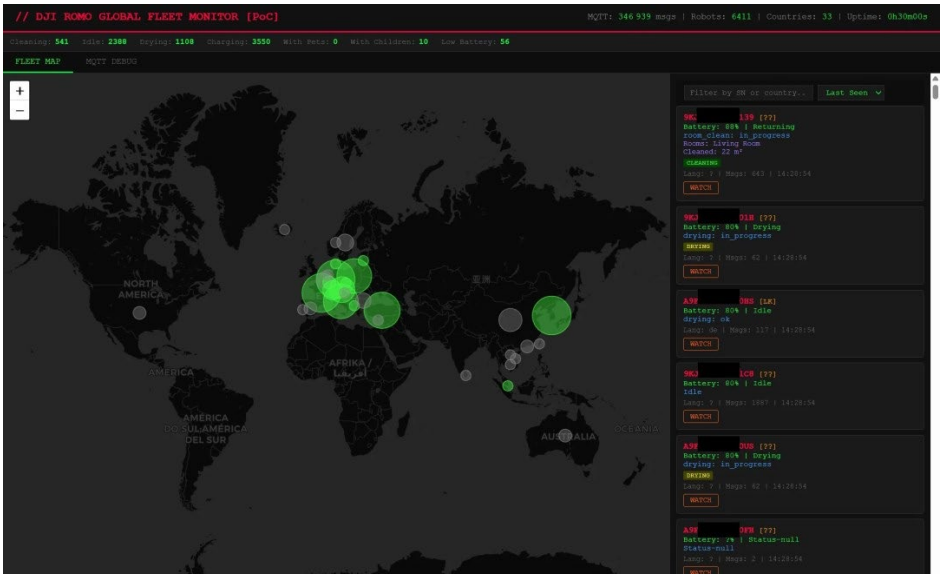
Fonte: https://en.wikipedia.org/wiki/Principle_of_least_privilege

- Desativação de Recursos Desnecessários: Se uma funcionalidade, porta ou serviço legado não é mais estritamente necessário para o funcionamento do sistema ou não está mais sendo utilizado, ele deve ser desligado ou bloqueado uma vez que aumenta a superfície de ataque e principalmente pela falta de interação, que pode fazer com que seja esquecido e se torna um risco ainda maior, se tornando algo conhecido como “Shadow IT”, que significa um recurso que existe na infraestrutura da empresa sem o conhecimento, aprovação ou supervisão do departamento de TI (IBM, s.d.).
- Segmentação e Isolamento: Dividir a arquitetura para que o comprometimento de um serviço não conceda acesso automático aos outros, como por exemplo isolar a rede de dados da rede de aplicação ou isolar as camadas de um software ou até mesmo o isolamento de ambientes com a finalidade de limitar o acesso dos usuarios.

Um ótimo exemplo de vetores e superficie de ataque é o fato de que mesmo dispositivos IoT como Lâmpadas Smart com conexão a internet são um vetor de ataque explorável, dando possível acesso à rede e possivelmente de outros sistemas dos locais que as utilizam (Cornell University, 2023). As lâmpadas são somente um vetor onde o adversário foi capaz de interagir e estudar seu funcionamento até conseguir acesso.

O mesmo também é verdade para Robôs, que também são considerados dispositivos IoT, neste caso o ultimo exemplo relacionado ao DJI Romo Robovac, que foi hackeado acidentalmente por Sammy Azdoufal (The Verge, 2026), um engenheiro de software, que tentava controlar o seu próprio robô com um controle de Playstation 5, e descobriu que tinha acesso a 6,700 dispositivos similares assim como acesso as suas câmeras, microfones e mapas das casas onde operam.

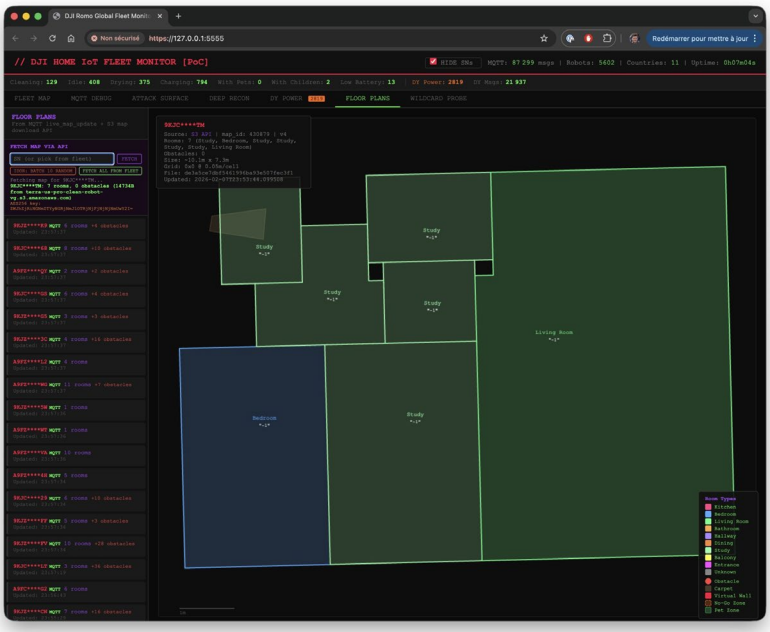
Figura 5. Mapa de dispositivos DJI Romo comprometidos em 24 países



Fonte: https://www.theverge.com/tech/879088/dji-romo-hack-vulnerability-remote-control-camera-access-mqtt

Outros dispositivos também podiam ser acessados levando o numero total de dispositivos comprometidos a mais de 10,000 (figura 5), incluindo dispositivos como centrais elétricas (DJI Power Station) e outros (techspot, 2026).

Figura 6. Mapa de uma casa acessado pelo DJI Romo



Fonte: https://www.theverge.com/tech/879088/dji-romo-hack-vulnerability-remote-control-camera-access-mqtt

Em ambos os casos, os dispositivos são vetores, e fazem parte de uma superfície de ataque dos locais onde são utilizados, revelando dados sensíveis (figura 6) e possivelmente expondo a própria rede acessos indevidos ou ataques.

2.4. Superfície de Ataque Externa e Serviços Expostos

Superficie de Ataque Externa (FortifyData, 2025) se refere a tudo que interage com usuários ou sistemas externos, seja como uma Superficie de Ataque de Rede ou de Software como mencionado no item anterior.

Os exemplos mais comuns são: servidores web, bancos de dados, APIs, serviços de acesso remoto, dispositivos IoT e interfaces administrativas. Mesmo que muitos desses serviços tenham sido projetados para operar publicamente, outros são expostos indevidamente por conta de erros de configuração, falta de segmentação de rede ou ausência de técnicas adequados de autenticação e controle de acesso.

A gerencia adequada de tais ambientes requere o conhecimento de como tal visibilidade funciona, ela pode ser categorizada em duas vertentes principais:

- Exposição Intencional: Serviços projetados especificamente para acesso público, como servidores web e APIs. Nesses casos, a proteção foca em

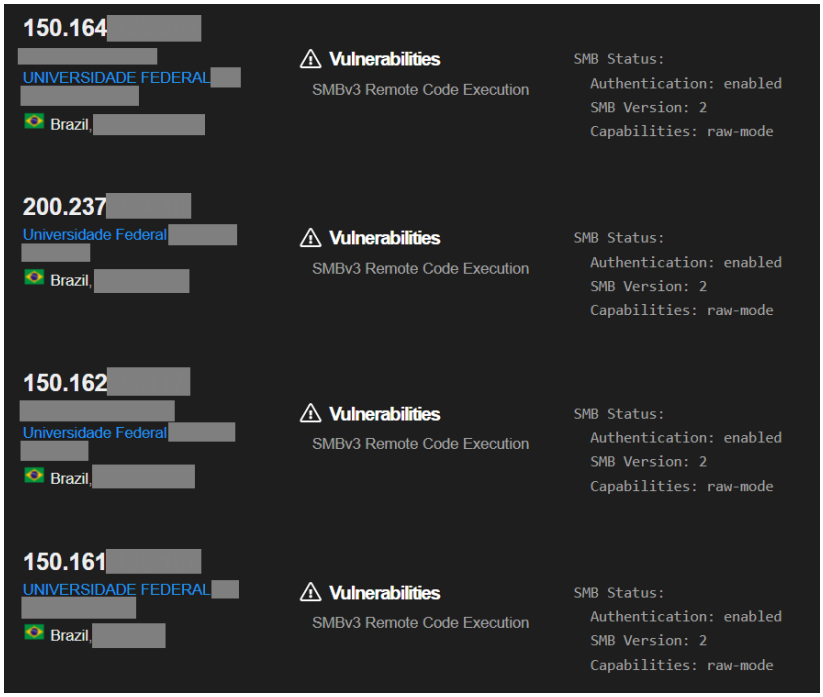
proteger a "porta de entrada" por meio de Web Application Firewalls (WAF), criptografia e testes de segurança.

- Exposição Acidental: Serviços estritamente internos, como bancos de dados ou portas SSH, que se tornam visíveis por falhas de configuração ou pela presença de recursos que não foram devidamente documentados ou foram abandonados (conhecido como Shadow IT). Que representa um dos maiores riscos cibernéticos na atualidade no mundo todo.

Uma vez que um vetor se encontra exposto, a internet atua como um ambiente de varredura constante, onde agentes maliciosos buscam vetores de ataque e tentam explorar vulnerabilidades. As táticas mais comuns para busca e exploração incluem:

- Mapeamento Automatizado: Pode ser feito com a utilização de plataformas de busca especializados, como o Shodan (figura 7), varrendo a internet continuamente para localizar e indexar portas abertas e serviços, sendo também possível identificar vulnerabilidades em alguns casos.

Figura 7. Shodan: Universidades Brasileiras com a vulnerabilidade SMBGhost

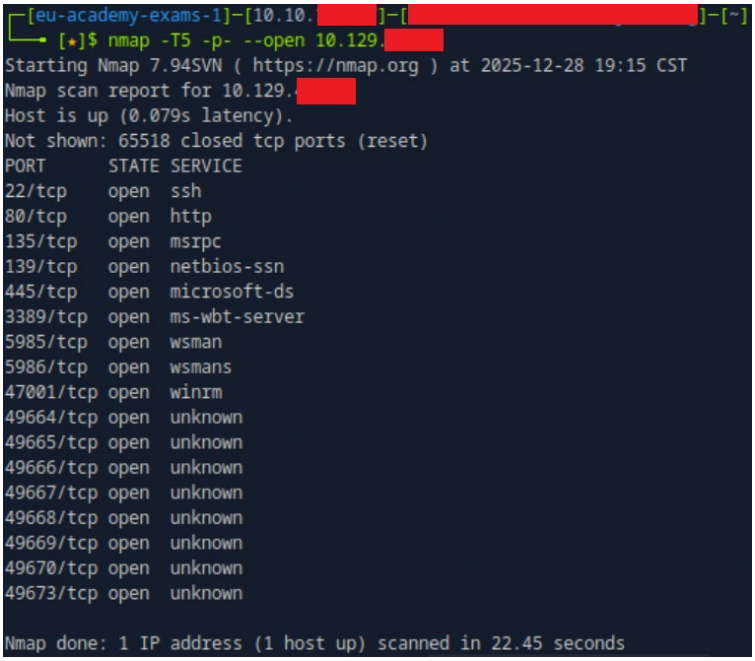


Fonte: Autoria própria

- Enumeração de serviços e portas (figura 8): Utilizando ferramentas mais intrusivas como Nmap, agentes maliciosos conseguem identificar diversas

informações sobre um alvo, como portas abertas, serviços em execução, regras de firewall, tipos de autenticação ativos em serviços específicos e versões de software, que podem expor vulnerabilidades existentes nos sistemas.

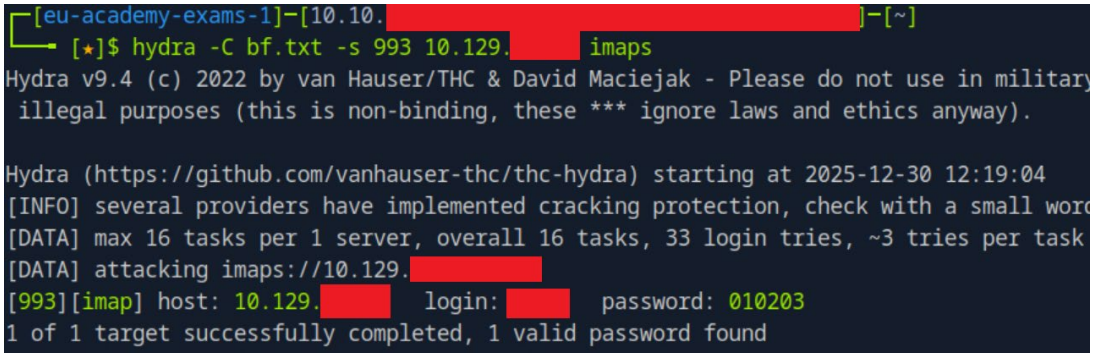
Figura 8. Escaneamento de ports utilizando Nmap



Fonte: Autoria própria

- Ataques de Força Bruta (figura 9): Execução de multiplas tentativas de acesso, na maioria das vezes através do uso de wordlists contendo milhares ou até milhões das credenciais mais utilizadas, credenciais padrão de certos sistemas ou wordlists criadas para alvos específicos. A ideia sendo que através de pura tentativa e erro, as credenciais corretas sejam encontradas.

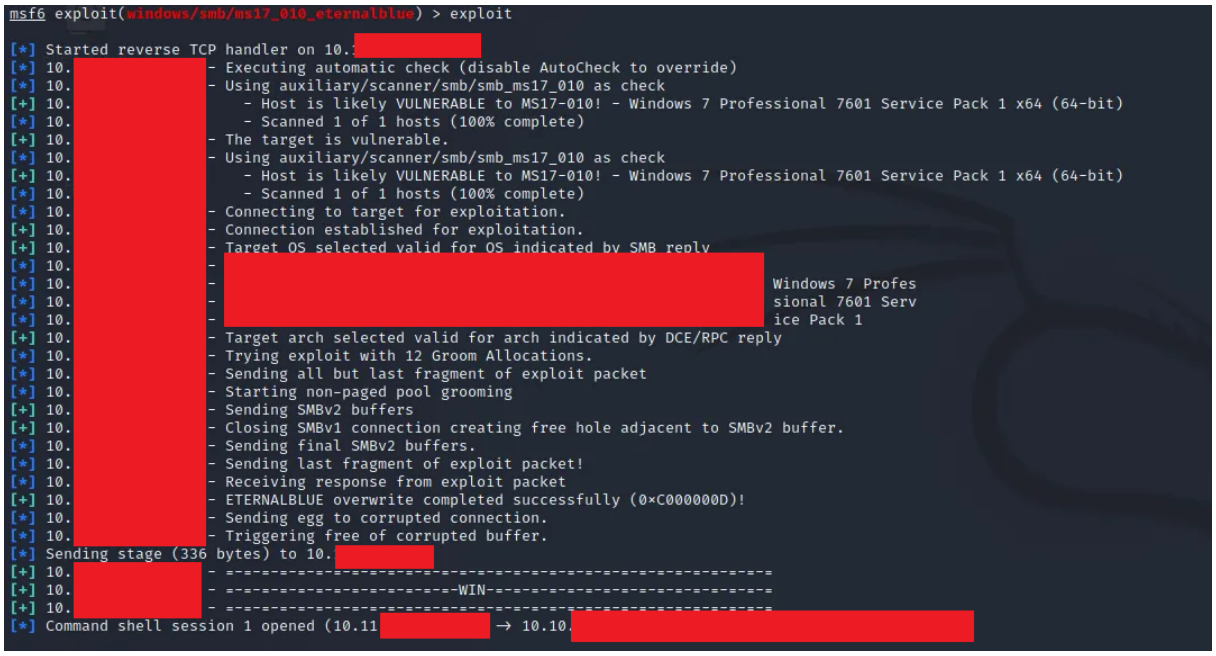
Figura 9. Hydra usando bruteforce conta servidor IMAP



Fonte: Autoria proópria

- Exploração de Vulnerabilidades (CVEs): Aproveitamento de falhas documentadas em sistemas que operam com softwares desatualizados, configurando a principal via de entrada para ataques de ransomware em redes corporativas e acesso indevido a dispositivos expostos (figura 10).

Figura 10. Exploração de vulnerabilidade EternalBlue



Fonte: Autoria própria

Em um mundo com ameaças constantes, algumas medidas devem ser tomadas para melhor mitigação e controle, visando manter a integridade dos sistemas:

- Arquitetura DMZ (Zona Desmilitarizada): Segregação de serviços em uma sub-rede lógica ou fisicamente separada, agindo como um perímetro de segurança,

isolando serviços e sistemas internos para que uma empresa consiga interagir com redes não seguras como a internet aberta mas mantendo a segurança da sua rede interna (fortinet, 2025).

- Acesso Seguro e VPNs: Envolve o controle absoluto do acesso a ferramentas de gerenciamento, redobrando verificações e isolamento. O acesso somente pode ser feito por meio de conexões autorizadas previamente, como VPNs e no caso de arquiteturas baseadas em ZTNA ou Rede de Confiança Zero, que utilizam autenticação continua para todos os pedidos de acesso mesmo internos. Essas estratégias visam separar o tráfego interno da rede pública e restringir (Palo Alto Networks, 2025).
    - VPNs: VPNs permitem a implementação de 3 medidas de controle de acesso, a autenticação de usuários, dispositivos e conexões, sendo também capaz de criar um “túnel” criptografado que isola todo o tráfego interno da rede externa, protegendo dados contra tentativas de monitoramento passivo e interceptação (NIST, 2020; Hong Kong CERT, 2024).
    - ZTNAs**:** Diferente de redes tradicionais, as redes Zero Trust não confiam implícitamente em nenhum dispositivo ou usuário que já se encontra na rede, continuamente realizando uma nova autenticação de todas as requisições de conexão. Os princípios centrais são a eliminação de confiança implícita (“never trust, always verify”), aplicação de menor privilégio para boa segregação de autorizações, segmentação granular dos recursos limitando o acesso somente a recursos necessarios e a premissa de que invasões e ataques podem ocorrer a qualquer momento, exigindo mecanismos de contenção e monitoramento constante (Palo Alto Networks, 2025).

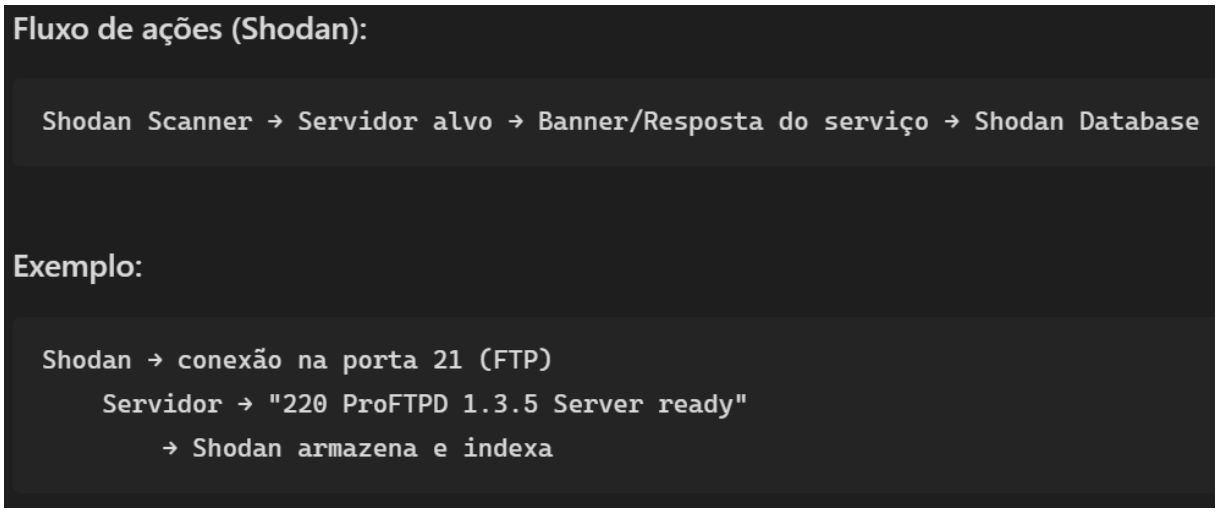
- Monitoramento de Superfície de Ataque Externo (EASM): É o uso de ferramentas que realizam escaneamentos automáticos e contínuos a partir de uma fonte externa contra a infraestrutura exposta ao exterior. Isso permite a identificação de vetores expostos como portas abertas, vulnerabilidades e erros de configuração. O escaneamento continuo garante uma rapida identificação e a mitigação de riscos antes de um possível ataque e exploração de vulnerabilidades (NCSC, 2025).

2.5. Monitoramento Passivo

O monitoramento passivo consiste da coleta e análise de informações relacionadas a vetores expostos na internet, sem interação direta com os sistemas analisados. Uma explicação simplificada de tal processo é o fato de que o monitoramento somente faz a indexação das informações que já são normalmente enviadas durante qualquer tipo de interação legitima, algo que não requer uma interação ou requisição específica ou fora do comum que possa forçar um comportamento atipico.

Ferramentas como Shodan, Censys e Netlas operam por meio do envio contínuo de requisições a serviços acessíveis publicamente, registrando todas as informações disponíveis, como portas abertas, banners de serviços, certificados digitais e versões de software. Esses dados são organizados em bases indexadas que permitem consultas e análises sobre a exposição de sistemas na internet (Shodan, s.d.; Censys, s.d.; Netlas, 2024).

Figura 11. Monitoramento Passivo (Shodan)

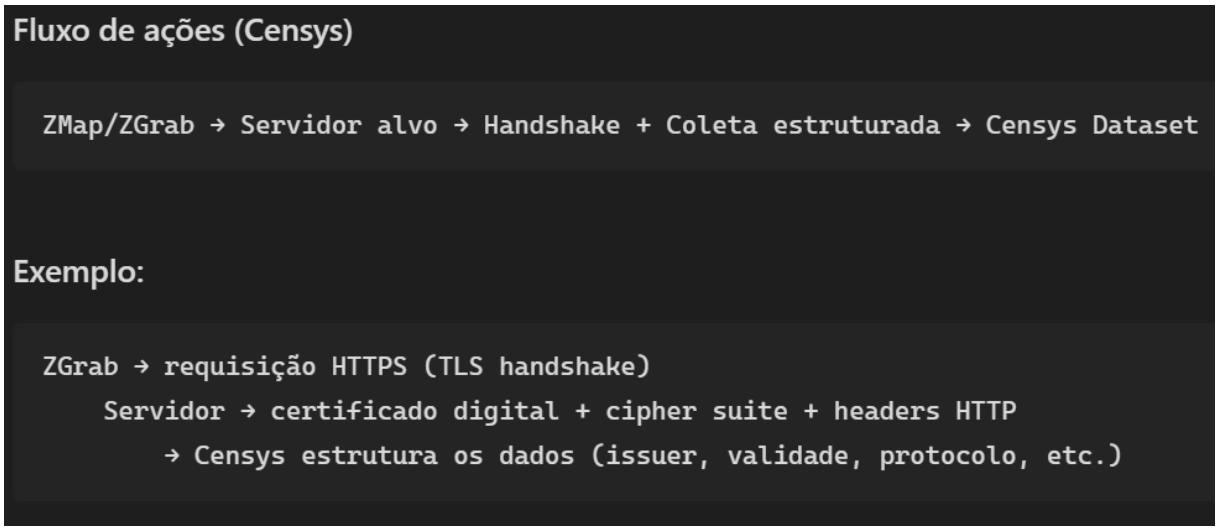


Fonte: Autoria Própria

Explicação da figura 11:

- Shodan envia requisições simples (e.g: TCP SYN, HTTP GET, conexão a porta 21/22/80/443).
- O servidor responde com um banner ou metadados do serviço (e.g: versão de servidor Apache, FTP, SSH).
- Shodan armazena essa resposta bruta e indexa para busca.

Figura 12. Monitoramento Passivo (Censys)



Fonte: Autoria Própria

Explicação da figura 12**:**

- Censys usa ferramentas como ZMap (descoberta de hosts) e ZGrab (coleta detalhada).
- Handshakes completos são realizados (ex: TLS, HTTP) e extrai dados estruturados.
- Os dados são processados e organizados em formato pesquisável (JSON).

Dessa forma, o monitoramento passivo se mostra uma abordagem eficiente para identificação de superfícies de ataque externo, sendo amplamente utilizado em atividades de OSINT (Inteligencia Open Source) assim como na análise e gerenciamento de segurança.

2.6. Análise das Principais Vulnerabilidades segundo o OWASP Top 10 (2025)

Este tópico apresenta a análise de algumas das vulnerabilidades presentes no ranking OWASP Top 10 2025, sendo a OWASP uma das instituições de maior referência e com mais reconhecimento na área de segurança de aplicações. O ranking reúne as falhas mais críticas e comuns observadas em sistemas web, com base em

dados reais de incidentes, feito com a cooperação de instituições assim como profissionais autônomos e pesquisadores da área. Compreender tais vulnerabilidades é fundamental uma melhor identificação dos riscos associados à exposição de vetores na internet, bem como para uma orientação de melhores práticas de desenvolvimento seguro e mitigação de ameaças. Nos seguinte subtópicos, são abordadas as vulnerabilidades, destacando suas características, formas de exploração e possíveis medidas de prevenção respectivamente.

2.6.1. Broken Access Control (A01:2025)

O controle de acesso aplica políticas de forma que os usuários não possam agir além das permissões que lhes foram atribuídas. Falhas geralmente resultam na divulgação não autorizada de informações, na modificação ou destruição de todos os dados, ou na execução de uma função comercial fora dos limites do usuário.

A vulnerabilidade A01:2025 – Broken Access Control ocorre pela ausência ou falha na implementação do controle de acesso dos usuários aos recursos de um dado sistema, mais comumente causado por erros de configuração ou de desenvolvimento de um sistema.

Em sistemas seguros, o controle de acesso garante que os usuários somente possam executar ações dentro de suas permissões. Quando o controle de acesso é insuficiente ou inexistente, os usuários são capazes de realizar ações restritas como acesso e modificação de dados ou até mesmo a execução de comandos dos quais não deveriam ter sequer acesso ou autorização para executar (OWASP TOP 10 2025, 2026).

Alguns exemplos incluem acesso URLs restritas como páginas de login internas sem a necessidade de conexão através de VPNs ou outros mecanismos, manipulação direta de identificadores ou queries, também conhecida como a vulnerabilidade IDOR, que permite qualquer usuário a diretamente alterar um identificador ou query presente na URL e ter acesso a páginas ou dados que não deveria (e.g. alterar user?id=78 para user?id=0 e a ausência de autenticação ou validação de tokens em requisições, possibilitando que usuários possam fazer requisições das quais não deveriam (utilizando o comando “curl”) e execução de métodos como POST, PUT e DELETE em APIs.

As consequências de tais falhas são críticas, podendo levar ao vazamento ou destruição massiva de dados, execução de comandos administrativos por usuários não autorizados ou até mesmo o comprometimento de outros dispositivos e sistemas.

De acordo com a OWASP, a vulnerabilidade de controle de acesso permanece em primeiro lugar como a mais explorada em aplicações web, sendo frequentemente associada a incidentes de segurança com alto impacto (OWASP, 2025).

Para a prevenção dessa vulnerabilidade OWASP recomenda que o controle de acesso seja implementado exclusivamente no lado do servidor ou em APIs Serverless confiáveis, impedindo sua manipulação por usuários. Se deve também adotar princípios como PoLP (principio do menor privilegio) e Zero Trust, permitindo acesso somente de recursos necessários e constantemente autenticando todas as requisições. Além disso, é importante centralizar e reutilizar módulos de controle de acesso, limitar o uso de CORS e a aplicação das regras de negócio de forma adequada.

Outras boas práticas incluem desabilitar a listagem de diretórios em servidores web, evitar a exposição de arquivos sensíveis, registrar logs de controle de acesso, implementar restrições de requisição para impedir ataques automatizados. Todas as sessões devem ser invalidadas corretamente após logout, e tokens JWT devem possuir tempo de vida reduzido assim como mecanismos de revogação. Por fim, OWASP recomenda o uso de bibliotecas consolidadas para controle de acesso e a utilização de testes durante o desenvolvimento para garantir o funcionamento correto desses mecanismos (OWASP, 2025).

2.6.2. Security Misconfiguration (A02:2025)

Esta vulnerabilidade ocorre quando um sistema, aplicativo ou serviço em nuvem é configurado de forma incorreta do ponto de vista da segurança, criando vulnerabilidades (OWASP TOP 10, 2025). Ocorrendo muitas vezes devido a falhas operacionais, ausência de padronização ou priorização de compatibilidade em detrimento da segurança.

Entre as causas mais comuns estão a presença de funcionalidades desnecessárias habilitadas, como portas, o uso de credenciais padrão para serviços e contas sem alteração, a exposição de mensagens de erro internas detalhadas que revelam credenciais do sistema como strings de conexão de bancos de dados. Além disso, configurações inseguras ou padrão em servidores, frameworks, bibliotecas e bancos de dados, assim como a ausência de cabeçalhos de segurança em respostas HTTP.

A prevenção de Security Misconfiguration se baseia na utilização de processos seguros e padronizados de configuração dos sistemas. Incluindo a implementação de hardening em todos os ambientes (desenvolvimento, teste e produção), garantindo que estejam configurados de forma resiliente e padronizada, porém com credenciais distintas.

É necessário ressaltar novamente que manter uma plataforma mínima e reduzir ao máximo possíveis vetores de Shadow IT é fundamental, removendo tudo que não esteja sendo utilizado ou que seja desnecessário, além de realizar revisões periódicas de configurações, permissões e atualizações de segurança. A utilização de arquiteturas segmentadas e o envio de cabeçalhos de segurança também contribuem para a redução da superfície de ataque.

Por fim, é recomendada a automação da verificação das configurações, evitando erros manuais de configuração, assim como o uso de mecanismos seguros de autenticação, como credenciais temporárias de vida curta fornecidos pela plataforma e controle de acesso baseado nas funções dos usuarios, ao invés de utilizar senhas estáticas embarcadas no código, arquivos ou pipelines.

2.6.3. Software Supply Chain Failures (A03:2025)

Essa vulnerabilidade ocorre quando há falhas ou comprometimentos no processo de desenvolvimento, distribuição ou atualização de software, geralmente envolvendo componentes de terceiros. Isso inclui bibliotecas, plugins, frameworks, ferramentas e dependências que, quando vulneráveis ou manipuladas maliciosamente, podem comprometer todo o sistema (OWASP TOP 10, 2025).

Exemplos comuns que levam a vulnerabilidades deste tipo são a utilização de plugins, em muitos casos tais plugins se tornam a porta de entrada de ataques uma vez que o dono do sistema não tem controle sobre tais componentes e a sua manutenção ou monitoramento também é falha. Especificamente paginas web que utilizam Wordpress e seus plugins costumam ser notórios pelas suas vulnerabilidades uma vez que os plugins raramente são corretamente mantidos ou atualizados, o que resulta em 96% dos ataques em paginas que utilizam Wordpress se origina em plugins (Security Week, 2025; Kaspersky Daily, 2025)

Indicações de que o sistema pode estar vulnerável são a ausência ou impossibilidade de controle adequado sobre versões de componentes e dependências pelos administradores, o uso de softwares desatualizados ou sem suporte e a falta de varreduras regulares por vulnerabilidades assim como a falta de atualizações de segurança. Também indicam risco a ausência de controle de versões na cadeia de desenvolvimento, o uso de componentes de terceiros (principalmente de fontes não confiáveis) e também a ausência de controles de acesso e do uso do princípio de menor privilégio juntamente com as politicas de controle de acesso (OWASP TOP 10, 2025).

É recomendado para a redução das falhas na cadeia de suprimento de software, a utilização de um processo estruturado de gestão de patches e dependências, que inclui a criação e manutenção de um SBOM para mapear todos os componentes e suas dependências diretas e indiretas, eliminando a possiblidade de Shadow IT e outros problemas relacionados. Se deve manter um inventário atualizado das versões utilizadas pelo sistema, utilizar monitoramento constante de bases publicas como CVE e NVD e automatizar a detecção de vulnerabilidades. Também é necessário garantir que somente serão utilizados componentes de fontes confiáveis, preferencialmente assinados. É necessário sempre que possível, remover dependências desnecessárias e atualizar sistemas e ferramentas de forma organizada, com testes e implantação gradual. Além disso, é necessário implementar uma gestão rigorosa de mudanças, implementar hardening em repositórios, pipelines e ambientes de desenvolvimento (com controle de acesso, MFA e segregação de funções), e também garantir a integridade dos artefatos. Por fim, deve haver um processo contínuo de monitoramento, priorização e aplicação de correções ao longo de todo o ciclo de vida do software.

2.6.4. Cryptographic Failures (A04:2025)

Esta vulnerabilidade ocorre quando dados de forma geral, não são devidamente protegidos utilizando criptografia, seja durante a transmissão ou no armazenamento de tais dados. Alguns exemplos sendo o uso incorreto de algoritmos (obsoletos ou com má implementação), falhas na administração de senhas e chaves, armazenamento de dados sensíveis sem criptografia ou utilização de protocolos inseguros. Todos estes fatores contribuem para o aumento do risco de exposição de dados sensíveis como senhas, informações pessoais e dados financeiros (OWASP TOP 10, 2025; NIST SP 800-175B, 2020).

Exemplos desse tipo de vulnerabilidade incluem:

- Uso de algoritmos obsoletos como MD5 ou SHA-1 que não são considerados seguros uma vez que já se sabe descriptografar dados que utilizaram tais métodos de criptografia.
- Reutilização ou má gestão de chaves criptográficas, geralmente observado quando um usuário utiliza a mesma senha para diversos serviços, de forma que um único caso de exposição de credenciais leva ao comprometimento de diversos serviços que por sua vez podem conter mais dados sensíveis e credenciais, em alguns casos também observados devido a chaves e senhas de baixo nível de segurança/complexidade
- Ausência de validação adequada de certificados digitais e a transmissão de dados sensíveis sem criptografia, como por exemplo, via HTTP ou protocolos inseguros.
- Também são frequentes erros como o uso de modos de operação inseguros como o ECB (Eletronic Code Book), geração inadequada de números aleatórios e armazenamento de chaves diretamente no código-fonte, o que facilita sua exposição e exploração (OWASP TOP 10, 2025; NIST SP 800-38A, 2001).

Para evitar a ocorrência desse tipo de vulnerabilidade, é necessário a classificação adequada dos tipos de dados manipulados e aplicar criptografia adequadamente tanto em trânsito quanto em repouso (durante armazenamento sem

transmissão), utilizando algoritmos e protocolos atualizados (como TLS 1.2 ou superior). Se deve tambem implementar uma gestão segura de chaves, idealmente com uso de HSMs (Hardware Security Modules), evitar o armazenamento desnecessário de dados sensíveis e garantir o uso de funções de hash robustas (como Argon2 ou PBKDF2) para senhas, dados bancários e outras informações sensíveis. Também é fundamental evitar algoritmos obsoletos, utilizar bibliotecas de fontes confiáveis sempre que possivel, aplicar criptografia autenticada, configurar corretamente serviços e realizar revisões periódicas de segurança, garantindo conformidade com os padrões e regulamentações vigentes e aplicaveis (OWASP TOP 10, 2025).

Alguns incidentes notáveis são a exposição de dados da empresa finlandesa Vastaamo, que oferecia serviços de psicoterapia, e que em 2018 sofreu um ataque de ransonware, onde o hacker responsável foi capaz de obter dados como nome de pacientes, números de segurança social (similar ao CPF), endereços e anotações das sessões de terapia com psicólogos. O ataque se deu devido ao fato de que o banco de dados utilizava credenciais padrão para o usuário root (administrador) e ao mesmo tempo não havia criptografia protegendo os dados relacionados aos pacientes e funcionários como a anonimização e criptografia de sessões de terapia (Twingate, 2024; Wikipedia, s.d). Como resultado, o ataque inicial de 2018 continuou em 2019 e finalmente em 2020 foi anunciado, devido ao uso de ransonware e extorsão. A pesar da empresa pagando os hackers, os dados foram vazados, expondo informações detalhadas e em muitos casos particulares e intimas dos pacientes, a empresa foi severamente multada e declarou falência devido a este incidente que é considerado um dos maiores ataques com vazamento de dados do ramo da saúde em anos recentes.

Outro exemplo foi o vazamento de dados da empresa de registro de domínios GoDaddy, onde um ataque ocorreu devido ao comprometimento de credenciais, mas não antes dos responsáveis pelo ataque possuírem acesso por mais de dois anos aos sistemas da empresa. De acordo com um relatório submetido pela GoDaddy para a SEC (United States Securities and Exchange Commission), a empresa estava armazenando usuários e senhas sFTP (Secure File Transfer Protocol) o protocolo de transferência de arquivos de SSH (Secure Shell) em texto simples ou em algum formato que poderia ser convertido facilmente em texto simples, não utilizando

hashing de forma correta, e levando a exposição dos dados de mais de 1.2 milhões de usuários (WorldFence, 2021).

Um exemplo não de ataque, mas de uma falha de criptografia recente, onde a Comissão de Proteção de Dados da Irlanda (DPC - Data Protection Commission), órgão responsável pela proteção de dados, descobriu durante um inquérito que a empresa Meta (proprietária do Facebook, Instagram e outras redes sociais) estaria armazenando centenas de milhões de senhas em texto simples sem nenhum tipo de criptografia interna ou hashing e autuou a empresa em € 91.000.000 devido a violações de regulamentações vigentes relacionadas a proteção de dados (Malwarebytes, 2024; DPC, 2024).

2.6.5. Authentication Failures (A07:2025)

Essa vulnerabilidade ocorre quando um sistema falha na autenticação de um usuário. Isso pode ocorrer devido a diversas falhas nos mecanismos de autenticação, gestão de sessões ou validação de credenciais, possibilitando acessos não autorizados a sistemas e dados sensíveis (OWASP TOP 10, 2025).

Alguns dos exemplos mais comuns que levam a esse tipo de vulnerabilidade envolvem a falta de mecanismos para prevenir ataques como “credential stuffing” e força bruta, que utilizam wordlists e tentam acessar sistemas através de tentativa e erro de forma automatizada, como por exemplo a utilização de senhas fracas ou padrão, ausência de autenticação multifator (MFA - Multi-Factor Authentication) e mecanismos inseguros de recuperação de senha, além de praticas de MFA Fatigue, que consiste na realização de múltiplas requisições de MFA até que o usuário autorize indevidamente um dos pedidos. Também são frequentes problemas de armazenamento inadequado de credenciais, reutilização de sessões e de credenciais, exposição de identificadores de sessão em locais inseguros e falhas na invalidação de sessões após logout ou inatividade.

Indicações de que o sistema pode estar vulnerável são a ausência de proteção contra tentativas automatizadas de login como a utilização captchas e outros testes de verificação de interação humana, ausência de limitação de tentativas de login incorretas, permissividade no uso de senhas fracas ou comprometidas, inexistência de autenticação multifator e falhas nos processos de recuperação de acesso. Outros riscos também são a má gestão de sessões, como reutilização de identificadores,

exposição de tokens e ausência de invalidação adequada dos mesmos, além de falhas na validação do escopo e uso das credenciais fornecidas e validação de credenciais no lado do cliente (client-side credential validation) que tende a expor as credenciais ou facilitar outros ataques como desabilitar, forjar ou fazer um bypass completo da autenticação.

Para reduzir esse tipo de vulnerabilidade, é necessário a implementação de diversas medidas de segurança tais como autenticação multifator, utilização de políticas modernas de senha e monitoramento de vazamentos de credenciais contra bases de dados vazadas. Também é importante limitar tentativas de login, monitorar atividades suspeitas e evitar o uso de credenciais padrão. Se deve adotar mecanismos seguros de gerenciamento de sessão, com geração de identificadores aleatórios e invalidação adequada, além de utilizar soluções consolidadas para autenticação e identidade sempre que possível, reduzindo a superfície de erro e aumentando a segurança geral do sistema (OWASP TOP 10, 2025; NIST SP 800-63B-4, 2025).

Alguns exemplos das consequencias dessas falhas foram os ataques contra a Uber (2022) e 23andMe (2023).

Em 2022, a conta de um prestador de serviços terceirizado da empresa Uber foi comprometida, aparentemente com credenciais vazadas, o atacante (membro de um grupo conhecido como Lapsus$) contactou o funcionário via whatsapp se passando por um funcionário da própria Uber, o recomendando aprovar a validação de MFA enquanto enviava múltiplas tentativas de autenticação MFA (MFA Fatigue) para a vítima. A estratégia funcionou e após comprometer a conta inicial, o atacante foi capaz de acessar outras ferramentas internas e chegou a publicar imagens de um portal interno assim como alterar algumas das configurações. Felizmente os atacantes não chegaram a vazar nenhum dado da empresa (Uber, 2022; Upguard, 2025).

Em 2023, a empresa 23andMe sofreu um ataque que levou ao vazamento de dados de aproximadamente 6.9 milhões de usuários. O ataque foi realizado utilizando Credential Stuffing, comprometendo mais de 14.000 usuários que tiveram suas credenciais vazadas anteriormente e não haviam habilitado MFA, possibilitando que dados médicos dos próprios usuários fossem obtidos assim como outros dados pessoais, além disso, através de mecanismos da própria plataforma relacionados a arvores genealógicas os atacantes foram capazes de acessar dados de 6.9 milhões de usuários ampliando o impacto do ataque. Devido a falha de proteger as

informações de seus usuários, a empresa 23andMe foi multada em £2.3m pelo governo do Reino Unido (23andMe, 2023; The HIPAA journal, 2023; The Guardian, 2025).

2.7. OSINT

Open Source Intelligence é o processo de analisar qualquer informação em domínio publico para avaliar ameaças, tomar decisões ou responder perguntas especificas (IBM, s.d.).

OSINT pode coletar dados de praticamente qualquer fonte dês de que esteja acessível publicamente, isso inclui posts de redes sociais como Instagram, Facebook, X/Twitter, LinkedIn, registros públicos de pessoas como serviços de “listas telefônicas” digitais como White Pages ou plataformas jurídicas como Escavador ou Jusbrasil entre outros.

Dependendo das informações que se tem como objetivos, outras plataformas podem ser utilizadas, no caso da presente pesquisa, utilizaremos plataformas de OSINT relacionadas a vetores expostos à internet como Shodan, Netlas, Censys, ExploitDb, NVD entre outras.

3. MATERIAIS E MÉTODOS

Este capítulo tem como propósito descrever os procedimentos e estratégias aplicadas no desenvolvimento deste trabalho. Serão apresentadas as principais ferramentas utilizadas para coleta de dados e sua subsequente análise de forma a exemplificar de forma mais clara os métodos de obtenção, tipos de dados que podem ser obtidos e a ética das ferramentas utilizadas assim como da análise que será feita.

3.1. Visão geral das plataformas de OSINT para superfície exposta

Foram utilizadas ferramentas como Shodan, Netlas e Censys são plataformas de OSINT (Open Source Intelligence) utilizadas para identificar dispositivos e serviços expostos na internet. Diferentemente de buscadores comuns que focam no conteúdo de páginas web, elas não são focadas em sites mas nas infraestruturas dos sites, dispositivos e serviços, apresentando dados como portas abertas, certificados, serviços responsivos e versões de software expostos à internet pública (Censys, s.d.; Shodan, s.d.; Netlas, 2024).

Para cruzar a informação adquirida através de tais plataformas, se pode utilizar bases de dados como NVD e Exploit Database, o último sendo um banco de dados open source de vulnerabilidades que funciona como um repositório em conformidade com o padrão CVE de exploits públicos, provas de conceito (PoCs) e softwares vulneráveis para Pentesters e pesquisadores de cyber segurança (Exploit Database, s.d.).

3.2. Limitações técnicas e considerações éticas

No caso da plataforma Censys, a coleta é mais detalhada e inclui informações sobre certificados digitais e protocolos, permitindo uma análise mais completa da infraestrutura exposta. Ao mesmo tempo, a possibilidade de identificar automaticamente potenciais vulnerabilidades é mais restrita do que em plataformas como Shodan ou Netlas (Censys, s.d.; Shodan, s.d.; Netlas, 2024).

Para evitar a exposição direta de informações criticas o presente estudo irá remover os nomes e endereços de IP de sistemas, dispositivos e instituições assim

como o nome e rostos de qualquer pessoa que se torne disponível em tais plataformas devido a exposição de portas e serviços.

3.3. Shodan

O Shodan é uma plataforma de busca voltada à identificação de dispositivos e serviços conectados à internet. Em vez de indexar páginas web, ela organiza informações técnicas obtidas de ativos expostos, como portas abertas, banners, protocolos, certificados e versões aparentes de software. Seu funcionamento baseia-se em varreduras automatizadas sobre endereços IP públicos, registrando as respostas fornecidas pelos serviços encontrados e armazenando esses dados em uma base pesquisável por filtros específicos.

Por isso, a plataforma é amplamente utilizada para mapear superfície de ataque, identificar exposições indevidas e levantar indícios de vulnerabilidades visíveis externamente como versões de software e outros, embora sem confirmar, por si só, a exploração real de uma falha e pelo fato de somente interagir de forma passiva coletando informações publicas é considerada uma plataforma e ferramenta ética (Shodan, s.d.).

3.4. Netlas

Netlas é uma plataforma de OSINT voltada à identificação e análise de vetores expostos à internet, com foco em respostas de serviços, certificados, DNS, WHOIS e outros dados técnicos úteis para reconhecimento externo e análise de superfície de ataque. Em vez de indexar páginas web, a plataforma organiza informações coletadas de serviços acessíveis publicamente e disponibiliza esses dados por mecanismos de busca e filtros específicos.

Seu funcionamento é baseado na coleta automatizada de respostas obtidas a partir de hosts conectados à internet, permitindo ao usuário pesquisar esses registros por meio do Responses Search Tool. Além da busca pública, o Netlas também oferece recursos próprios para descoberta de superfície de ataque e varredura direcionada, como o Attack Surface Discovery Tool e o Private Scanner, este último voltado à obtenção de dados atualizados sobre alvos definidos pelo usuário (Netlas, 2024).

No contexto deste trabalho o Netlas desempenha o mesmo trabalho que o Shodan, algumas diferenças pequenas existem em relação a detecção de vulnerabilidades, porém ainda assim mantém a ética que as demais plataformas utilizadas, somente interagindo de forma passiva para coletar informações públicas.

3.5. Censys

Censys é uma plataforma de inteligência de internet voltada à descoberta, ao monitoramento e à análise de vetores acessíveis publicamente, como hosts, serviços, certificados e propriedades web. Em vez de indexar páginas como um buscador tradicional, a plataforma organiza dados técnicos obtidos por varreduras contínuas da internet, permitindo identificar exposições externas, relações entre ativos e mudanças na infraestrutura ao longo do tempo.

Segundo a própria empresa, são realizadas pequenas tentativas de conexão a endereços de IP públicos e, quando serviços ativos são encontrados, se completa handshakes de protocolo para coletar apenas informações visíveis publicamente, sem explorar vulnerabilidades nem contornar barreiras técnicas. Além disso, sua documentação destaca que a plataforma mantém conjuntos de dados sobre hosts, certificados e web properties, o que a torna especialmente útil para análise de superfície de ataque externa, investigação de ameaças e acompanhamento histórico de vetores expostos.

Apesar de coletar dados de forma mais detalhada sobre os alvos, a plataforma Censys também segue práticas éticas e é visto como uma plataforma mais avançada e detalhada que as demais, utilizada para pesquisas mais detalhadas e provendo serviços específicos para gerenciamento de superfície de ataque entre outros.

3.6. National Vulnerability Database (NVD)

O NVD (National Vulnerability Database) é o repositório oficial do governo dos Estados Unidos voltado à padronização e disponibilização de dados de gerenciamento de vulnerabilidades. Mantido pelo National Institute of Standards and Technology (NIST), o NVD reúne informações estruturadas sobre falhas de segurança, identificadores de produtos, métricas de impacto e referências técnicas, com o objetivo

de apoiar automação em gestão de vulnerabilidades, medição de segurança e conformidade.

De acordo com o próprio NIST, a base é composta por dados padronizados segundo o SCAP (Security Content Automation Protocol) e inclui registros de falhas de software, nomes de produtos, métricas de severidade e referências relacionadas à segurança. No contexto deste trabalho, o NVD é relevante por permitir o cruzamento entre serviços, versões de software e vulnerabilidades publicamente catalogadas, servindo como apoio para análise técnica e contextualização dos riscos identificados (NVD, s.d.).

3.7. Exploit Database

O Exploit Database (Exploit-DB) é um banco de dados público de exploits, proofs of concept (PoCs) e softwares vulneráveis, mantido pela empresa OffSec como um projeto sem fins lucrativos de utilidade pública. De acordo com a própria plataforma, o objetivo é que a plataforma se comporte um arquivo compatível com o padrão CVE, desenvolvido para atender pesquisadores de vulnerabilidades e profissionais de cyber segurança, focado em disponibilizar material técnico acionável em vez de simples descrições.

No contexto deste trabalho, o Exploit-DB permite complementar a análise de vulnerabilidades com exemplos públicos de exploração associados a falhas já conhecidas, ajudando a contextualizar o risco prático de determinados serviços ou versões de software expostos.

Além do repositório principal de exploits, a plataforma também mantém bases auxiliares, como a Google Hacking Database (GHDB), voltada ao catálogo de consultas que podem revelar informações sensíveis indexadas publicamente por mecanismos de busca. Isso amplia seu uso em atividades de pesquisa e reconhecimento técnico, especialmente quando o objetivo é relacionar uma vulnerabilidade conhecida com formas públicas de exploração ou evidências práticas de exposição.

Em relação a ética, a plataforma possui regras claras de uso e submissão para garantir que não haja incentivo direto de ataques e que também não utilizará dados proveniente de ações ilegais (Exploit Database, s.d.):

- Testes autorizados: utilize os exploits (PoCs) fornecidos apenas para testes de penetração ou verificação de vulnerabilidades em ambientes controlados e autorizados.
- Divulgação responsável: o banco de dados apoia a pesquisa responsável em segurança, documentando vulnerabilidades sem incentivar ataques.
- Proibição de ataques a sistemas ativos: envios que tenham como alvo sites ativos ou sistemas sem consentimento são rejeitados para evitar o uso indevido.
- Foco defensivo: o objetivo principal é ajudar os administradores de sistemas a avaliar riscos e corrigir vulnerabilidades de forma eficaz.

3.8. Metodologia de coleta e análise

A metodologia adotada neste trabalho se baseia em uma abordagem descritiva e quantitativa com foco na observação passiva de vetores publicamente acessíveis no Brasil.

Com este objetivo, foram utilizadas plataformas de OSINT especializadas em exposição de vetores na internet, com o objetivo de identificar serviços, protocolos, portas, banners, versões aparentes de software e outros metadados técnicos visíveis publicamente. Com estas informações, os registros obtidos foram organizados e consolidados em uma base única, permitindo a padronização de análises posteriores.

3.8.1. Delimitação do objeto de estudo

O objeto de estudo da presente pesquisa consiste na analise da exposição de serviços, dispositivos e aplicações publicamente acessíveis pela internet no Brasil, focando em ativos que aparentam utilizar configurações inseguras, falhas de autenticação, softwares potencialmente desatualizados ou associação com vulnerabilidades conhecidas.

A análise foi feita utilizando dados técnicos, visíveis externamente de modo passivo, como portas abertas, protocolos, banners, certificados digitais, versões aparentes de software, páginas de login expostas e outros metadados.

Não fazem parte do escopo deste trabalho a exploração ativa de vulnerabilidades, testes invasivos ou qualquer atividade que envolva ou possa

requerer acesso não autorizado ou a tentativa de acesso aos sistemas observados, restringindo o estudo à coleta e interpretação de dados públicos obtidos de forma ética.

3.8.2. Fontes de dados utilizadas

As fontes utilizadas neste trabalho são em sua maioria, plataformas de OSINT voltadas à identificação de ativos expostos na internet também incluindo bases públicas de vulnerabilidades.

Para a coleta de informações sobre serviços, portas, protocolos, banners, certificados e versões aparentes de software, serão utilizadas as plataformas Shodan, Censys e Netlas. Tais plataformas permitem observar, por meio de dados publicamente acessíveis, a presença de serviços expostos no Brasil e suas principais características técnicas para uma melhor analise quantitativa e comparativa.

Também serão utilizadas bases de dados como o National Vulnerability Database (NVD) e Exploit Database juntamente com o padrão CVE. Essas fontes são bancos de dados públicos de vulnerabilidades, permitindo a verificação da existência de vulnerabilidades e a gradação de severidade de tais vulnerabilidades caso existam utilizando os dados das plataformas de OSINT caso as mesmas não identifiquem vulnerabilidades diretamente.

Também será utilizada o ranking OWASP Top 10 de 2025 como referência teórica para relacionar determinados achados com categorias conhecidas de vulnerabilidades, como falhas de configuração, falhas de autenticação, problemas criptográficos e uso de componentes vulneráveis, mas sobretudo serve como referencia principal dos maiores problemas relacionados a segurança cibernética de forma atualizada.

Desta forma as fontes utilizadas cumprem funções complementares: Shodan, Censys e Netlas fornecem os dados de exposição, enquanto NVD, CVE, Exploit Database e OWASP auxiliam na interpretação técnica e na classificação dos riscos.

3.8.3. Considerações éticas

A pesquisa será conduzida exclusivamente com dados publicamente acessíveis, obtidos através de plataformas de OSINT e bases de dados publicas de vulnerabilidades. Não serão realizados testes invasivos, exploração de vulnerabilidades, tentativas de autenticação, força bruta ou qualquer forma de interação não autorizada com os sistemas identificados.

Para reduzir quaisquer riscos de exposição indevida de forma direta ou acidental, endereços IP, nomes de instituições, nomes de usuários, rostos, domínios e demais informações sensíveis e identificáveis serão anonimizados nos dados e exemplos utilizados. A análise será apresentada com finalidade acadêmica e para fins defensivos, respeitando os termos de uso das plataformas e o uso responsável dos dados.

4. DESENVOLVIMENTO DA PESQUISA

Após a apresentação dos fundamentos teóricos e dos procedimentos metodológicos adotados neste trabalho, este capítulo apresenta o desenvolvimento da pesquisa realizada sobre a exposição de ativos digitais no Brasil. A análise concentra-se na observação de serviços publicamente acessíveis pela internet, buscando identificar padrões de exposição, tecnologias utilizadas, protocolos em funcionamento e possíveis indícios de vulnerabilidades associadas a configurações inadequadas ou versões de software potencialmente desatualizadas.

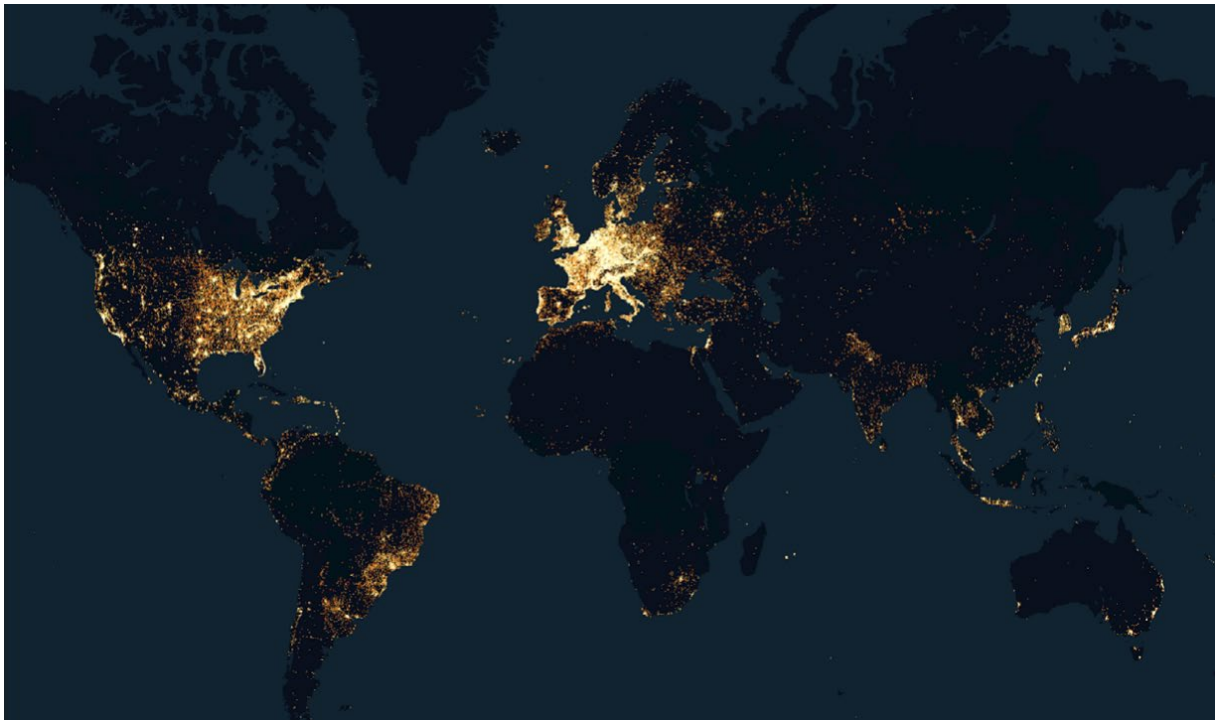
Para isso, foram utilizados dados obtidos por meio de plataformas de OSINT voltadas ao mapeamento da superfície de ataque externa, como Shodan, Censys e Netlas. A partir dessas fontes, são analisados diferentes tipos de serviços expostos, com atenção especial a protocolos amplamente utilizados ou historicamente associados a riscos de segurança, como HTTP, SMB, FTP, Telnet e SSH. Também são considerados ativos de maior criticidade, dispositivos IoT e interfaces de login acessíveis publicamente, uma vez que tais elementos podem representar pontos relevantes de entrada para agentes mal-intencionados quando não são devidamente protegidos.

Dessa forma, o capítulo busca transformar os dados coletados em uma visão organizada e interpretativa do cenário brasileiro de exposição digital. A intenção não é realizar testes invasivos ou confirmar a exploração de vulnerabilidades, mas observar, de maneira ética e não intrusiva, sinais públicos que possam indicar riscos à segurança da informação. Assim, as análises apresentadas contribuem para compreender a dimensão da superfície de ataque existente no país e reforçam a importância de práticas adequadas de configuração, atualização, monitoramento e gestão de ativos conectados à internet.

4.1. Exposição Geral

De acordo com o relatório “The 2023 State of the Internet Report”, aproximadamente 88% dos sites e serviços na internet utilizam HTTP, e dentre aqueles que utilizam HTTP, 60% não utilizam HTTP com criptografia (Censys, 2023). O mapa de tal distribuição pode ser observado na figura 13 abaixo.

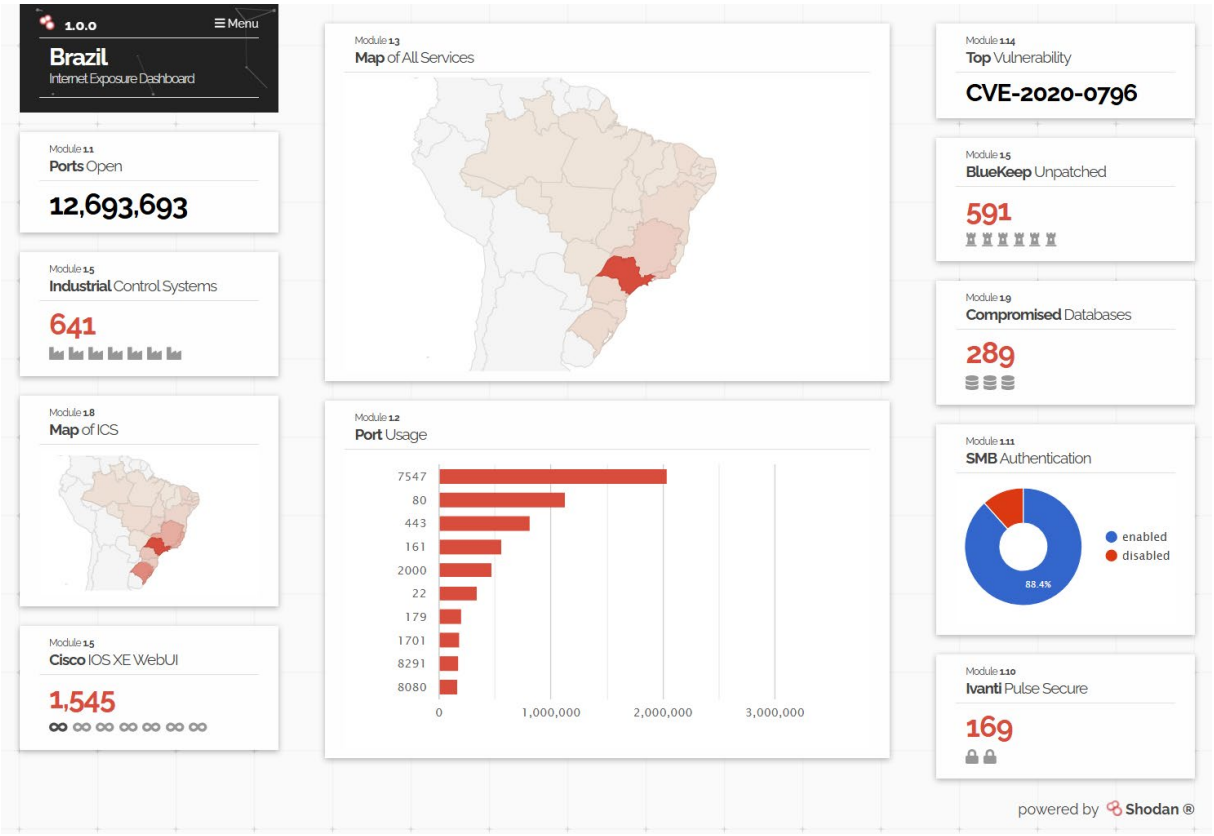
Figura 13. Censys - Mapa de Hosts que utilizam HTTP no mundo



Fonte: The 2023 State of The Internet Report

Segundo a plataforma Shodan (figura 14), existem 12,693,693 ativos expostos no Brasil. Também existem 289 bancos de dados comprometidos e cerca de 11.6% dos serviços de SMB não utilizam nenhum tipo de autenticação.

Figura 14. Shodan - Dashboard de Exposição da Internet no Brasil



Fonte: Shodan Internet Exposure Dashboard - Brazil

Em contrapartida, as plataformas Censys e Netlas (figura 15) acusam um numero mais baixo provavelmente devido a utilizarem filtros diferentes, sendo o total de ativos expostos detectados pela plataforma Censys 8,273,724 e o total detectado pela plataforma Netlas 6,695,507.

Figura 15. Ativos expostos no Brasil utilizando Netlas e Censys

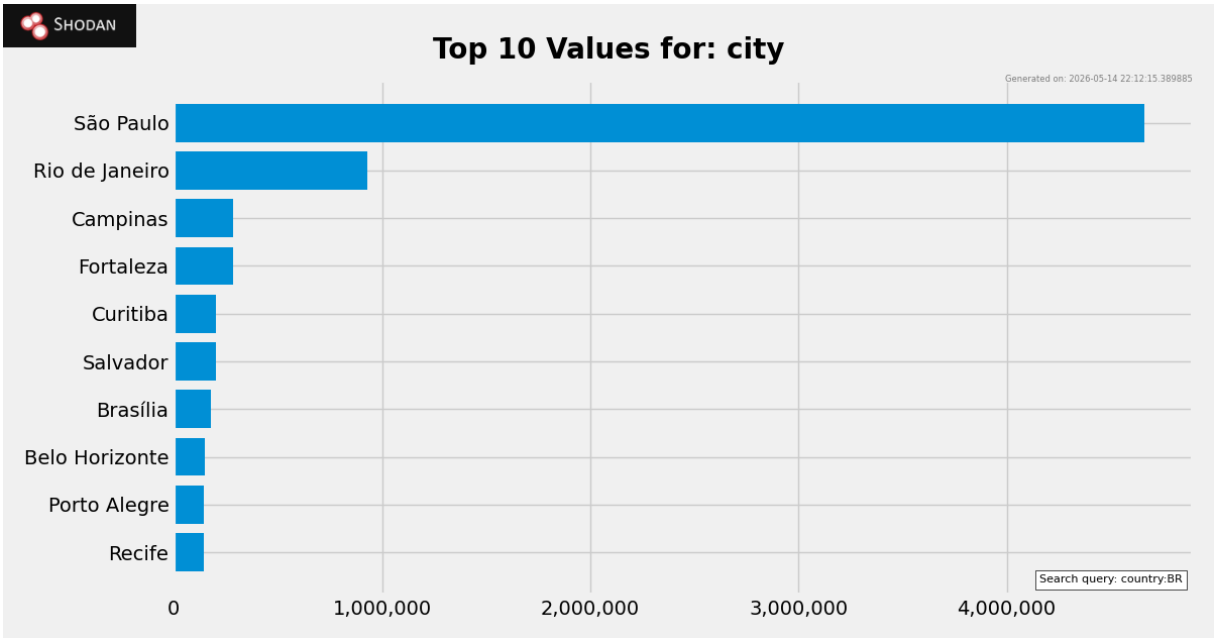
Fonte: Autoria Própria

A variação de resultados se dá pela diferença de objetivos e alvos das plataformas:

- Shodan foca na detecção rápida de dispositivos e serviços expostos, tendo como alvos principais a varredura de dispositivos IoT, servidores, roteadores e versões específicas de software.
- Censys tem como seu principal objetivo realizar uma análise aprofundada, de nível de pesquisa e precisa da infraestrutura de rede e dos certificados, com alvo principal nas configurações dos hosts, em todas as portas e nas cadeias de certificados TLS/SSL.
- Netlas tem como principal objetivo o reconhecimento focado em domínios e monitoramento da superfície de ataque, e tem como alvos principais domínios, subdomínios, registros DNS e hosts virtuais como alvos principais.

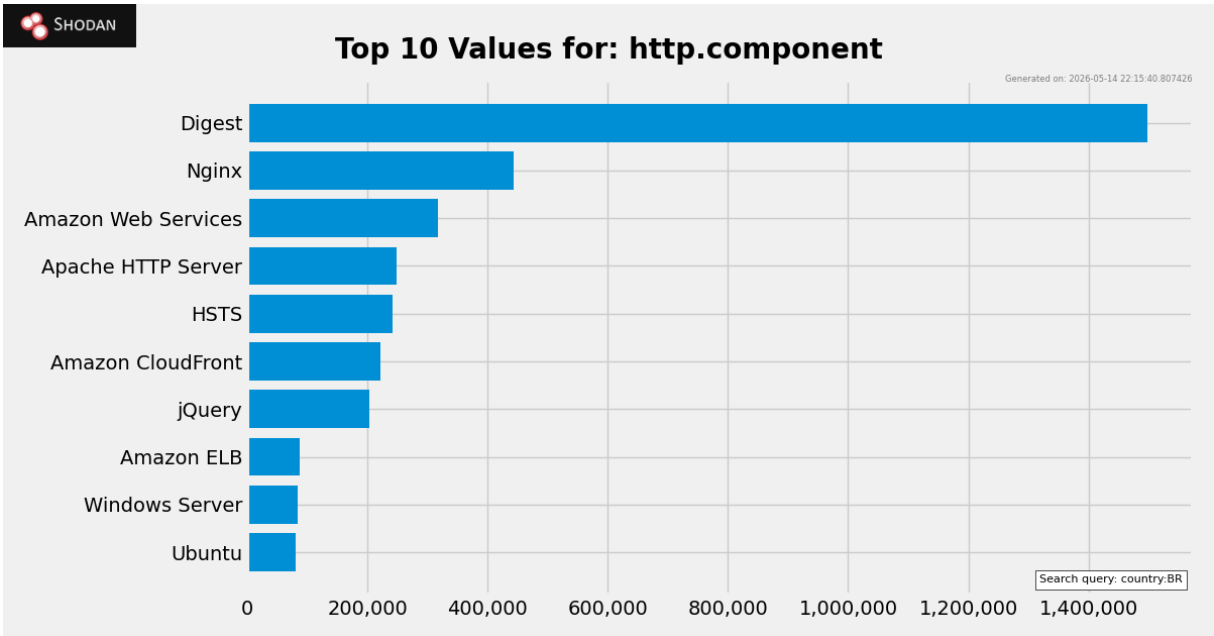
Utilizando a plataforma Shodan (figura 16, 17 e 18), é possível observar as principais cidades, tecnologias, e produtos (softwares) usados pelos hosts com ativos expostos no Brasil:

Figura 16. Shodan - Total de ativos expostos no Brasil por cidade



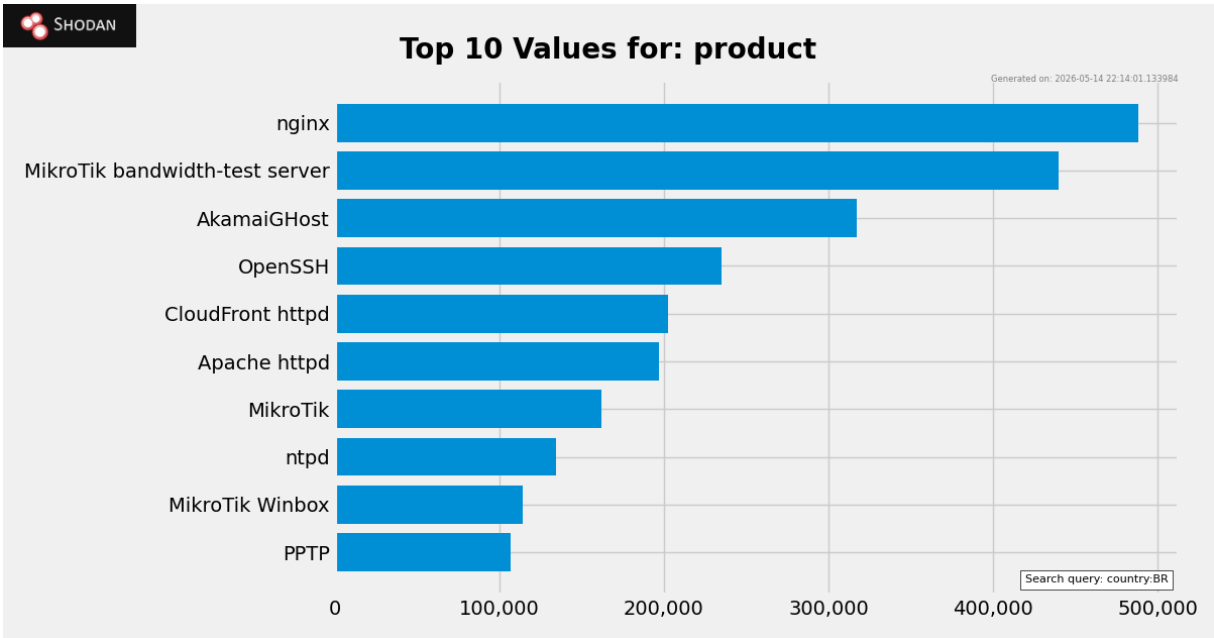
Fonte: Shodan facets

Figura 17. Shodan - Tecnologias web utilizadas por hosts com ativos expostos



Fonte: Shodan facets

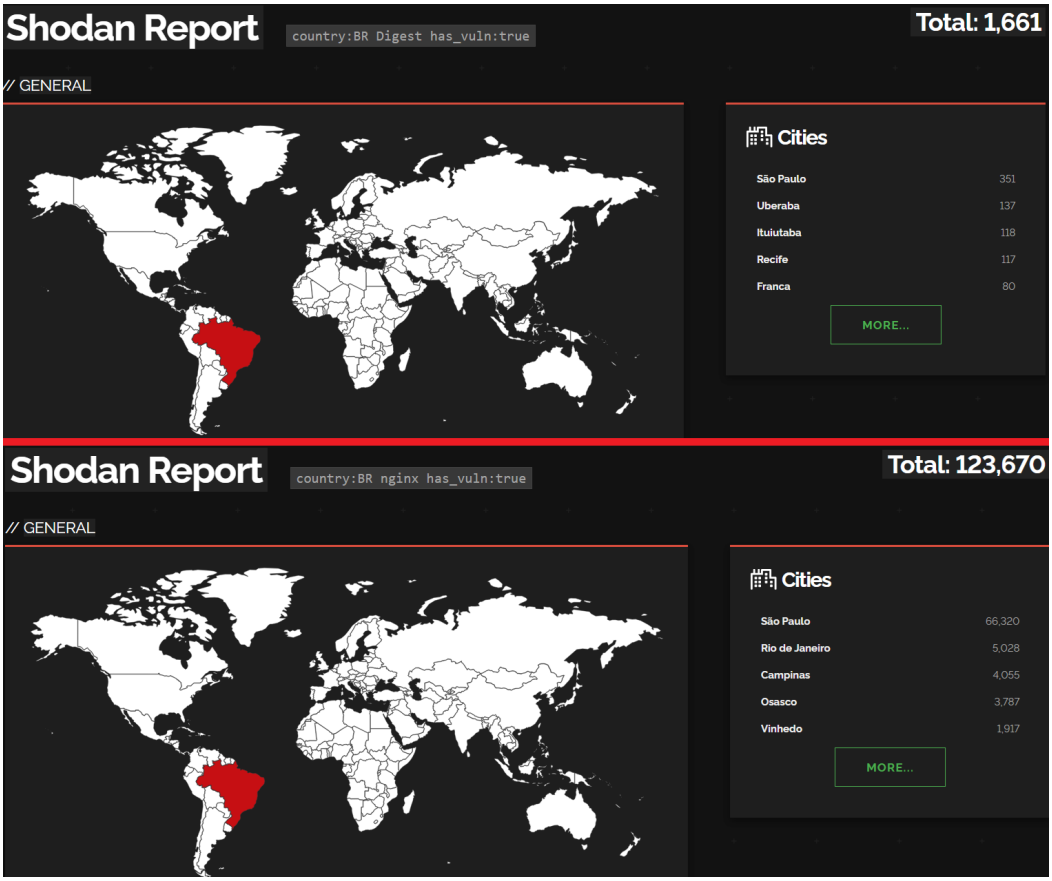
Figura 18. Shodan - Produtos mais utilizados por hosts com ativos expostos



Fonte: Shodan facets

A plataforma Shodan (figura 19) identificou que as tecnologias Digest e Nginx são as mais expostas no Brasil, como ilustrado na imagem 19 a baixo, embora as duas tecnologias sejam amplamente utilizadas e tenham um nível de exposição elevado, Digest surpreendentemente possui poucas vulnerabilidades, com um total de 1,615,950 hosts expostos e somente 1,661 (0.1%) hosts com indícios de vulnerabilidades, enquanto Nginx tem um total de 498,454 resultados e destes, 123,674 (25%) possuem indícios de vulnerabilidades.

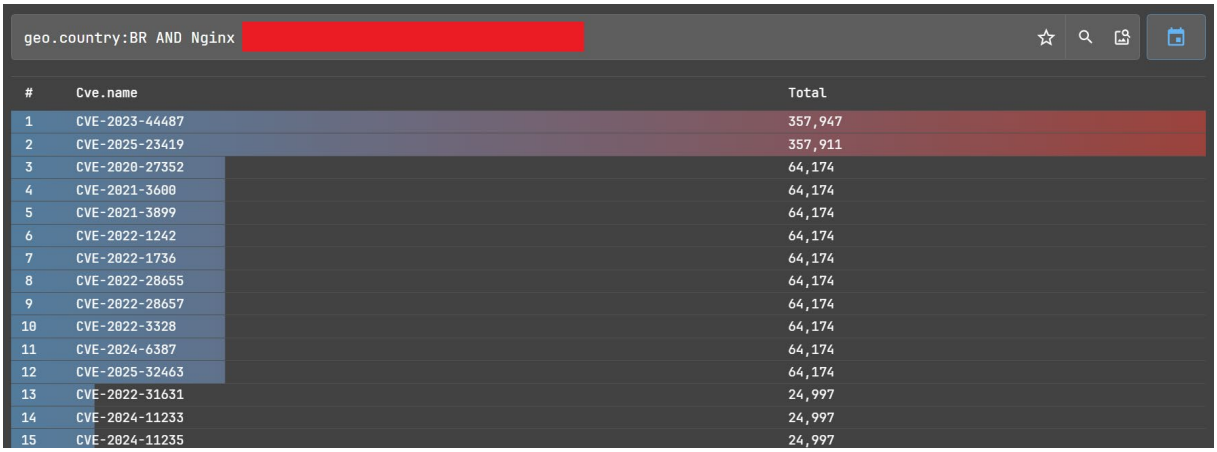
Figura 19. Shodan - Vulnerabilidades em hosts utilizando Digest e Nginx



Fonte: Autoria própria

Utilizando a plataforma Netlas (figura 20) confirmamos que existe uma percentagem grande de hosts que utilizam Nginx com vulnerabilidades, do total de 543,389 hosts identificados, destes, 431,684 (79.5%) possuem vulnerabilidades.

Figura 20. Netlas - Hosts utilizando Nginx com vulnerabilidades



#	Cve.name	Total
1	CVE-2023-44487	357,947
2	CVE-2025-23419	357,911
3	CVE-2020-27352	64,174
4	CVE-2021-3600	64,174
5	CVE-2021-3899	64,174
6	CVE-2022-1242	64,174
7	CVE-2022-1736	64,174
8	CVE-2022-28655	64,174
9	CVE-2022-28657	64,174
10	CVE-2022-3328	64,174
11	CVE-2024-6387	64,174
12	CVE-2025-32463	64,174
13	CVE-2022-31631	24,997
14	CVE-2024-11233	24,997
15	CVE-2024-11235	24,997

Fonte: Netlas

4.2. Exposição no Brasil

A partir da análise geral da superfície de exposição, esta seção direciona o estudo para o contexto brasileiro, observando serviços e protocolos acessíveis publicamente a partir de dados obtidos em plataformas de monitoramento passivo. A investigação busca identificar padrões de exposição, tecnologias predominantes, possíveis configurações inseguras e indícios de vulnerabilidades associadas aos ativos localizados no Brasil. Para organizar essa análise, os serviços foram separados por categorias e protocolos, iniciando-se pelos hosts que utilizam HTTP, devido à ampla adoção desse protocolo em aplicações web e ao risco que sua exposição pode representar quando não acompanhada de mecanismos adequados de segurança, como criptografia, atualização de servidores e controle de acesso.

4.2.1. Exposição de hosts utilizando HTTP

Como mencionado anteriormente, segundo a plataforma Shodan (figura 21), o total de ativos expostos é de 12,693,693, sendo que 6,508,192 se original em hosts utilizando HTTP, que correspondem a pouco mais de 51% do total de ativos expostos.

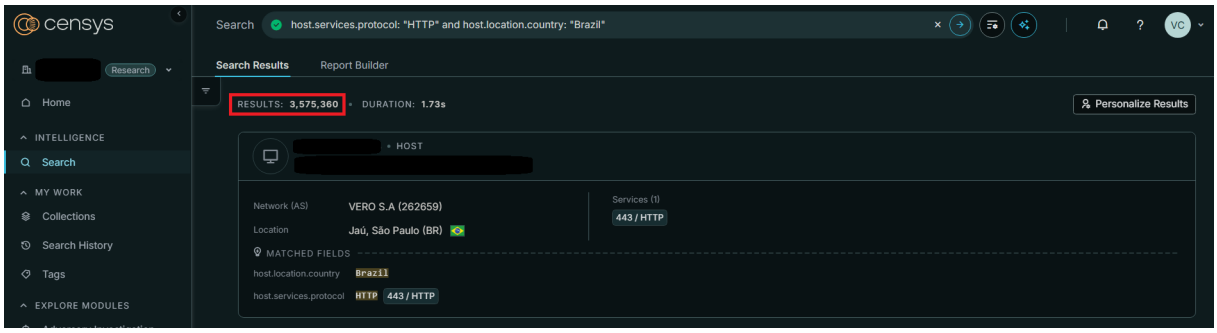
Figura 21. Shodan - Hosts utilizando HTTP no Brasil

Fonte: Autoria própria

Da mesma forma, dos 8,273,724 de ativos expostos no Brasil detectados pela plataforma Censys (figura 22), 3,576,905 tem origem em hosts utilizando HTTP, que corresponde a pouco mais de 43% dos ativos detectados, enquanto na plataforma Netlas (figura 23), dos 6,695,507 ativos detectados, somente 1,831,059 tem origem

em hosts utilizando HTTP, que corresponde a pouco mais de 27% dos resultados detectados inicialmente pela plataforma.

Figura 22. Censys - Hosts utilizando HTTP no Brasil



Fonte: Autoria própria

Figura 23. Netlas - Hosts utilizando HTTP no Brasil

Fonte: Autoria própria

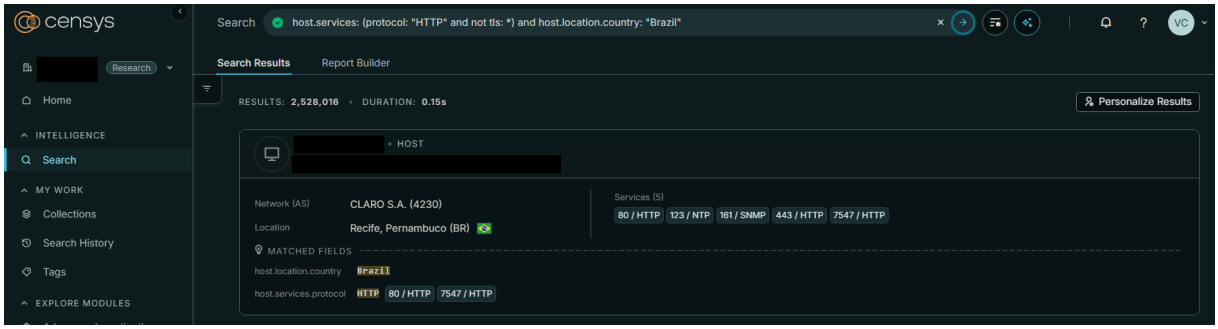
Utilizando Shodan (figura 24), conseguimos aferir que dentre os hosts utilizando HTTP, um total de 5,512,987 não usa criptografia por meio de SSL (Secure Sockets Layer) ou TLS (Transport Layer Security), representando cerca de 87% dos hosts que utilizam HTTP encontrados no brasil pela plataforma.

Figura 24. Shodan - Hosts utilizando HTTP sem SSL ou TLS no Brasil

Fonte: Autoria própria

Na plataforma Censys (figura 25), o total de hosts no brasil que não utilizam SSL ou TLS é de 2,528,016, que corresponde a quase 71% dos ativos de hosts que utilizam HTTP detectados no Brasil pela plataforma.

Figura 25. Censys - Hosts utilizando HTTP sem SSL ou TLS no Brasil



Fonte: Autoria própria

A quantidade de hosts no Brasil utilizando HTTP sem a adoção de SSL ou TLS representa um risco consideravel, e indica que parte significativa dos sistemas publicamente acessíveis transmitem dados sem nenhuma proteção criptográfica. O SSL (atualmente obsoleto), e seu sucessor TLS são protocolos criados para proteger a comunicação entre cliente e servidor através do uso de criptografia, implementando os princípios de confidencialidade, integridade e autenticação da conexão e impedindo o acesso ou alteração dos dados por usuários não autorizados.

Os resultados obtidos indicam uma superfície de exposição e de ataque muito grande. No Shodan os hosts HTTP sem SSL/TLS representam cerca de 87% dos hosts HTTP identificados e pouco mais de 43% do total de ativos expostos no Brasil.

Na Censys, os hosts HTTP sem SSL/TLS correspondem a quase 71% dos hosts HTTP e aproximadamente 39,8% do total de ativos detectados no Brasil. Embora a variação de resultados seja devido a diferenças na coleta de dados de cada plataforma, eles demonstram que uma parcela grande de serviços web publicamente acessíveis no Brasil opera sem quaisquer mecanismos básicos de proteção de dados ou trafego. Isso demonstra o alto risco de ataques como interceptação de dados, sequestro de sessão, exposição de credenciais e ataques do tipo man-in-the-middle, especialmente em redes não confiáveis ou publicas.

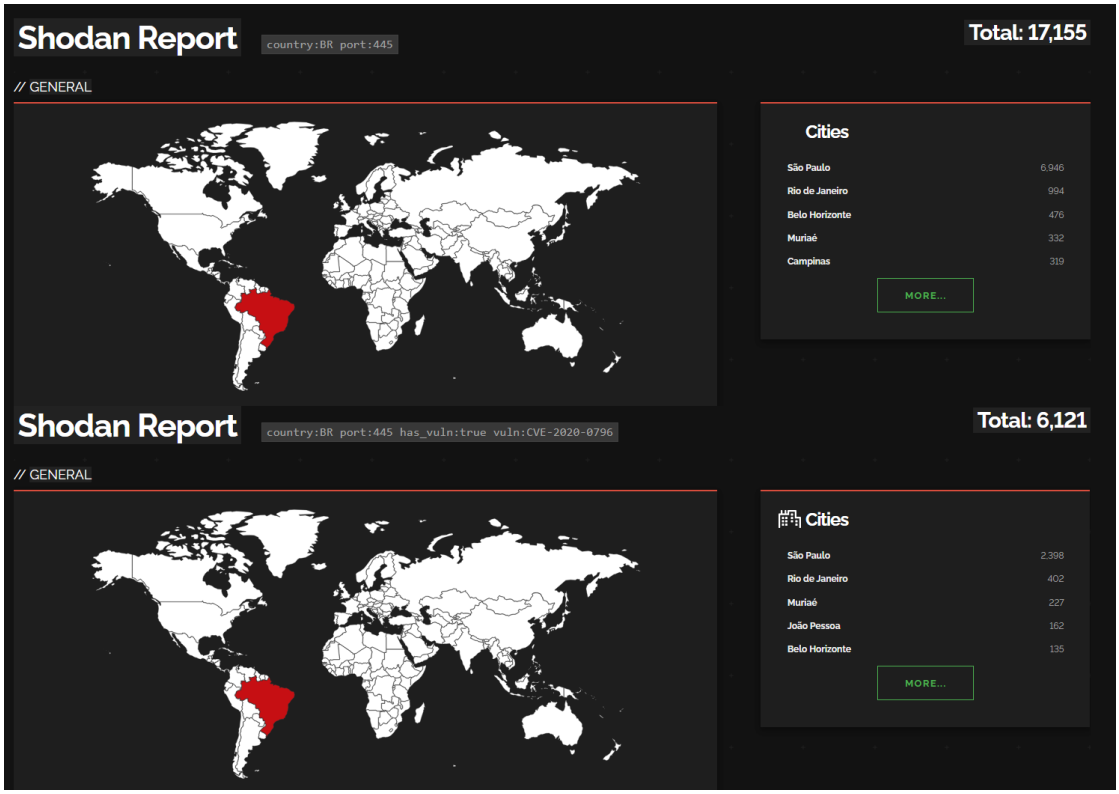
4.2.2. Exposição de hosts utilizando SMB no Brasil

O protocolo SMB (Server Message Block) tem como finalidade o compartilhamento de arquivos entre computadores em uma rede local, permitindo também o acesso a impressoras, diretórios e outros recursos disponibilizados por servidores ou outros computadores presentes na rede. É muito utilizado em ambientes corporativos para facilitar o acesso de usuários autorizados a arquivos internos de forma centralizada.

Utilizando Shodan, um total de 17,155 hosts utilizando SMB foi encontrado, destes, cerca de 1,664 hosts não possuem nenhum tipo de autenticação, possibilitando que qualquer usuario consiga acessar os recursos internos da rede a qualquer momento. Segundo o Shodan Internet Exposure Dashboard, cerca de 11.6% dos hosts utilizando SMB no Brasil não utilizam autenticação.

Escaneando por vulnerabilidades, a plataforma Shodan (figura 26) identificou indícios de que 6,624 hosts utilizando SMB podem possuir vulnerabilidades, destes, 6,121 hosts utilizam uma versão do protocolo SMB associada com a vulnerabilidade SMBGhost (CVE-2020-0796), identificada em 2020, que possibilita a execução remota de código arbitrariamente dentro da maquina alvo, tendo uma nota de severidade CVSS de 10.0 (NVD, 2020).

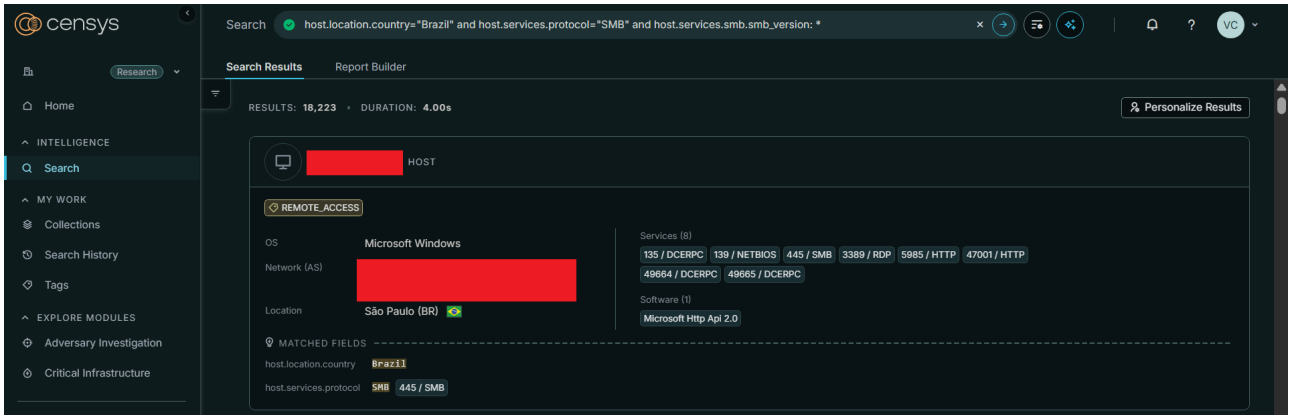
Figura 26. Shodan - Total de hosts utilizando SMB no Brasil e com SMBGhost



Fonte: Autoria Própria

Utilizando a plataforma Censys (figura 27), um total de 18,223 hosts utilizando SMB foram detectados no brasil. A analise de vulnerabilidades, e status de autenticação, não é quantificável através da plataforma Censys utilizando a licença de pesquisa, então não será explorada aqui.

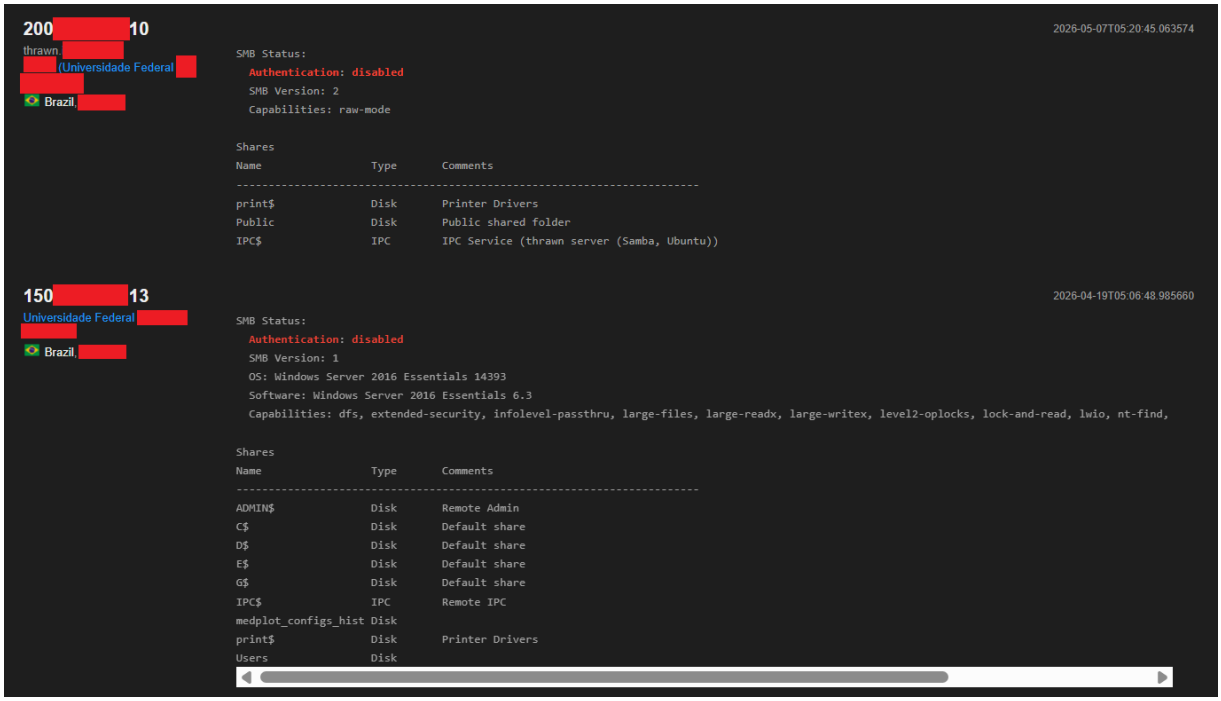
Figura 27. Censys - Hosts utilizando SMB no Brasil



Fonte: Autoria própria

Alguns dos hosts utilizando SMB (figura 28), são instituições como Universidades, empresas e outras entidades que expõem seus dados e sistemas a riscos reais de ataques. Sejam estes dados sensíveis, dados de produtos e pesquisas ou o sistema em sí.

Figura 28. Shodan - Universidades utilizando SMB sem autenticação

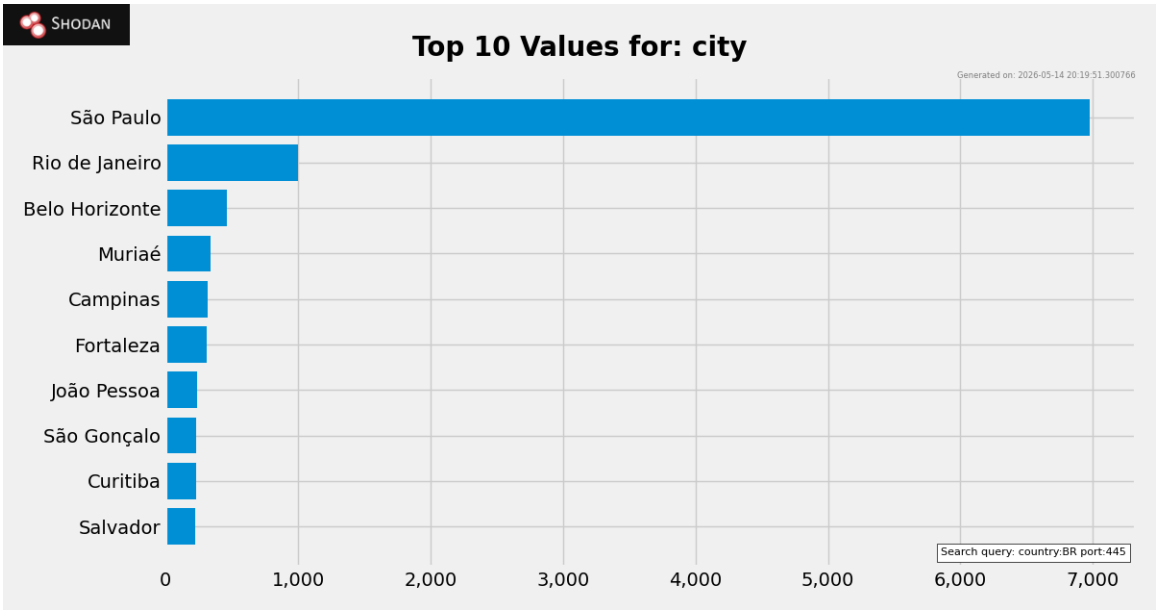


Fonte: Autoria própria

Os riscos de utilizar um protocolo de compartilhamento de arquivos internos sem autenticação é alarmante o suficiente por si só, aliado com a possibilidade de que o mesmo host também possua vulnerabilidades que permitam a um atacante executar código remotamente no host e possivelmente comprometer o sistema inteiro ou rede é algo que merece maior visibilidade uma vez que o total de hosts que podem ter vulnerabilidades representa pouco mais de 38% do total de hosts utilizando SMB no Brasil, é importante ressaltar que a verificação e confirmação de tais vulnerabilidades não pode ser feita de forma ética por requerer interação direta e não autorizada com o host.

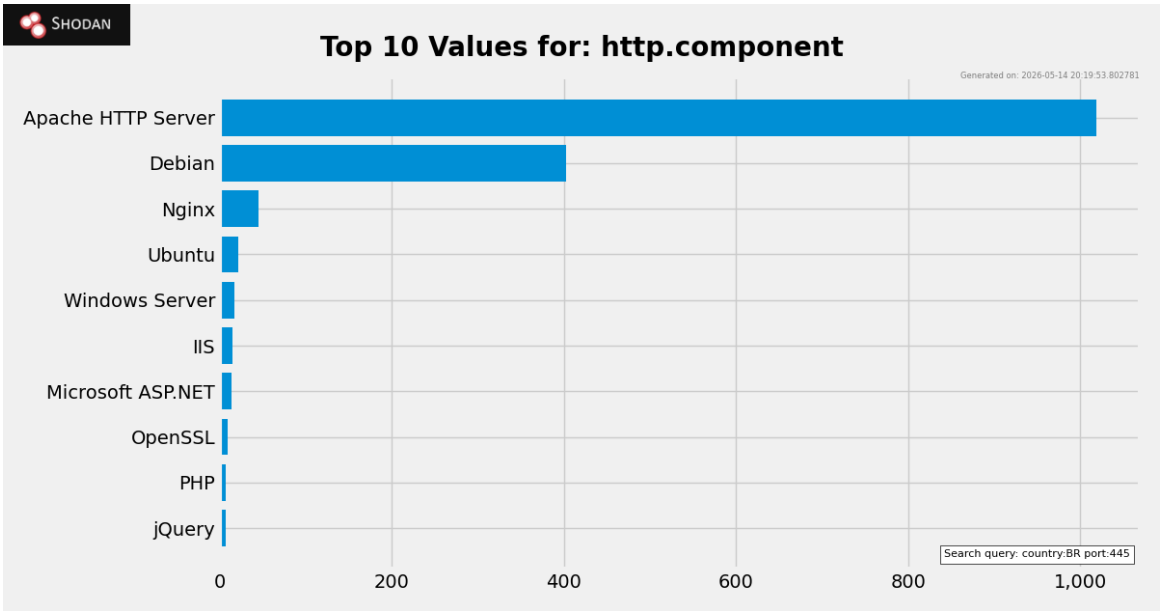
Utilizando Shodan (figuras 29, 30 e 31), é possível observar as principais cidades onde hosts SMB estão localizados, tecnologias web mais utilizadas e produtos (software) mais utilizado por estes hosts.

Figura 29. Shodan - Cidades onde se encontram hosts SMB



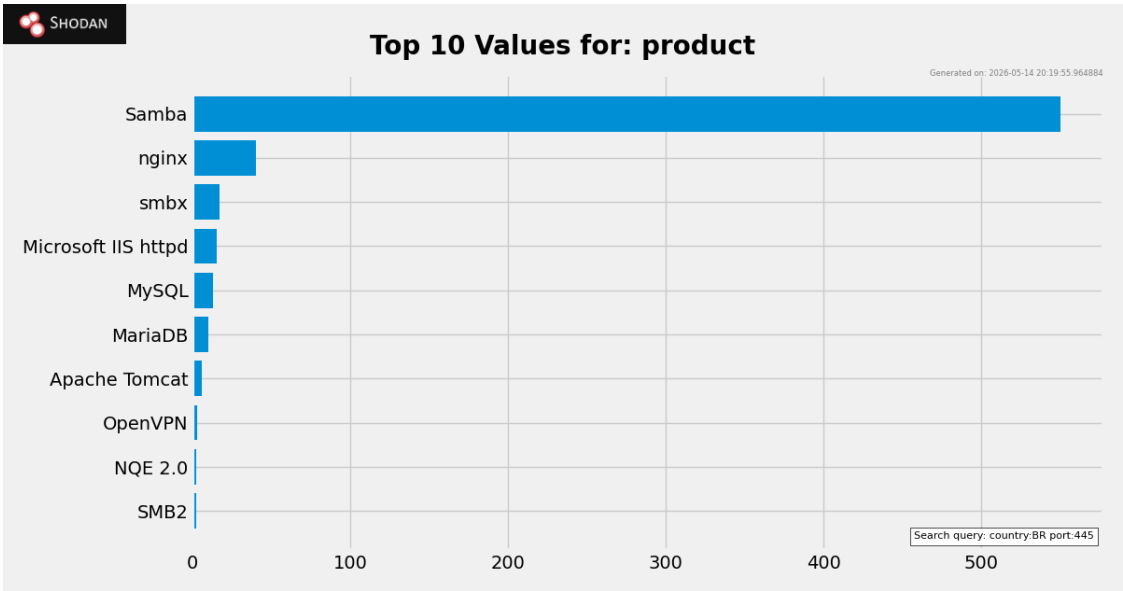
Fonte: Shodan facets

Figura 30. Shodan - Tecnologias web mais utilizadas por hosts SMB



Fonte: Shodan facets

Figura 31. Shodan - Produtos mais utilizados por hosts de SMB



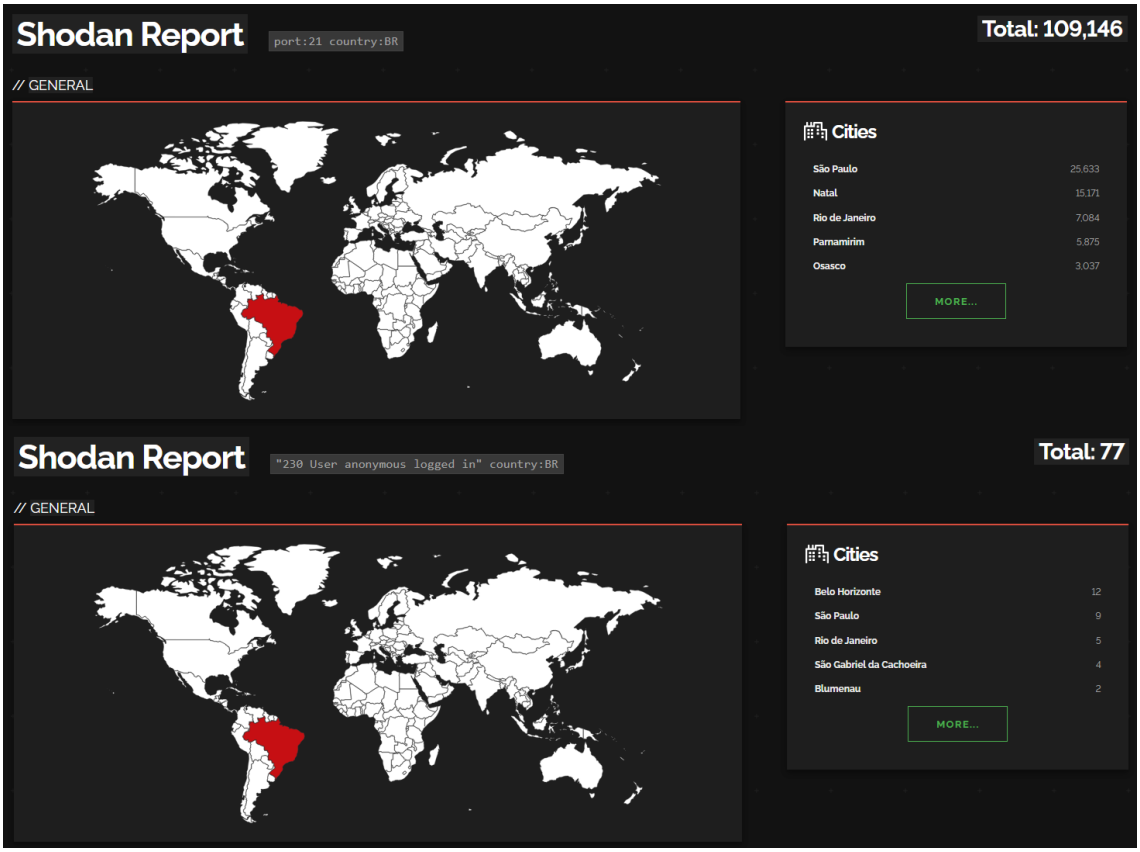
Fonte: Shodan facets

4.2.3. Exposição de hosts utilizando FTP no Brasil

O protocolo FTP (File Transfer Protocol) é utilizado para a transferência de dados entre um cliente e um servidor, seja utilizando a internet ou em uma rede local, permite download e upload de arquivos e utiliza duas portas para a conexão, sendo a porta 21 para controle e a porta 20 para transferência de dados.

Ao utilizar a plataforma Shodan, buscando por hosts que possuem a porta 21 exposta, encontramos 109,146 resultados (figura 32). Uma vez que o protocolo FTP também pode utilizar ou não autenticação, foi feita uma busca pelo código de status 230 que é utilizado quando opções de login anônimo estão habilitadas. Um total de 77 hosts foram identificados (figura 32), em sua maioria Universidades e órgãos governamentais.

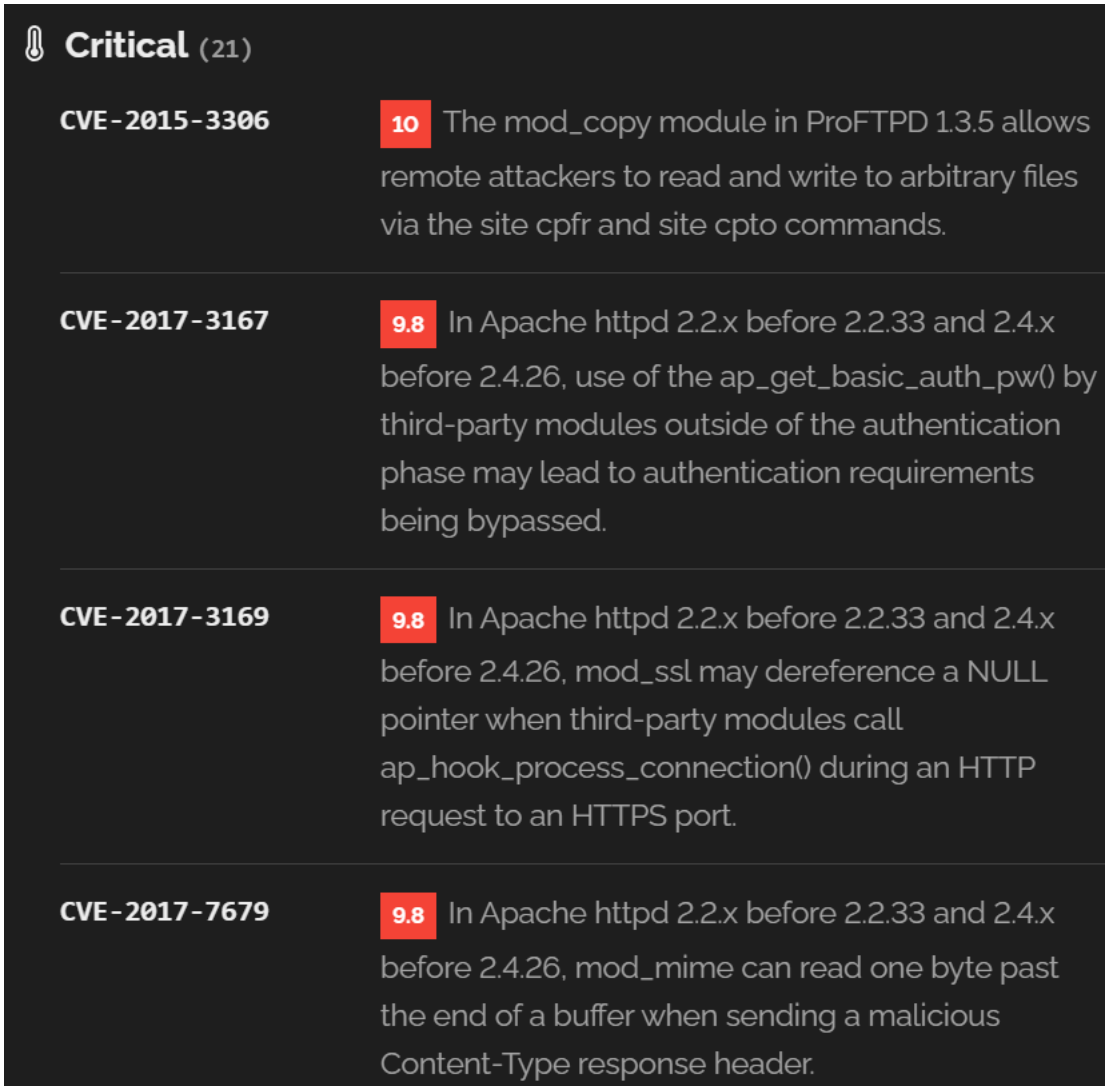
Figura 32. Shodan - Total de hosts utilizando FTP no brasil e login anônimo



Fonte: Autoria própria

Dentre os hosts FTP no Brasil, a plataforma Shodan (figuras 32 e 33) detectou que 943 possuem indícios de vulnerabilidades, a maioria possuindo vulnerabilidades tanto relacionadas com o protocolo FTP tanto com outras tecnologias utilizadas pelo host como vulnerabilidades de tecnologias relacionadas a outros protocolos ou até mesmo ao servidor.

Figura 33. Shodan - Diversas vulnerabilidades encontradas em um host FTP



Fonte: Autoria própria

Utilizando a plataforma Censys (figura 34), que tende a ser mais focado em protocolos, a contagem de hosts utilizando FTP no Brasil sobe para 122,304 resultados, muitos não utilizam as portas padrão (21 e 20). Infelizmente, novamente a busca por certas vulnerabilidades é limitada na plataforma Censys e não foi possível buscar por hosts que permitem login anônimo.

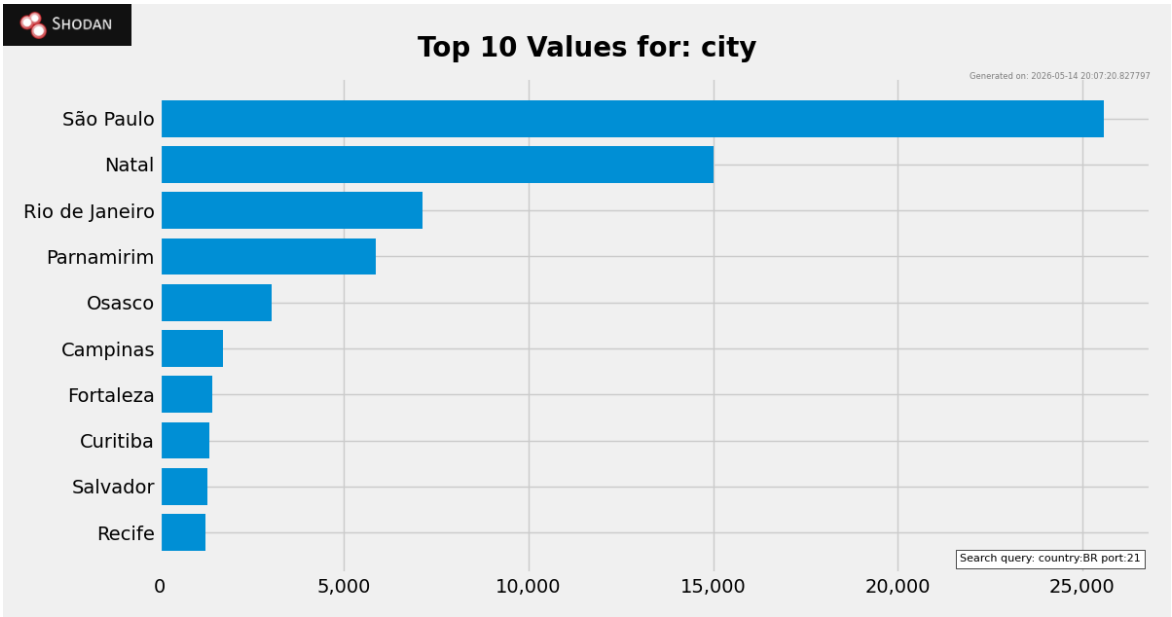
Figura 34. Censys - Hosts utilizando FTP no Brasil

Fonte: Autoria própria

Embora FTP não seja tão expressivo ou tão vulnerável quanto HTTP ou SMB, muitos dos hosts identificados (cerca de 1,427) são de grande importância, envolvendo instituições de pesquisa, universidades e diversos órgãos do governo, tornando a exposição e possível vulnerabilidade dos ativos ainda mais alarmante, seja por vulnerabilidades ou acesso anonimo.

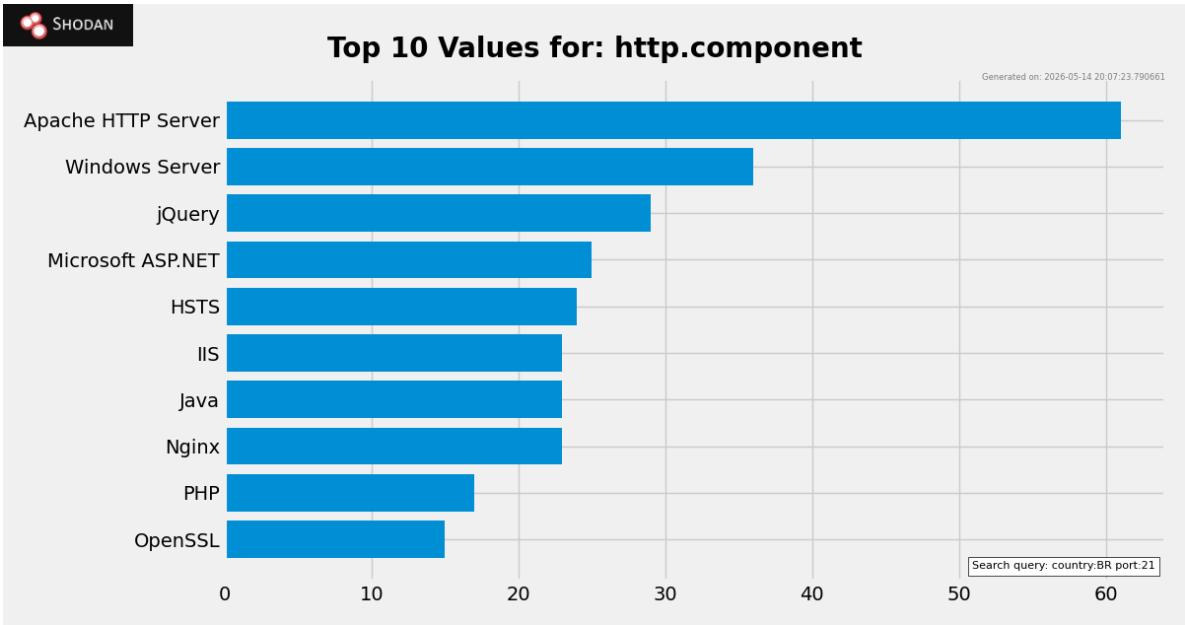
Utilizando a plataforma Shodan (figuras 35, 36, 37), podemos identificar as cidades onde ativos FTP estão mais expostos, as tecnologias utilizadas e produtos (software) sendo utilizados.

Figura 35. Shodan - Hosts utilizando FTP



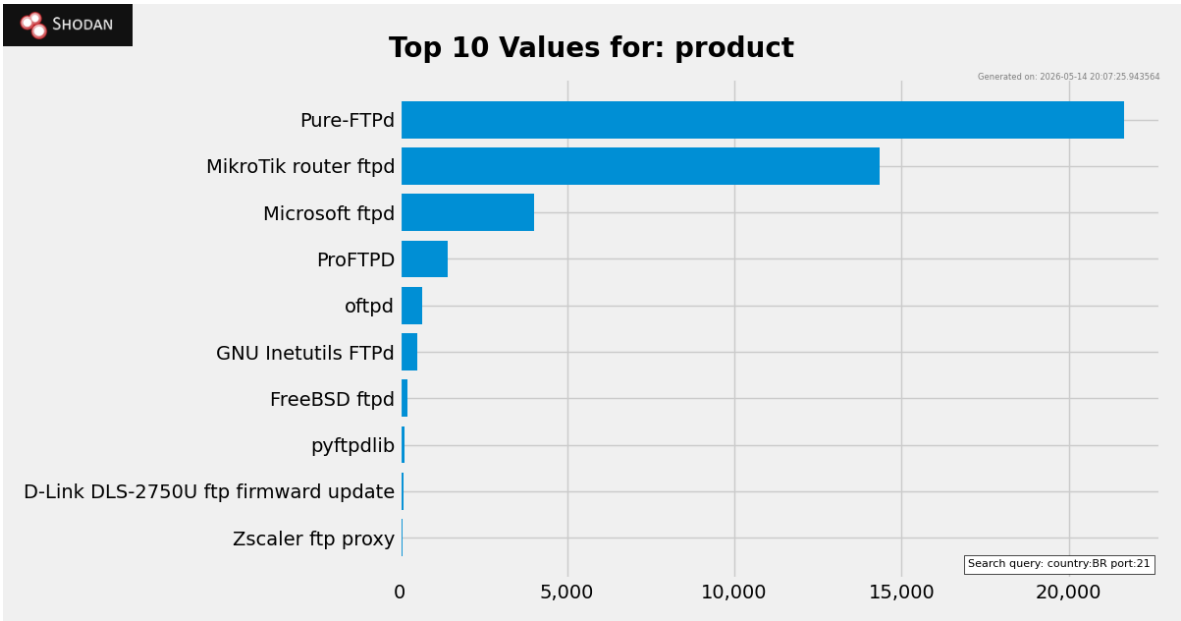
Fonte: Shodan facets

Figura 36. Shodan - Tecnologias web utilizadas por hosts FTP



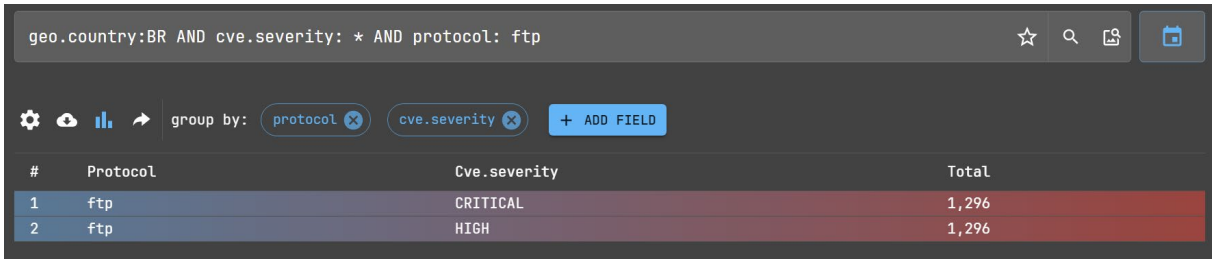
Fonte: Shodan facets

Figura 37. Shodan - Produtos mais utilizados por hosts FTP



Fonte: Shodan facets

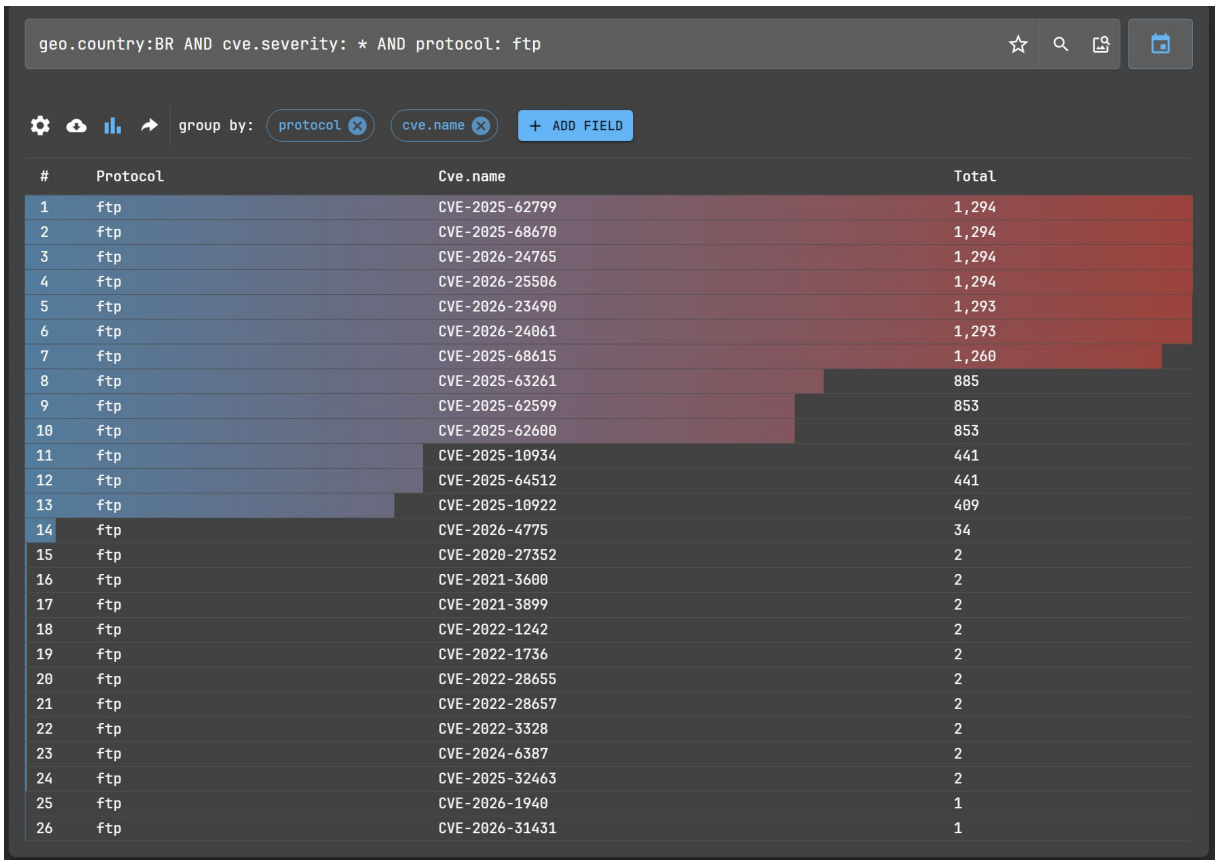
Figura 38. Netlas - Severidade de vulnerabilidades em hosts utilizando FTP



#	Protocol	Cve.severity	Total
1	ftp	CRITICAL	1,296
2	ftp	HIGH	1,296

Fonte: Netlas

Figura 39. Netlas - Vulnerabilidades encontradas em hosts utilizando FTP



#	Protocol	Cve.name	Total
1	ftp	CVE-2025-62799	1,294
2	ftp	CVE-2025-68670	1,294
3	ftp	CVE-2026-24765	1,294
4	ftp	CVE-2026-25506	1,294
5	ftp	CVE-2026-23490	1,293
6	ftp	CVE-2026-24061	1,293
7	ftp	CVE-2025-68615	1,260
8	ftp	CVE-2025-63261	885
9	ftp	CVE-2025-62599	853
10	ftp	CVE-2025-62600	853
11	ftp	CVE-2025-10934	441
12	ftp	CVE-2025-64512	441
13	ftp	CVE-2025-10922	409
14	ftp	CVE-2026-4775	34
15	ftp	CVE-2020-27352	2
16	ftp	CVE-2021-3600	2
17	ftp	CVE-2021-3899	2
18	ftp	CVE-2022-1242	2
19	ftp	CVE-2022-1736	2
20	ftp	CVE-2022-28655	2
21	ftp	CVE-2022-28657	2
22	ftp	CVE-2022-3328	2
23	ftp	CVE-2024-6387	2
24	ftp	CVE-2025-32463	2
25	ftp	CVE-2026-1940	1
26	ftp	CVE-2026-31431	1

Fonte: Netlas

Os dados obtidos através da plataforma Netlas (figuras 38 e 39) demonstram um elevado numero de vulnerabilidades, porém em sua maioria, não são vulnerabilidades associadas com o protocolo mas sim com outras tecnologias ou com os sistemas operacionais do host.

4.2.4. Exposição de hosts utilizando TELNET no Brasil

Telnet é um protocolo de rede cliente-servidor da camada de aplicação que permite o acesso remoto e o controle de dispositivos através de uma interface de linha de comandos. Devido a transmitir dados em texto simples, dados transmitidos através do protocolo correm grande risco de interceptação, levando a sua substituição pelo protocolo SSH (Secure Shell) para uma administração remota mais segura de dispositivos e redes. Por padrão, o protocolo Telnet opera na porta 23.

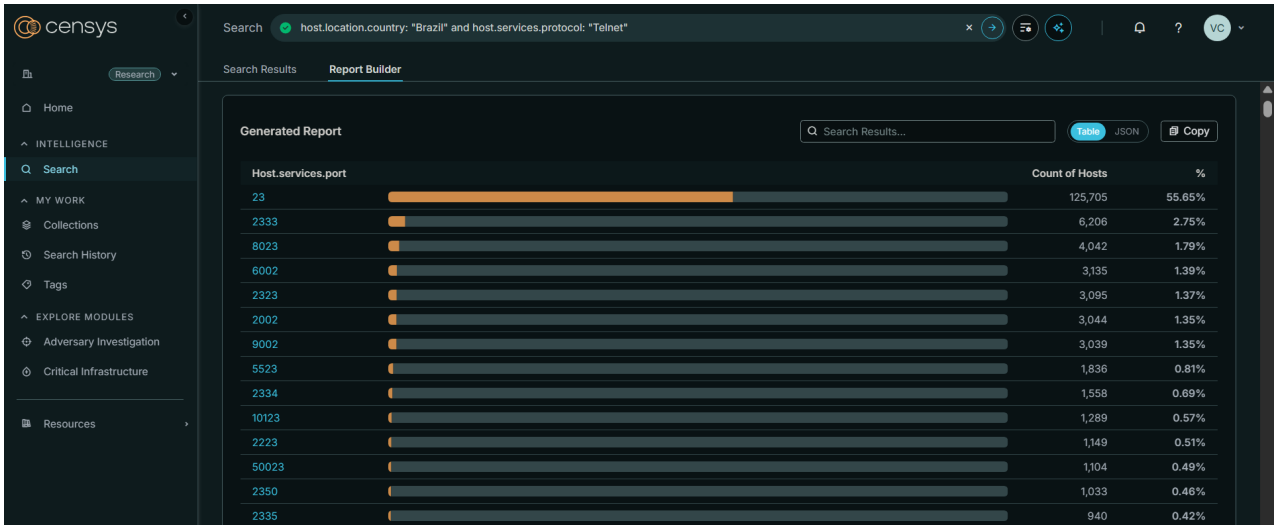
Utilizando a plataforma Shodan (figura 40), é possível identificar um total de 119,970 utilizando Telnet na porta padrão. E 52 destes hosts foram identificados como possivelmente vulneráveis, embora as vulnerabilidades não sejam relacionadas ao protocolo Telnet em sí, logo não serão incluídos neste tópico.

Figura 40. Shodan - Hosts utilizando Telnet no Brasil

Fonte: Autoria própria

Utilizando a plataforma Censys (figura 41), 192,570 hosts foram identificados, principalmente devido ao fato de que a plataforma Censys busca o protocolo independente da porta sendo utilizada.

Figura 41. Censys - Hosts utilizando Telnet no Brasil, portas utilizadas

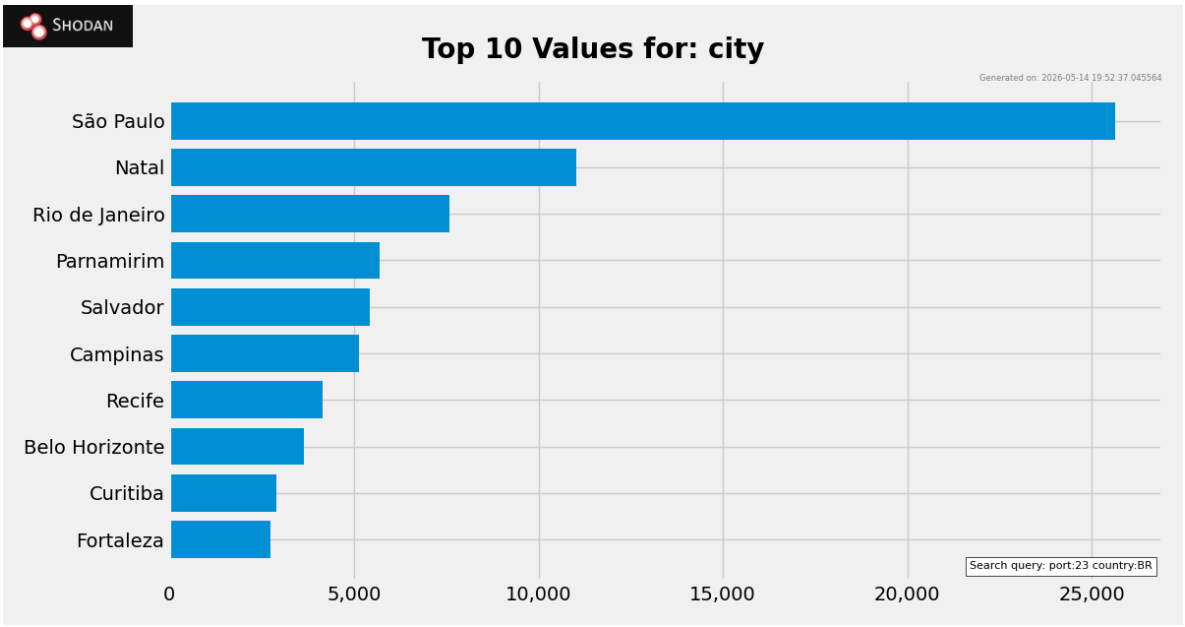


Fonte: Autoria própria

Devido ao fato de que qualquer dado transmitido através do protocolo Telnet não ter qualquer tipo de criptografia, o protocolo em sí pode ser considerado uma vulnerabilidade, uma vez que credenciais e dados sensíveis podem ser interceptados.

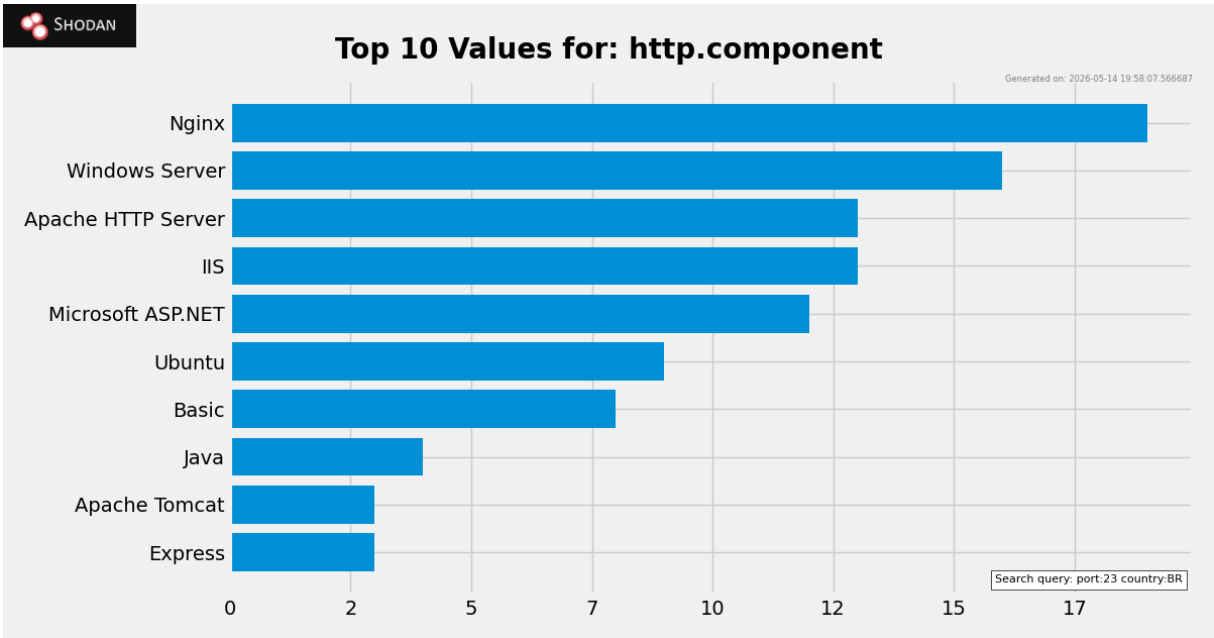
Utilizando a plataforma Shodan (figuras 42, 43, 44), é possível verificar as cidades onde o protocolo Telnet é mais utilizado assim como as tecnologias mais utilizadas por seus hosts.

Figura 42. Shodan - Cidades onde hosts de Telnet são mais comuns



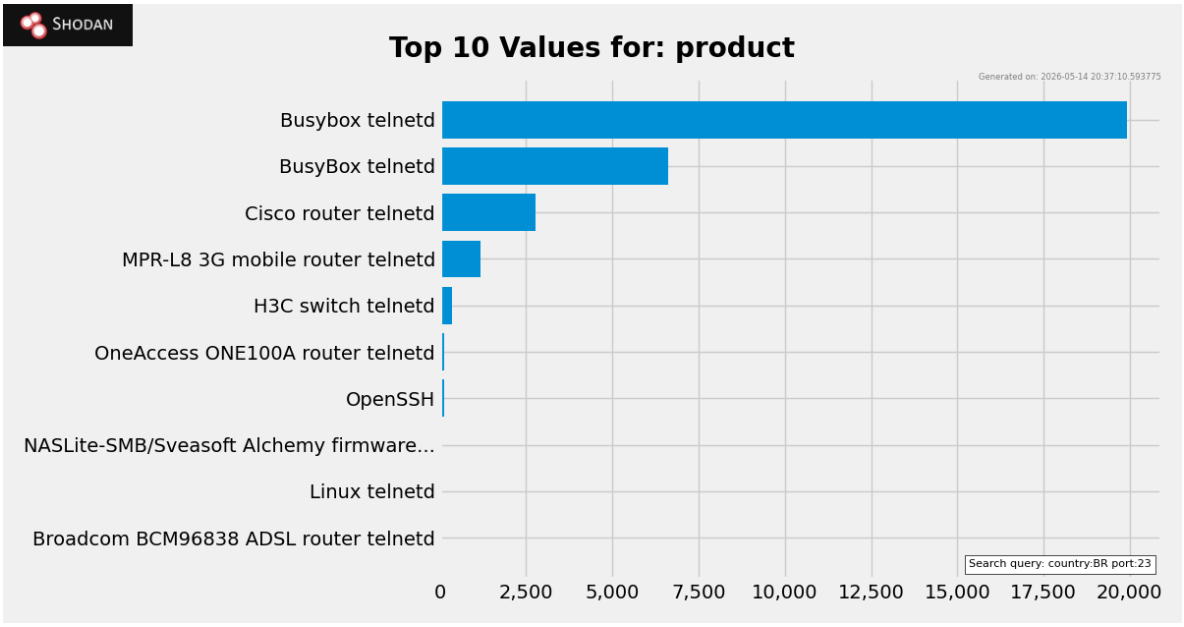
Fonte: Shodan facets

Figura 43. Shodan - Tecnologias utilizadas por hosts de Telnet



Fonte: Shodan facets

Figura 44. Shodan - Produtos utilizados por hosts de Telnet



Fonte: Shodan facets

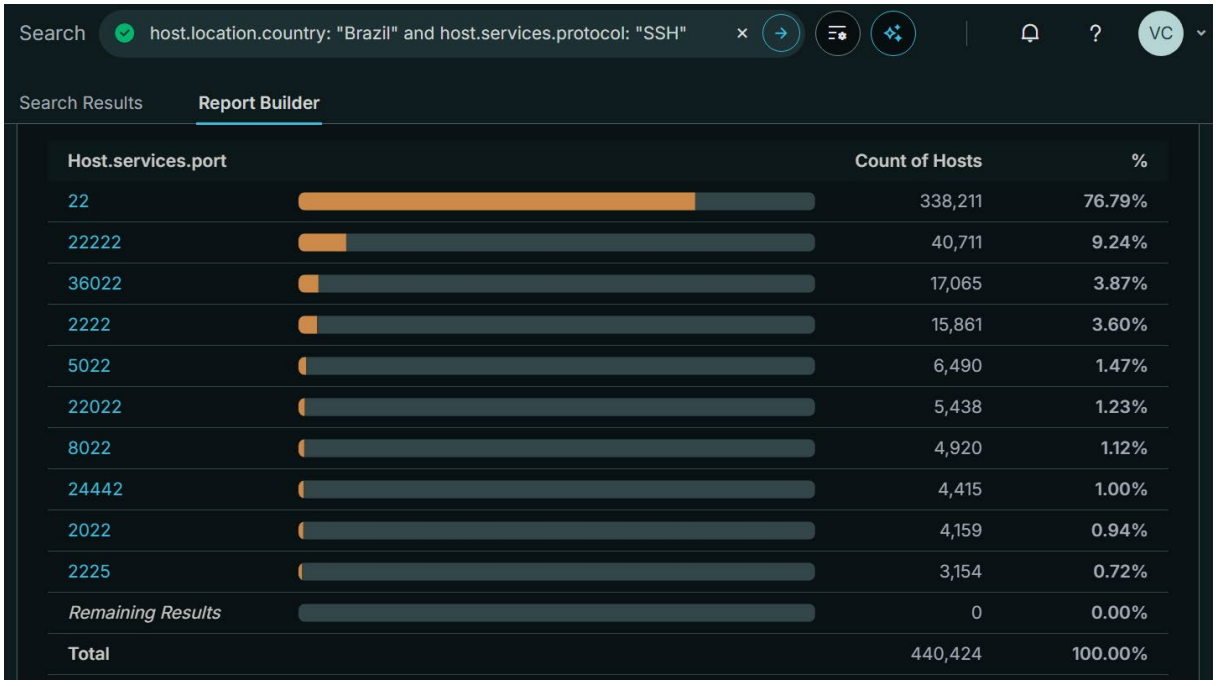
4.2.5. Exposição de hosts utilizando SSH no Brasil

Assim como explorado no tópico anterior, o protocolo SSH foi criado como uma alternativa segura para o Telnet e FTP, utilizando criptografia e autenticação seguros para acesso remoto de dispositivos e redes. O protocolo utiliza muitos

mecanismos de segurança como criptografia de ponta a ponta, tunneling e possui autenticação robusta, sendo mais comum em hosts que utilizam sistemas Linux e Unix estando presente na maioria dos servidores globais. Por padrão o protocolo utiliza a porta 22 para conexões.

Utilizando a plataforma Shodan, um total de 337,910 resultados quando escaneando a porta 22 no Brasil, porém a plataforma Censys (figura 45) que se especializa em protocolos, retorna 440,424 resultados, demonstrando também que cerca de 24% dos hosts expostos não utilizam a porta padrão e por isso não foram detectados pela plataforma Shodan utilizando a query de porta padrão.

Figura 45. Censys - Top 10 hosts utilizando SSH no Brasil

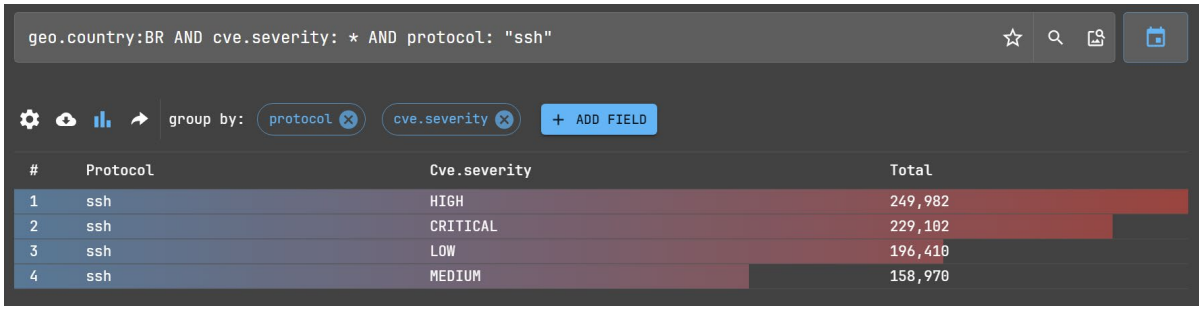


Host.services.port	Count of Hosts	%
22	338,211	76.79%
22222	40,711	9.24%
36022	17,065	3.87%
2222	15,861	3.60%
5022	6,490	1.47%
22022	5,438	1.23%
8022	4,920	1.12%
24442	4,415	1.00%
2022	4,159	0.94%
2225	3,154	0.72%
Remaining Results	0	0.00%
Total	440,424	100.00%

Fonte: Censys Report Builder

A plataforma Netlas retorna um total de 324,769 hosts utilizando SSH no Brasil, porém é capaz de nos fornecer uma analise mais abrangente de possíveis vulnerabilidades e verificando que 281,601 dos hosts de SSH possuem vulnerabilidades, representando 86% do total.

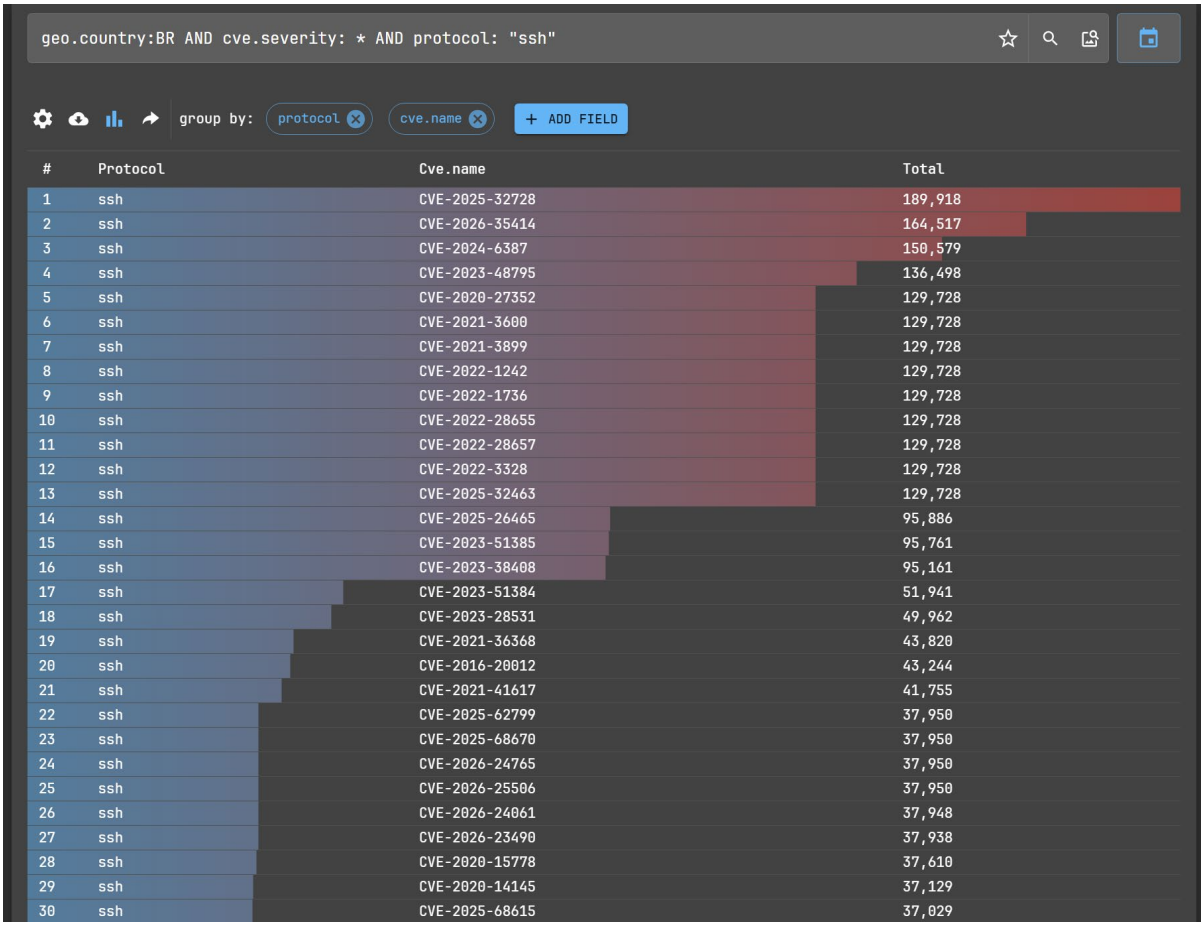
Figura 46. Netlas - Severidade de vulnerabilidades em hosts utilizando SSH



#	Protocol	Cve.severity	Total
1	ssh	HIGH	249,982
2	ssh	CRITICAL	229,102
3	ssh	LOW	196,410
4	ssh	MEDIUM	158,970

Fonte: Netlas

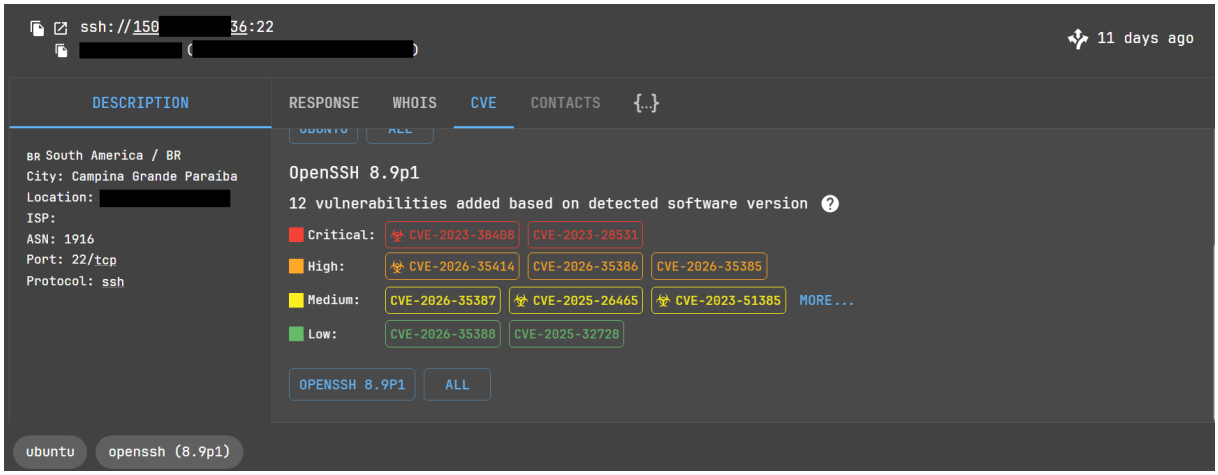
Figura 47. Netlas - 30 vulnerabilidades mais comuns em hosts utilizando SSH



#	Protocol	Cve.name	Total
1	ssh	CVE-2025-32728	189,918
2	ssh	CVE-2026-35414	164,517
3	ssh	CVE-2024-6387	150,579
4	ssh	CVE-2023-48795	136,498
5	ssh	CVE-2020-27352	129,728
6	ssh	CVE-2021-3600	129,728
7	ssh	CVE-2021-3899	129,728
8	ssh	CVE-2022-1242	129,728
9	ssh	CVE-2022-1736	129,728
10	ssh	CVE-2022-28655	129,728
11	ssh	CVE-2022-28657	129,728
12	ssh	CVE-2022-3328	129,728
13	ssh	CVE-2025-32463	129,728
14	ssh	CVE-2025-26465	95,886
15	ssh	CVE-2023-51385	95,761
16	ssh	CVE-2023-38408	95,161
17	ssh	CVE-2023-51384	51,941
18	ssh	CVE-2023-28531	49,962
19	ssh	CVE-2021-36368	43,820
20	ssh	CVE-2016-20012	43,244
21	ssh	CVE-2021-41617	41,755
22	ssh	CVE-2025-62799	37,950
23	ssh	CVE-2025-68670	37,950
24	ssh	CVE-2026-24765	37,950
25	ssh	CVE-2026-25506	37,950
26	ssh	CVE-2026-24061	37,948
27	ssh	CVE-2026-23490	37,938
28	ssh	CVE-2020-15778	37,610
29	ssh	CVE-2020-14145	37,129
30	ssh	CVE-2025-68615	37,029

Fonte: Netlas

Figura 48. Netlas - Vulnerabilidades encontradas em Host utilizando SSH



Fonte: Netlas

Os dados adquiridos através da plataforma Netlas (figura 46, 47 e 48) demonstram que a maioria das vulnerabilidades que podem afetar hosts utilizando SSH no Brasil são de severidade alta e critica, algo alarmante uma vez que múltiplas vulnerabilidades são geralmente encontradas em um único host, criando múltiplos vetores de ataque e expondo sistemas a diversos riscos.

4.2.6. Ativos expostos de maior criticidade

Alguns hosts tem um nível de importância maior que outros, seja por alguma ligação a infraestrutura, dados governamentais ou pesquisas que podem conter dados confidenciais, alguns exemplos seriam órgãos governamentais, universidades e instituições de pesquisa dentre outros. Infelizmente um numero preocupantemente alto de tais instituições está exposta, muitas também possuem indicios de que possam estar vulneráveis.

Por motivos éticos e de segurança, queries que possam expor instituições sensíveis serão suprimidos dos exemplos.

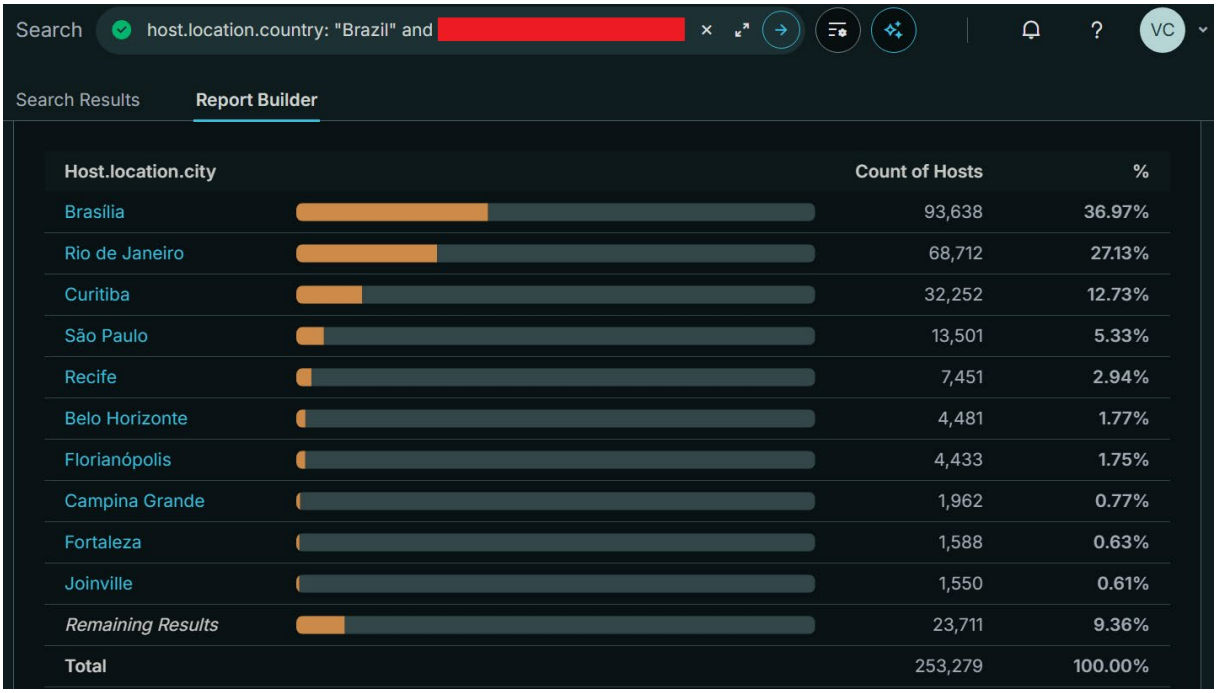
Utilizando a plataforma Shodan (figura 49), um total de 147,386 hosts que podem ser descritos como instituições de alta criticidade que possuem diversos ativos expostos.

Figura 49. Shodan - Instituições de alta criticidade com ativos expostos

Fonte: Shodan report

Utilizando a plataforma Censys (figura 50) com uma query buscando pelos mesmos tipos de instituição retornou um numero ainda maior de resultados, totalizando 253,279 hosts de alta criticidade com ativos expostos, tornando o fato ainda mais alarmante.

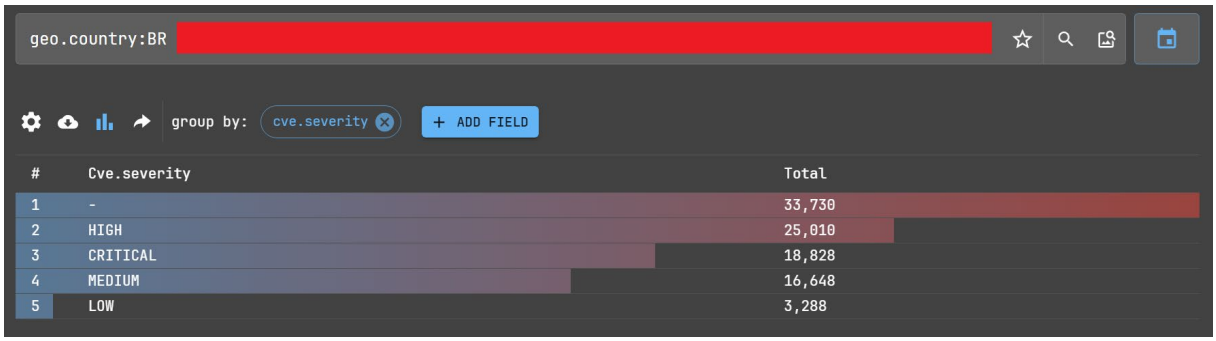
Figura 50. Censys - Hosts de alta criticidade com ativos expostos



Fonte: Censys report builder

Embora a plataforma Netlas tenha encontrado um total de hosts da mesma categoria com ativos expostos, a identificação de vulnerabilidades pela plataforma é mais eficiente nas condições de pesquisa, tendo um total de 59,144 hosts desta categoria e conseguiu identificar 33,730 dentre estes que possuem indícios de vulnerabilidades.

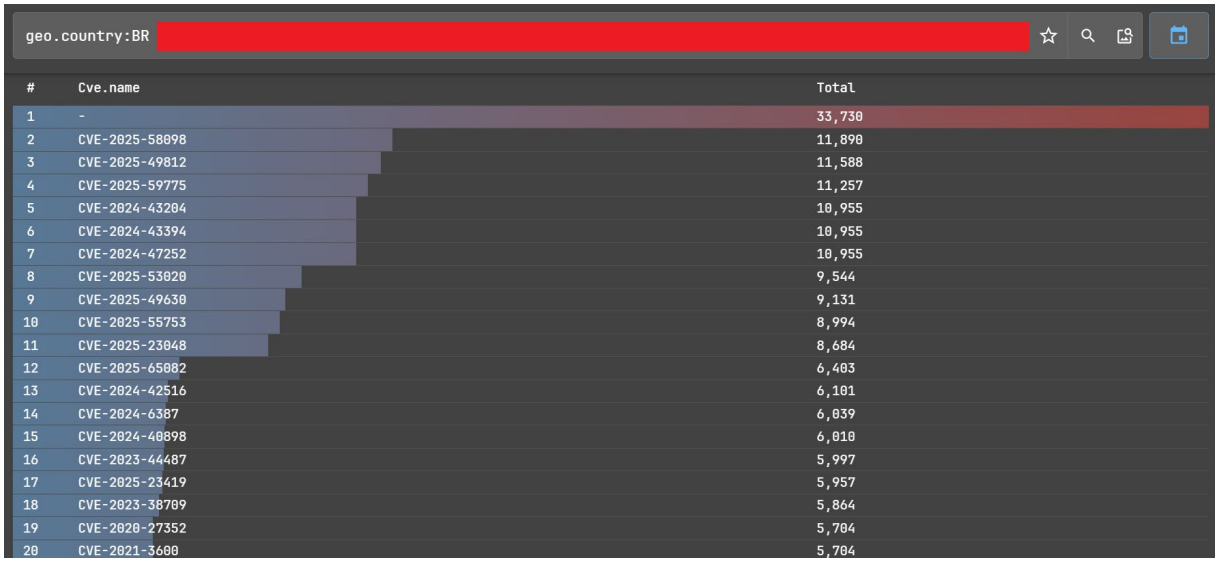
Figura 51. Netlas - Severidade de vulnerabilidades em hosts de alta criticidade



#	Cve.severity	Total
1	-	33,730
2	HIGH	25,010
3	CRITICAL	18,828
4	MEDIUM	16,648
5	LOW	3,288

Fonte: Netlas

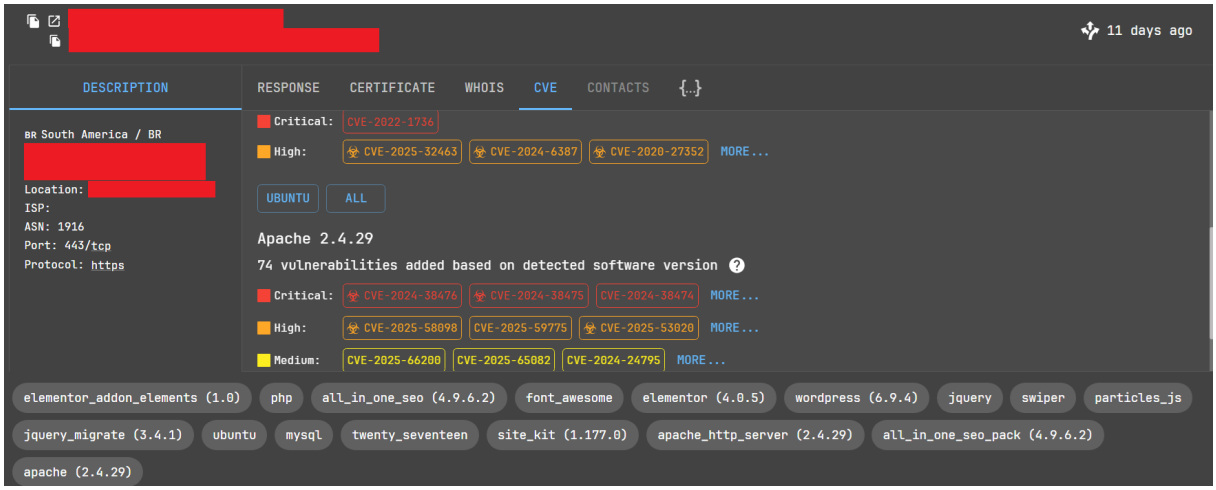
Figura 52. Netlas - Possiveis vulnerabilidades em hosts de alta criticidade



#	Cve.name	Total
1	-	33,730
2	CVE-2025-58098	11,890
3	CVE-2025-49812	11,588
4	CVE-2025-59775	11,257
5	CVE-2024-43204	10,955
6	CVE-2024-43394	10,955
7	CVE-2024-47252	10,955
8	CVE-2025-53020	9,544
9	CVE-2025-49630	9,131
10	CVE-2025-55753	8,994
11	CVE-2025-23048	8,684
12	CVE-2025-65082	6,403
13	CVE-2024-42516	6,101
14	CVE-2024-6387	6,039
15	CVE-2024-40898	6,010
16	CVE-2023-44487	5,997
17	CVE-2025-23419	5,957
18	CVE-2023-38709	5,864
19	CVE-2020-27352	5,704
20	CVE-2021-3600	5,704

Fonte: Netlas

Figura 53. Netlas - Host de alta criticidade com dezenas de vulnerabilidades



Fonte: Netlas

As vulnerabilidades observadas nas figura 51, 52 e 53 acima, principalmente considerando o volume de vulnerabilidades por host, torna a situação extremamente preocupante devido ao fato de que em muitos casos pode ser considerado um risco a segurança nacional por afetar diretamente a infraestrutura e órgãos do governo. Outros hosts também possuem Login Anonimo habilitado através do protocolo FTP e muitos utilizam softwares com vulnerabilidades conhecidas desde 2009.

4.2.7. Exposição de dispositivos IOT no Brasil

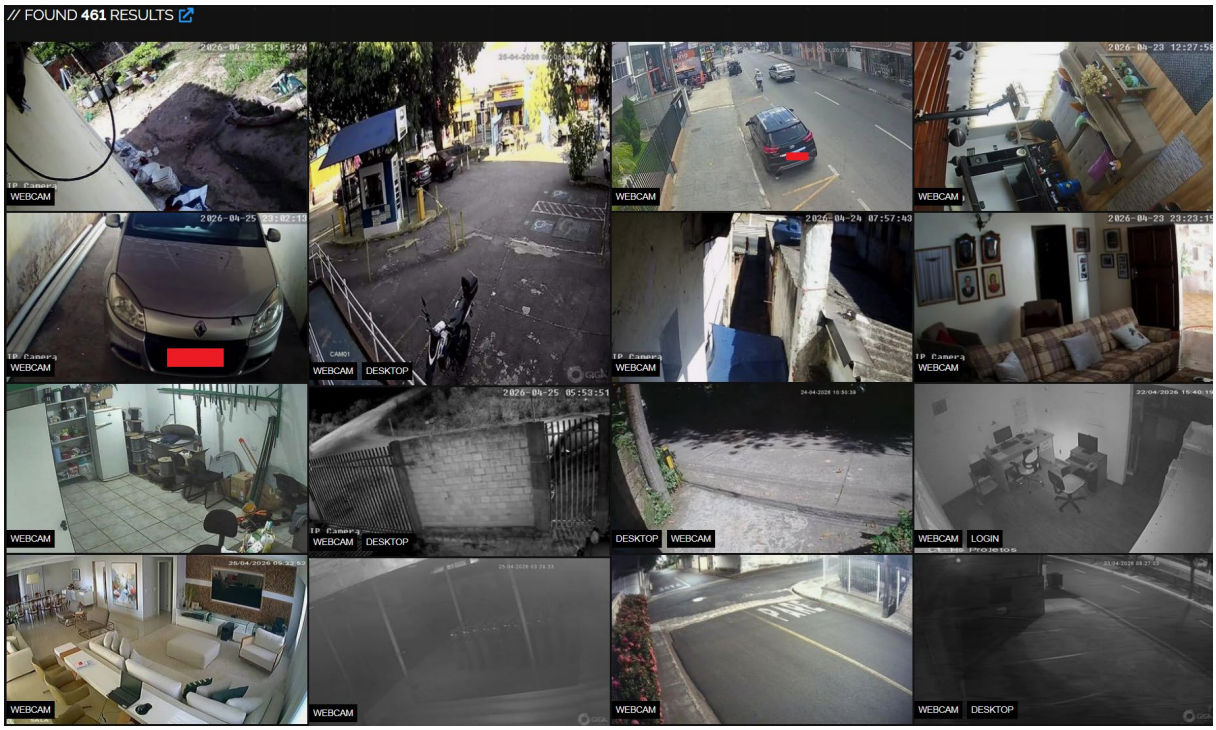
Dispositivos IoT (Internet of Things) estão presentes em quase todos os ambientes, alguns exemplos são câmeras de segurança, webcams, dispositivos de limpeza autônomos (rombas) e outros.

Tais dispositivos caso expostos publicamente posam um risco real, uma vez que o fato de estarem expostos, muito provavelmente não seguem boas praticas de segurança e muitos destes provavelmente contém vulnerabilidades e se torna uma porta de entrada para possíveis ataques.

Utilizando a plataforma Shodan, é possível observar que cerca de 461 cameras estão expostas no Brasil, algo que envolve casas, empresas e até computadores particulares.

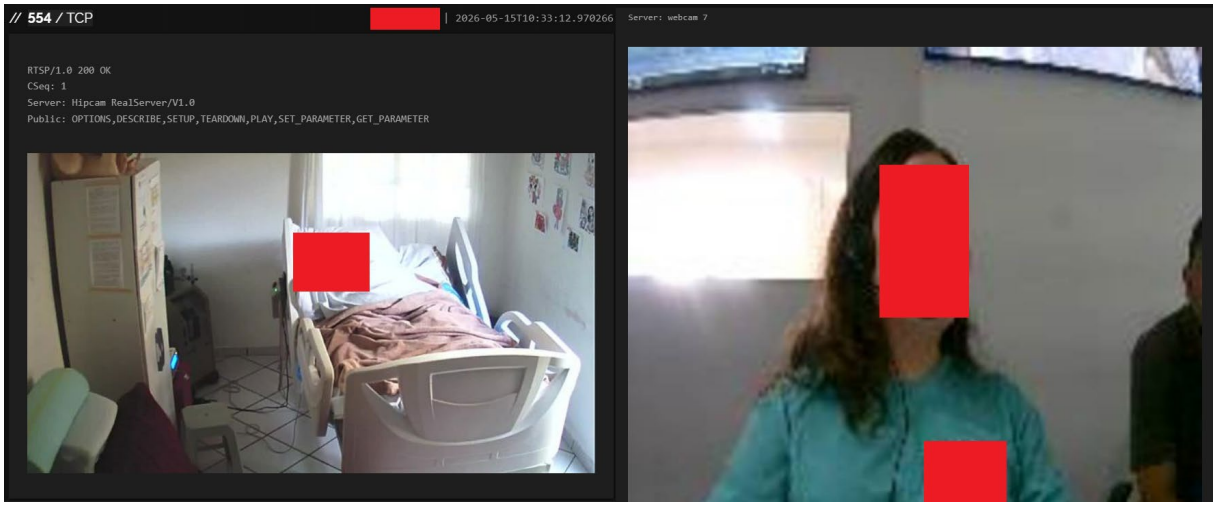
Nas figuras 54, 55 e 56 é possível observar que vários tipos de câmeras são acessíveis publicamente, em alguns casos expondo

Figura 54. Shodan - Cameras de segurança/webcams expostas no Brasil



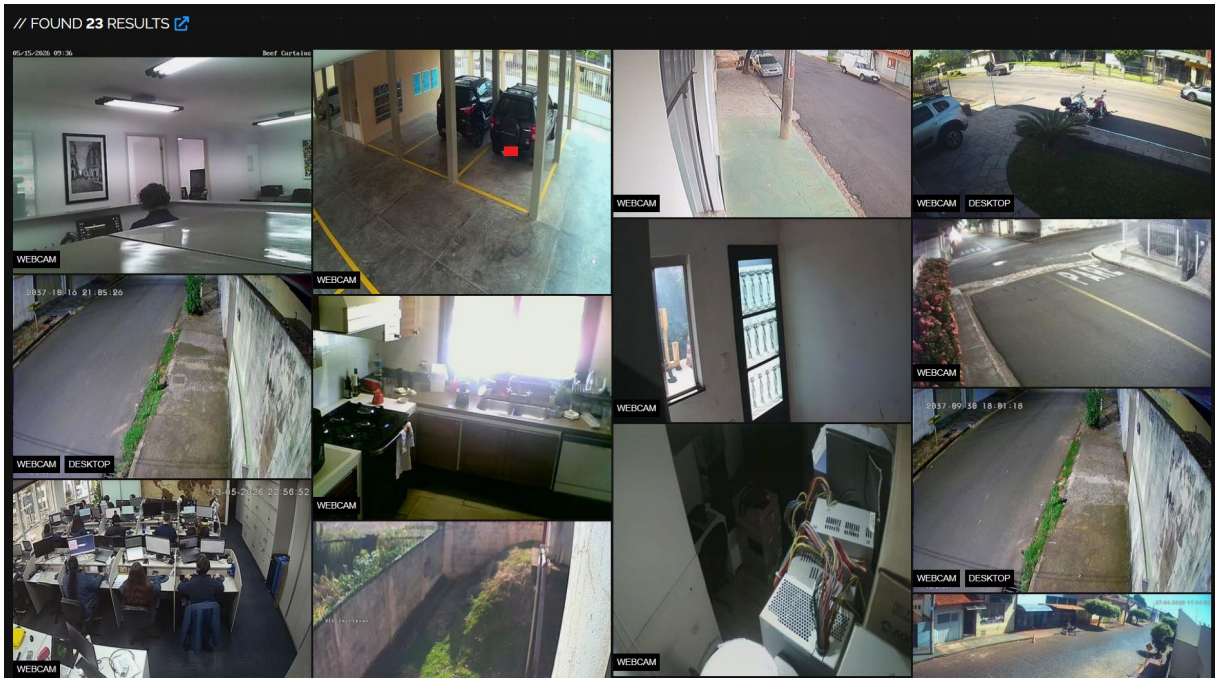
Fonte: Shodan images

Figura 55. Shodan - Exemplos criticos de cameras expostas



Fonte: Shodan images

Figura 56. Shodan - Cameras de segurança com indicios de vulnerabilidade



Fonte: Shodan images

As imagens acima ilustram perfeitamente os riscos de dispositivos IoT expostos, em especial as câmeras da imagem 52, que permitem que usuários não autorizados tenham acesso a um sistema de segurança e possivelmente sejam capazes de realizar um ataque contra o mesmo.

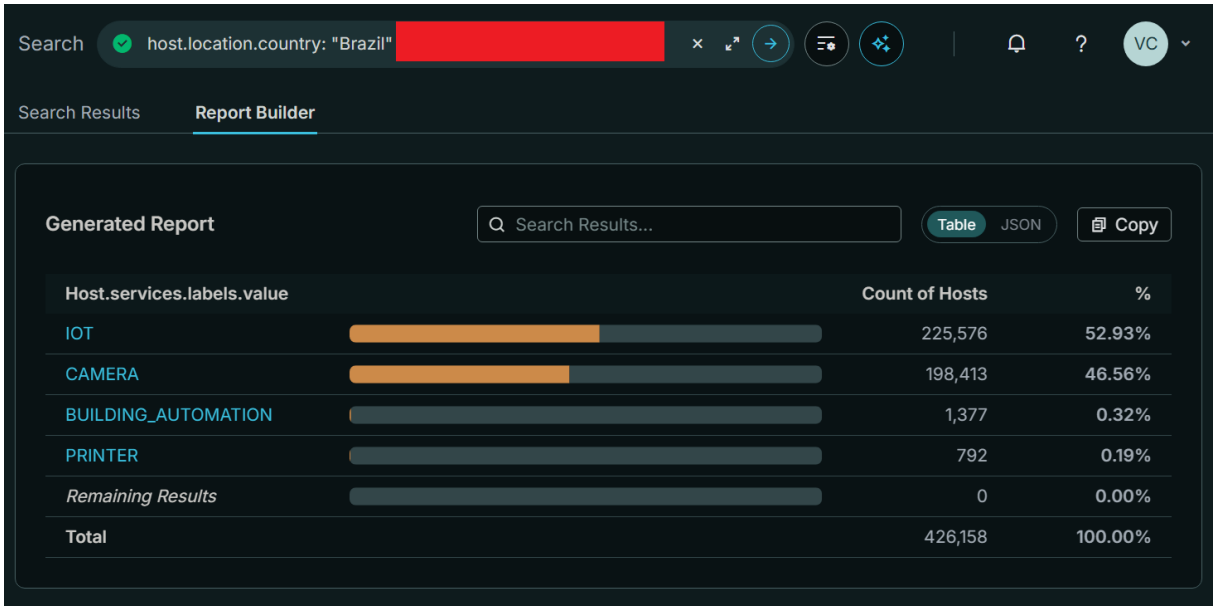
A imagem 53 contem imagens de uma câmera de segurança e de uma webcam de uma empresa, ambas estão expostas e possuem múltiplas portas abertas e expostas, a segunda câmera também possui múltiplas vulnerabilidades e posam um risco real a rede e aos dispositivos da empresa as utilizando e ambas as câmeras posam um risco de privacidade.

A imagem 54 mostra câmeras com vulnerabilidades conhecidas, com um total de 23 dispositivos encontrados, demonstrando que muitos destes dispositivos possuem vulnerabilidades e posam riscos reais. Os resultados obtidos incluem somente vulnerabilidades das câmeras e não nos hosts em sí, muitos dispositivos não foram incluídos pelas vulnerabilidades estarem presentes no host e não no dispositivo IoT, demonstrando que o risco é ainda maior.

Utilizando a ferramenta Censys (figura 57), podemos realizar uma varredura mais profunda de dispositivos IoT, retornando um total de 426,158 resultados, destes, um total de 225,576 são dispositivos IoT e 198,413 são câmeras (webcams e câmeras

de segurança), 1,377 são dispositivos de automação de imóveis e 792 são impressoras como ilustrado na imagem abaixo, demonstrando mais uma vez que o volume de ativos expostos no Brasil é muito alto.

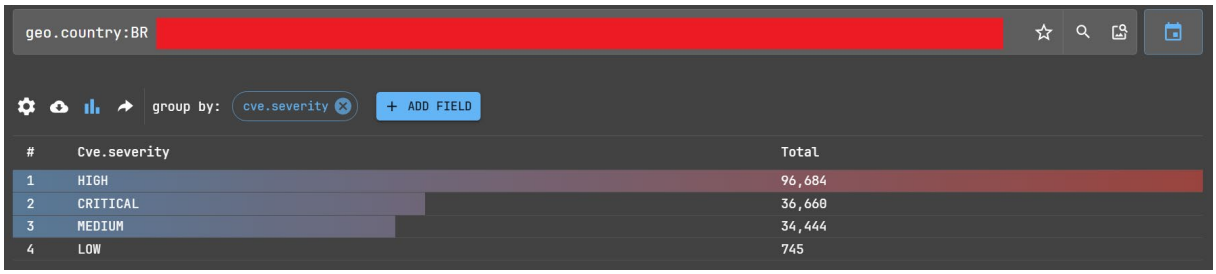
Figura 57. Censys - Dispositivos IoT expostos no Brasil



Fonte: Censys report builder

Utilizando a plataforma Netlas (figura 58 e 59), foi possível identificar cerca de 97,168 dispositivos IoT de diversos tipos com vulnerabilidades conhecidas, em sua maioria de severidade alta e critica, mais uma vez expondo a magnitude do problema relacionado a ativos expostos, uma vez que estes dispositivos podem ser impressoras ou qualquer outro dispositivo “smart” com conexão à internet.

Figura 58. Netlas - Dispositivos IoT por severidade de vulnerabilidades no Brasil



Fonte: Netlas

Figura 59. Netlas - Vulnerabilidades mais comuns em dispositivos IoT no Brasil

#	Cve.name	Total
1	CVE-2025-21587	37,456
2	CVE-2025-30749	37,456
3	CVE-2025-50059	37,456
4	CVE-2025-50063	37,454
5	CVE-2025-50106	37,454
6	CVE-2025-53066	37,454
7	CVE-2026-21932	37,454
8	CVE-2026-21945	37,454
9	CVE-2024-20952	37,415
10	CVE-2024-21147	37,415
11	CVE-2023-44487	23,519
12	CVE-2025-23419	23,267
13	CVE-2025-58098	20,228
14	CVE-2025-49812	19,981
15	CVE-2025-59775	19,420
16	CVE-2024-43204	19,173
17	CVE-2024-43394	19,173
18	CVE-2024-47252	19,173
19	CVE-2025-53020	18,690
20	CVE-2025-49630	18,157
21	CVE-2025-55753	18,152
22	CVE-2025-23048	17,897
23	CVE-2022-31631	16,581
24	CVE-2024-11233	16,581
25	CVE-2024-11235	16,581
26	CVE-2024-11236	16,581
27	CVE-2025-14178	16,581
28	CVE-2025-14180	16,581
29	CVE-2025-1735	16,581
30	CVE-2024-11234	16,576

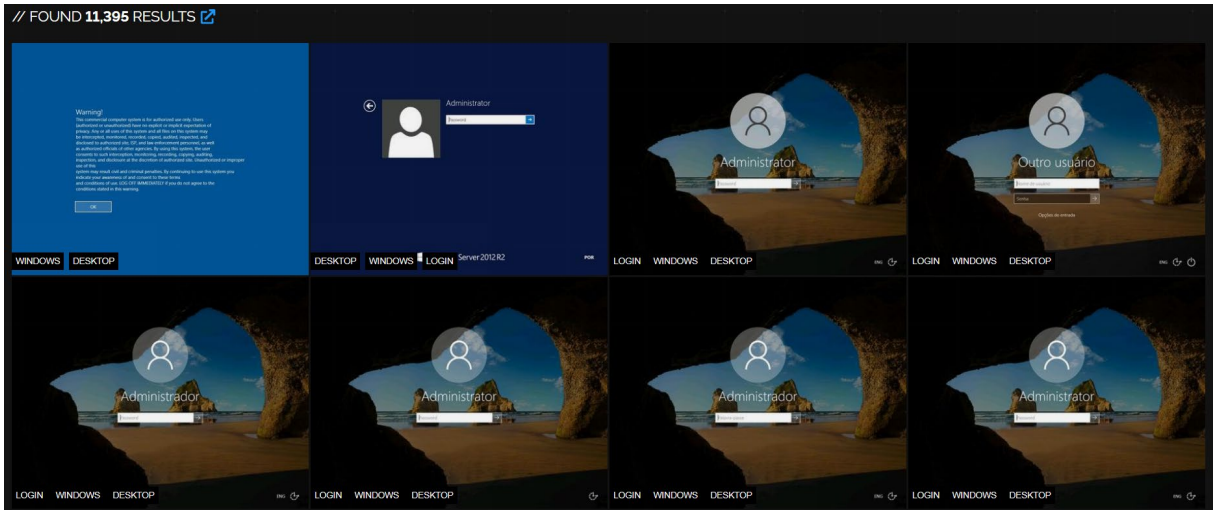
Fonte: Netlas

4.2.8. Interfaces de Login expostas no Brasil

As interfaces de login remoto são um ativo de alta periculosidade caso expostos, muitas vezes devido ao fato de serem para uso administrativo.

Utilizando a plataforma Shodan (figura 60), um total de 11,395 paginas de login remoto foram encontradas. Devido a serem paginas de Login, é possível visualizar a versão e tipo de sistema operacional através da própria interface.

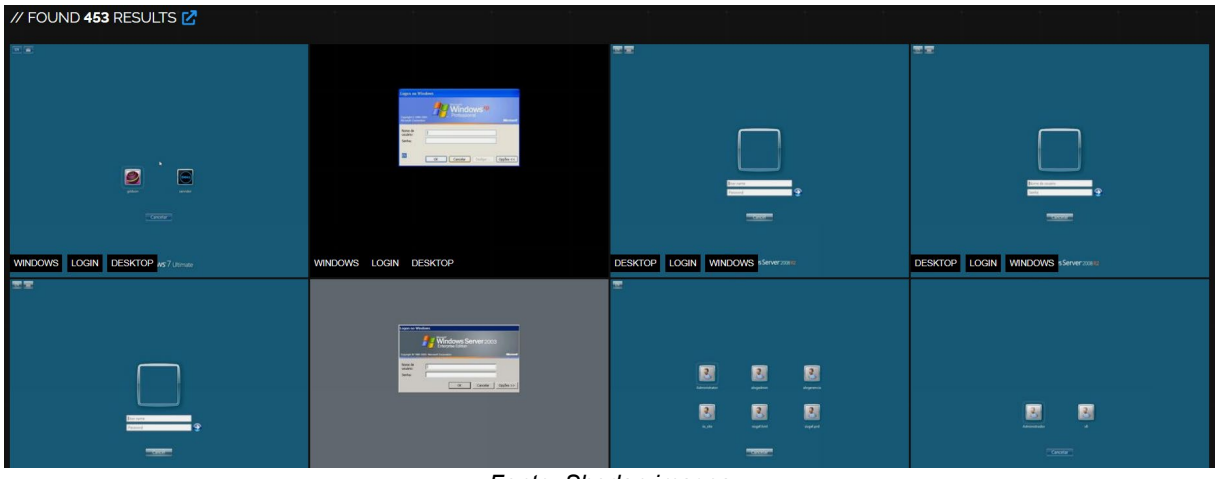
Figura 60. Shodan - Interfaces de login remoto expostas no Brasil



Fonte: Shodan images

Cerca de 453 possuem vulnerabilidades conhecidas, e todas as interfaces da imagem abaixo (figura 61) possuem a vulnerabilidade “Eternal Blue” que possibilita a execução remota código na maquina alvo, levando a um comprometimento completo do alvo e foi a causa de diversos ataques globais como os malwares “Wannacry” e “NotPetya”.

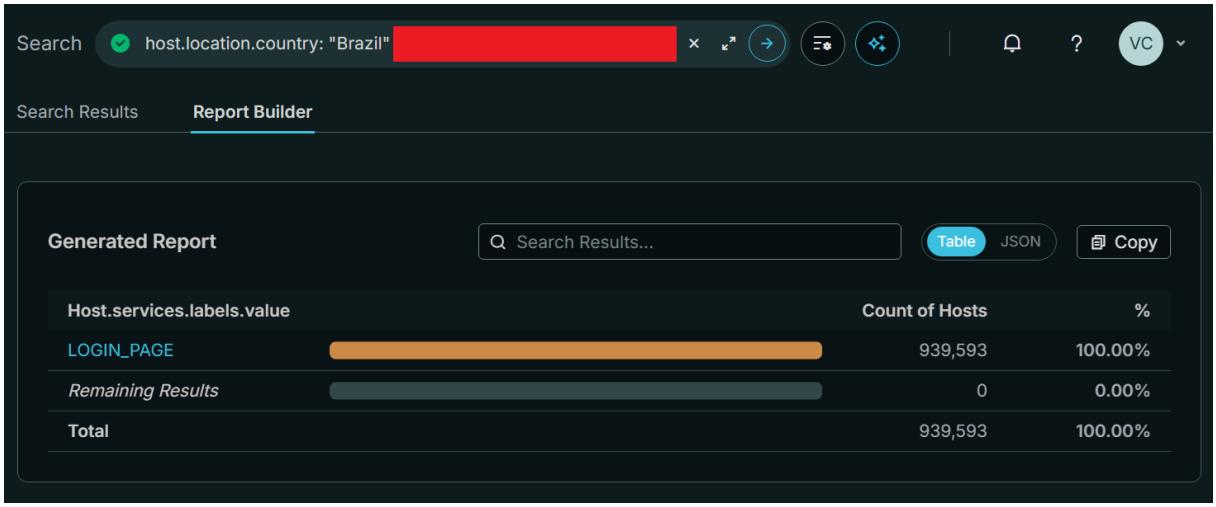
Figura 61. Shodan - Interfaces de login expostas e com vulnerabilidades



Fonte: Shodan images

Utilizando a plataforma Censys (figura 62), um total de 939,593 resultados foi encontrado, muitos destes hosts também utilizam outros serviços e em alguns casos também tem dispositivos IoT ligados a eles.

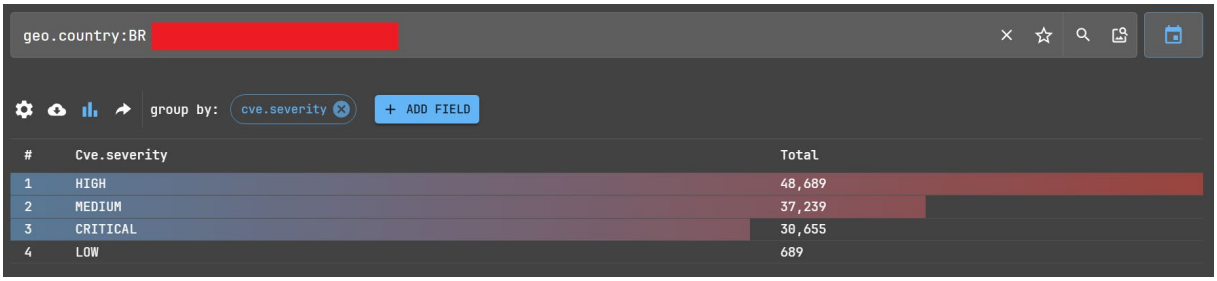
Figura 62. Censys - Interfaces de login expostos



Fonte: Censys report builder

Utilizando a plataforma Netlas (figura 63), é possível verificar que a maioria das interfaces de login remoto que possuem vulnerabilidades, possuem severidade Alta e Média.

Figura 63. Netlas - Severidade de vulnerabilidades em hosts com login exposto



Fonte: Netlas

5. RESULTADOS OBTIDOS

Neste capítulo, são apresentados e discutidos os principais resultados obtidos a partir da análise dos ativos expostos e dos serviços identificados ao longo da pesquisa. Diferentemente do capítulo anterior, que detalhou o desenvolvimento da investigação e a organização dos dados por tipo de serviço, esta etapa busca sintetizar os achados mais relevantes, destacando padrões de exposição, uso de protocolos potencialmente inseguros, presença de interfaces acessíveis publicamente e indícios de vulnerabilidades associadas aos ativos observados. Dessa forma, os resultados são organizados de maneira a evidenciar os riscos mais recorrentes no cenário brasileiro e a relacioná-los com as práticas de segurança discutidas na fundamentação teórica, reforçando a importância da manutenção, configuração adequada e monitoramento contínuo de sistemas conectados à internet.

5.1. Visão Geral

O presente trabalho tem como objetivo a analise de ativos expostos no Brasil, algo que foi devidamente explorado, ilustrando a escala de exposição, a exposição e vulnerabilidade das tecnologias com maior exposição, exposição e vulnerabilidades de protocolos assim como a utilização de protocolos obsoletos.

De forma geral o trabalho foi capaz de demonstrar com exemplos reais e de diversas fontes a gravidade da situação e a importância de se seguir melhores práticas de segurança.

5.2. Exposição no Brasil

A exposição no brasil como demonstrado é grande, porém a maioria dos problemas encontrados é devido a falta de manutenção de sistemas, seja pela utilização de componentes obsoletos e vulneráveis, ou pela falta de atualização de sistemas operacionais e outras tecnologias utilizadas.

No caso das vulnerabilidades e nível de exposição demonstrados no tópico 4.1, elas podem ser classificadas como pertencendo às vulnerabilidades A03 – Software Supply Chain Failures e A01 - Broken Access Control, respectivamente devido a falta de atualização dos softwares utilizados e de controle de acesso.

É importante citar que a exposição de grande parte dos hosts é devido ao item A01 e deve ser remediado através do uso de proxies e VPNs para que seja possível limitar o acesso e visibilidade do host a somente dispositivos e usuários autorizados.

5.3. Uso de protocolos obsoletos ou sem segurança

A análise dos protocolos identificados nos ativos expostos permite compreender parte dos riscos associados à superfície de ataque observada no Brasil. Embora alguns protocolos ainda sejam amplamente utilizados em ambientes corporativos e institucionais, sua exposição direta à internet pode representar um problema quando ocorre sem criptografia, sem autenticação adequada, com versões desatualizadas ou com configurações inseguras. Nesse contexto, protocolos como HTTP, SMB, FTP, Telnet e SSH foram analisados de forma separada, considerando suas características, seus usos mais comuns e os indícios de vulnerabilidades encontrados nas plataformas consultadas. A seguir, inicia-se a discussão pelo HTTP, por ser um dos protocolos mais presentes em serviços web e por apresentar riscos relevantes quando utilizado sem mecanismos adequados de proteção, especialmente em páginas de login, interfaces administrativas e sistemas que trafegam informações sensíveis.

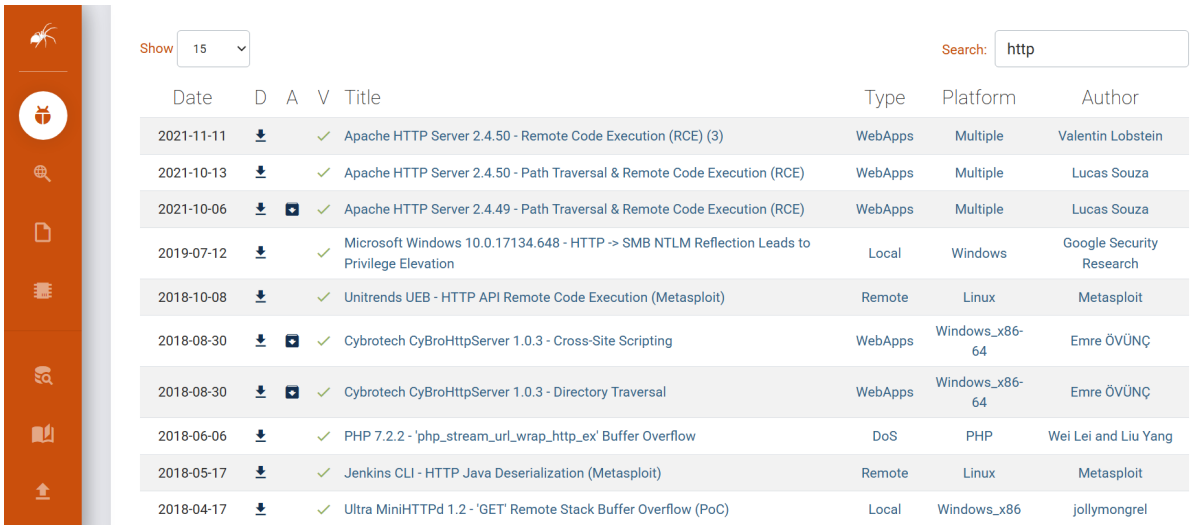
5.3.1. HTTP

Em relação ao tópico 4.2.1 e a utilização de HTTP sem nenhum tipo de criptografia no Brasil, representando entre aproximadamente 40% e 43% de todos os ativos expostos no Brasil, se enquadra em múltiplos tópicos do ranking OWASP TOP 10, mais precisamente A04 - Cryptographic Failures, A02, - Security Misconfiguration, A01 - Broken Access Control, A03 - Software Supply Chain Failures.

Os riscos de tais vulnerabilidades são o comprometimento de dados em trânsito (sendo enviados e recebidos) assim como o próprio comprometimento dos sistemas envolvidos uma vez que é possível adquirir informações sensíveis e também devido a múltiplas outras vulnerabilidades presentes devido a falta de manutenção dos mesmos. O fato de muitas destas vulnerabilidades serem antigas faz com que o risco seja ainda maior, uma vez que já existe um extenso número de métodos de

exploração das mesmas disponíveis publicamente seja em bancos de dados públicos (figura 64 abaixo) como em ferramentas de exploração como Metasploit e outros.

Figura 64. ExploitDB - Exploits para vulnerabilidades de hosts HTTP



Fonte: Exploit Database

Em sua grande maioria, se deve a sistemas com pouca ou nenhuma manutenção, o que permite acesso de praticamente qualquer usuário aos dados sendo enviados e recebidos por tais hosts, demonstrando falta de acesso de controle (A01), total falta de medidas de proteção de dados devido a falta de atualização de software ou implementação de protocolos como SSL/TLS (A04, A02, A03), muitos dos quais podem ser sanados com atualizações periódicas e no caso de deficiências na área de criptografia, soluções como implementação de protocolos mais seguros devem ser buscadas, e a exposição excessiva pode ser sanada através de melhor configuração de portas e serviços que não precisem estar expostos.

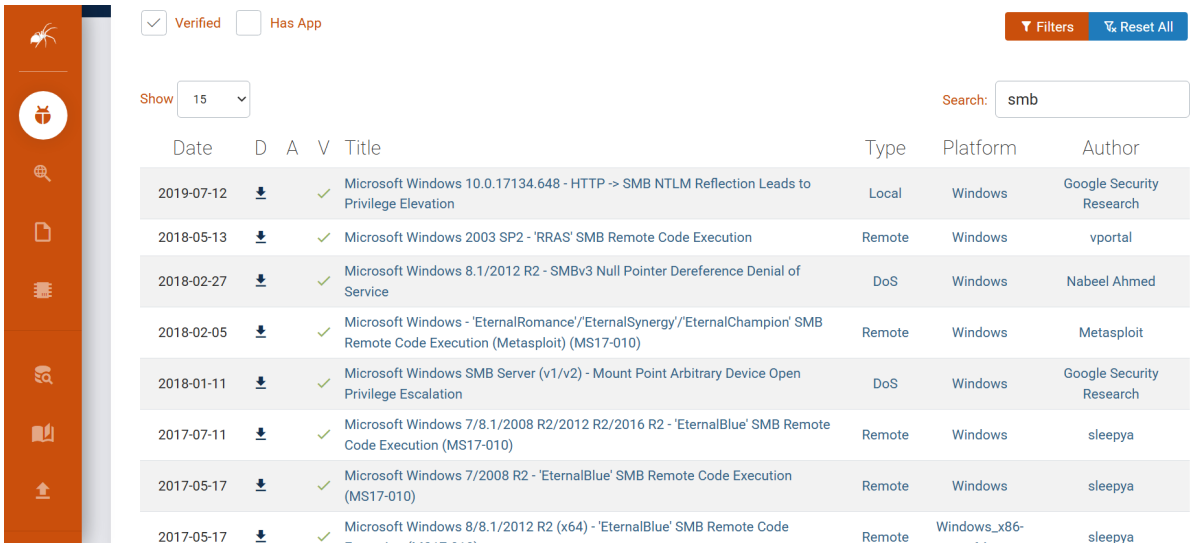
5.3.2. SMB

Em relação ao tópico 4.2.2, foi examinado o uso de SMB no Brasil, sendo este protocolo afetado pela vulnerabilidade mais comum no país, o SMBGhost.

Foi constatado que cerca de 11% dos hosts detectados no Brasil não utilizam nenhum tipo de autenticação, enquanto cerca de 38% dos hosts utilizando SMB no Brasil possuem vulnerabilidades, sendo que aproximadamente 92% destes possuem indícios da vulnerabilidade SMBGhost que tem um funcionamento muito similar à

vulnerabilidade “EternalBlue” que foi a causa de dois ataques globais de larga escala e posa um risco real no Brasil, principalmente devido ao fato de que existem diversos métodos de exploração verificados das mesmas em diversos bancos de dados públicos (como na figura 65 abaixo) e o histórico de exploração em massa de tais vulnerabilidades .

Figura 65. ExploitDB - Exploits para vulnerabilidades de hosts SMB



Fonte: Exploit Database

As vulnerabilidades são resultados de falhas relacionadas aos seguintes itens presentes no ranking OWASP TOP 10: A01 - Broken Access Control, A02 - Security Misconfiguration e A03 - Software Supply Chain Failures. Em relação aos itens A01 e A02, se deve ter mais cuidado ao fazer a configuração dos hosts e possivelmente tornar necessário que a conexão seja feita a partir de um IP especifico para evitar que o host continue exposto. Em relação ao item A03, atualização periódicas e uso de tecnologias mais modernas solucionaria grande parte do problema uma vez que tais vulnerabilidades são antigas e já foram corrigidas em versões mais recentes dos softwares utilizados.

5.3.3. FTP

Um protocolo obsoleto, que mesmo sem estar muito vulnerável no Brasil a pesar de que muitos de seus hosts possuem vulnerabilidades que não estão ligadas

ao protocolo em sí, ainda é muito utilizado por instituições importantes como universidades e orgãos governamentais.

As vulnerabilidades associadas a este protocolo e seus hosts correspondem aos items: A01 - Broken Access Control, A02 - Security Misconfiguration, A03 - Software Supply Chain Failures, A04 - Cryptographic Failures e A07 - Authentication Failures.

A primeira vulnerabilidade a ser abordada se encaixa na categoria A03, e é a falta de atualização e existência de múltiplas vulnerabilidades, muitas vezes antigas e com explorações conhecidas como exemplificado abaixo na imagem 65. A correção de tal problema pode ser feito com atualizações periódicas ou através da utilização de um protocolo mais moderno como SSH que possui funcionalidades similares e com mais segurança.

Figura 66. ExploitDb – Exploits para vulnerabilidades de hosts FTP

Fonte: Exploit Database

Como exemplificado na imagem 66 acima, há uma gama de exploits para o protocolo em questão, muitas delas também presentes em ferramentas voltadas à exploração de vulnerabilidades.

Vulnerabilidades relacionadas aos itens A01, A02, A04 e A07 são relacionadas a falta de segurança ou erros de configuração dos hosts de FTP, uma vez que em muitos deles o Login anônimo está habilitado demonstrando erros de configuração que provavelmente podem indicar o uso de senhas padrão entre outras coisas.

5.3.4. Telnet

A utilização do protocolo Telnet foi explorada no item 4.2.4 e rendeu resultados interessantes, infelizmente o simples uso do protocolo em si já pode ser considerado uma vulnerabilidade devido a total falta de mecanismos de segurança e pode ser visto como aceitável somente em usos limitados como conexão a equipamentos antigos em uma rede interna, teste de ports TCP, e debugging. Além dos riscos de interceptação de dados, Telnet como todo protocolo antigo também possui diversos modos de exploração de vulnerabilidades conhecidos.

Figura 67. ExploitDB - Exploits para vulnerabilidades de hosts Telnet

Fonte: Exploit Database

Como o protocolo não é seguro por natureza, sua vulnerabilidade se encaixa na categoria A03 - Software Supply Chain Failures do ranking OWASP Top 10, mais precisamente pelo fato de ser obsoleto e deveria ser preferencialmente substituído pelo uso de SSH que possui diversos mecanismos de segurança. Além disso, como se pode constatar pela imagem 67, também existem vários exploits para o protocolo, aumentando ainda mais o risco. A atualização e outras medidas que sanariam deficiências em outros protocolos não é aplicável neste caso pela incapacidade do próprio protocolo de proteger os dados sendo enviados e recebidos, algo que também

se adequa ao item A04 - Cryptographic Failures porém não há atualizações ou plugins que possam resolver o problema de forma eficiente.

5.3.5. SSH

A utilização do protocolo SSH foi explorada no item 4.2.5 e foi possível verificar que felizmente o numero de hosts utilizando SSH é maior que o numero de hosts utilizando Telnet, porém também foi possível identificar que uma boa parcela dos hosts de SSH possuem vulnerabilidades.

Utilizando a plataforma Netlas foi possível observar que 87% dos hosts utilizando SSH no Brasil possuem alguma vulnerabilidade, um volume alarmante de hosts vulneráveis, em sua maioria devido a outros componentes e falta de atualizações.

Figura 68. ExploitDB - Exploits para vulnerabilidades em hosts SSH

Fonte: Exploit Database

As vulnerabilidades dos hosts SSH no Brasil se encaixam mais no item A03 - Software Supply Chain Failures, que em sua maioria pode ser remediada através de atualizações periódicas, garantindo que vulnerabilidades conhecidas sejam corrigidas. Na figura 68 é possível ver que existem diversos exploits ligado ao protocolo, o que confirma o fato de que a mera exposição pode se tornar um risco real.

5.3.6. Ativos expostos de maior criticidade

Um fato importante abordado no tópico 4.2.6 detalha a vulnerabilidade de hosts que possuem grande importância, estes hosts na maioria dos casos não aparentam seguir boas praticas de manutenção e muitos possuem uma quantidade muito alta de vulnerabilidades em um único host.

As vulnerabilidades observadas em tais hosts se encaixam em todas as categorias abordadas por este trabalho: A01 - Broken Access Control, A02 - Security Misconfiguration, A03 - Software Supply Chain Failures, A04 - Cryptographic Failures, A07 - Authentication Failures.

Os hosts citados são considerados de alta criticidade devido a sua importancia, sendo alguns destes: tribunais estaduais e federais, ministérios, universidades publicas e privadas, agencias nacionais, orgãos governamentais (municipais, estaduais e da união), fundações de pesquisa, empresas do setor de energia, instituições ligadas a segurança publica e outros.

Para sanar as vulnerabilidades encontradas, as principais remediações seriam atualizações periódicas e a utilização de tecnologias mais modernas, como sugerido para o item A03, melhores configurações de segurança dentre outras medidas seriam capazes de sanar problemas relacionados a exposição e controle de acesso correspondendo às demais vulnerabilidades.

5.3.7. IoT

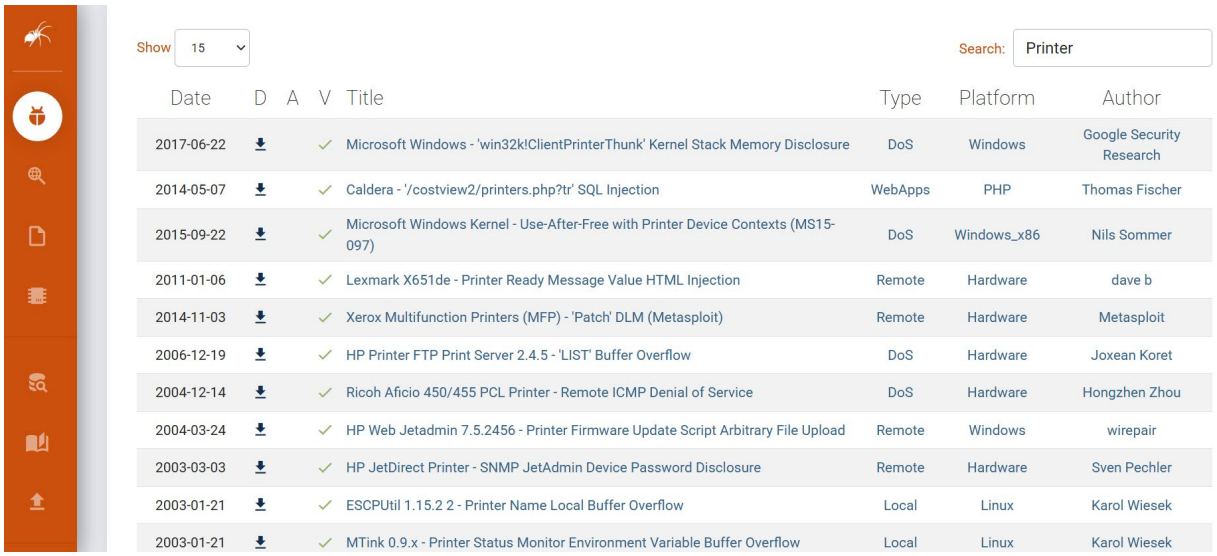
No item 4.2.7 foi explorada a exposição de dispositivos IoT, que em alguns casos sua mera exposição já pode ser considerada como uma violação de privacidade, como foi demonstrado no caso das câmeras de segurança e webcams, e em relação a outros dispositivos que em alguns casos possuem vulnerabilidades, posam um risco direto aos dispositivos conectados na rede, sejam estes dispositivos impressoras, lâmpadas smart, ou eletrodomésticos como foi citado no item 2.3.

Impressoras e outros dispositivos já foram hackeados simplesmente por estarem expostos, como quando um hacker obteve controle de 50.000 impressoras para promover um youtuber e conscientizar o publico sobre os riscos de exposição (Tech radar, 2018). É importante citar que existem ferramentas especializadas de

ataque contra dispositivos como IoT, como impressora para ganhar acesso ao dispositivo IoT assim como outros na própria rede.

Muitos dos dispositivos IoT encontrados possuem vulnerabilidades assim como os seus hosts (e.g. imagem 69 abaixo), tornando o risco ainda maior. Em muitos casos, dispositivos IoT podem se tornar partes de Botnets (uma rede de dispositivos conectados a internet que foram comprometidos e são controlados remotamente), alguns exemplos de tais botnets são: Mirai, Mozi, Masjesu e PumaBot (The Hacker News, 2026; Check Point, s.d.).

Figura 69. ExploitDB - Exploits para vulnerabilidades em impressoras



Fonte: Exploit Database

No caso de dispositivos IoT, a maioria dos problemas pode ser associado aos seguinte itens presentes no ranking OWASP TOP 10: A01 - Broken Access Control, A02 - Security Misconfiguration e A03 - Software Supply Chain Failures.

Especificamente em relação a câmeras, impressoras e outros dispositivos IoT que podem transmitir imagens e dados sensíveis, é necessário que haja autenticação e que o acesso seja restrito somente a dispositivos e usuários pré aprovados. Em relação a impressoras, idealmente devem ser acessadas somente por dispositivos dentro da própria rede e uma melhor configuração dos ports é necessária. Sensores e outros dispositivos devem ser configurados de uma maneira similar, solucionando assim os itens A01 e A02.

Em relação a câmeras e outros hosts que possuem vulnerabilidades, é necessário que se faça atualizações periódicas para que as vulnerabilidades

conhecidas sejam corrigidas utilizando as versões mais recentes, resolvendo o item A03.

É importante citar que muitos dispositivos IoT utilizam peças ou software de terceiros assim como protocolos como Telnet ou Ftp, onde se originam muitas de suas vulnerabilidades, e neste caso não existem meios de remediação para um usuário comum além de atualizações e melhores configurações.

5.3.8. Interfaces de Login

No item 4.2.8, a exposição de interfaces de login remoto foi explorada, um total de 939,593 interfaces expostas foi identificada na plataforma Censys, com mais de 11.000 destas sendo visualizadas através da ferramenta Shodan.

Os riscos associados a interfaces de login remoto podem ser associados a três principais itens presentes no ranking OWASP TOP 10: A01 - Broken Access Control, A02 - Security Misconfiguration e A03 - Software Supply Chain Failures. Os itens A01 e A02 podem ser associados a exposição da interface em si, que não deveria ser visível publicamente e é necessário um melhor controle de acesso através de uma whitelist de dispositivos ou IPs, possivelmente utilizando Proxies ou VPNs para a solução de tais problemas e o item A03 pode ser associado com a utilização de softwares obsoletos, seja de componentes ou do sistema operacional em sí.

Como foi citado anteriormente, a mera exposição de tais interfaces gera oportunidades de ataques, seja pela utilização de ataques do tipo Brute Force, enumeração de portas e serviços para exploração de outras possíveis vulnerabilidades, e em muitos casos como demonstrado na figura 61, a simples versão do sistema operacional pode ser o suficiente para que um método de ataque seja decidido.

5.4. Mitigações e prevenções recomendadas

As mitigações abaixo foram organizadas conforme as categorias do ranking OWASP Top 10 de 2025, utilizadas neste trabalho seguindo as recomendações de mitigação das vulnerabilidades e expandindo o tópico com a utilização de ferramentas reais.

Algumas medidas, como SIEM, WAF, NGFW, monitoramento de credenciais vazadas e cofres de segredos, não substituem correções estruturais, mas atuam como controles complementares para reduzir exposição, detectar abuso e limitar o impacto de uma possível exploração.

As mitigações recomendadas abaixo são uma expansão das recomendações de mitigação com a adição de ferramentas e técnicas reais para tratamento e prevenção de tais vulnerabilidades.

5.4.1. A01 - Broken Access Control

De acordo com o OWASP Top 10 Team, falhas de controle de acesso ocorrem quando usuários conseguem agir fora de suas permissões previstas ou quando não há nenhum controle de ações, se podendo acessar, modificar ou excluir dados indevidamente. A OWASP recomenda que o controle de acesso seja aplicado no lado do servidor para maior segurança e que, exceto para recursos públicos, a política adotada seja “negar por padrão” (deny by default).

No presente trabalho foi possível constatar que esta é a maior vulnerabilidade em hosts no Brasil, que expõem muitas partes criticas se sua infraestrutura sem nenhum tipo de contramedida.

Mitigações

- Aplicar o princípio do menor privilégio, garantindo que usuários, serviços, APIs e quaisquer outros dispositivos tenham seu acesso limitado a apenas aos recursos ligados a sua função.
- Utilizar política de acesso “negar por padrão”, liberando somente portas, serviços, diretórios, interfaces administrativas e APIs realmente necessários.

- Restringir interfaces administrativas, painéis de login, serviços SMB, SSH, FTP e dispositivos IoT por meio de VPN, proxy reverso, listas de IP permitidos, ACLs (access control list), grupos de segurança em nuvem ou segmentação de rede.
- Impedir que serviços internos, como SMB, bancos de dados, painéis administrativos e interfaces de gerenciamento, fiquem diretamente expostos à internet, preferencialmente substituindo o uso de protocolos obsoletos como SMB e FTP sempre que possível.
- Implementar controles de acesso centralizados e reutilizáveis, evitando que cada módulo da aplicação tenha uma lógica própria e inconsistente de autorização.
- Bloquear a exposição de diretórios, arquivos de backup, arquivos .git, metadados e listagem de diretórios em servidores web.
- Registrar falhas de autorização e gerar alertas quando houver tentativas repetidas de acesso negado, especialmente em interfaces administrativas, APIs, painéis remotos e serviços sensíveis.
- Utilizar limitação de requisições (rate limiting) para reduzir o impacto de ferramentas automatizadas, enumeração de caminhos, varreduras e abuso de APIs.
- Utilizar WAFs como controle complementar para aplicações web expostas. Exemplos: Cloudflare WAF, AWS WAF e F5 Advanced WAF.
- Utilizar firewalls e Next Generation Firewalls (NGFWs) para limitar tráfego e impedir exposição desnecessária de serviços internos. Exemplos: Fortinet FortiGate, Palo Alto Networks NGFW e Cisco Secure Firewall.
- Utilizar SIEMs para centralizar logs, correlacionar eventos e identificar tentativas de acesso indevido. Exemplos: Microsoft Sentinel, Splunk Enterprise Security e IBM QRadar SIEM.

5.4.2. A02 - Security Misconfiguration

Segundo o OWASP Top 10 Team, configurações inseguras ocorrem quando sistemas, aplicações ou serviços em nuvem são configurados de forma inadequada do ponto de vista de segurança.

Foram encontrados inúmeros hosts no Brasil contendo esta vulnerabilidade, em muitos casos não é possível identificar a extensão de tais erros de configuração mas os problemas básicos de configuração muitas vezes indicam que configurações ainda mais importantes certamente não foram feitas.

Mitigações:

- Criar um processo repetível de hardening para servidores, aplicações, bancos de dados, dispositivos IoT, serviços em nuvem e ambientes de desenvolvimento, teste e produção.
- Remover recursos desnecessários, incluindo portas abertas sem uso, serviços legados, contas padrão, páginas de teste, frameworks não utilizados, exemplos de instalação e documentação exposta. Se necessário realizar uma auditoria completa para remover Ghost ITs existentes.
- Revisar periodicamente configurações de servidores web, serviços SMB, FTP, SSH, painéis administrativos, bancos de dados, buckets de armazenamento e dispositivos IoT.
- Desabilitar credenciais padrão e trocar senhas administrativas antes da entrada do sistema em produção.
- Padronizar configurações seguras entre ambientes, evitando que produção, homologação e desenvolvimento utilizem permissões inconsistentes ou credenciais reutilizadas.
- Aplicar segmentação de rede, containers, VLANs, grupos de segurança em nuvem e ACLs, separando serviços públicos de serviços internos.
- Configurar cabeçalhos de segurança em aplicações web, como HSTS, Content Security Policy, X-Frame-Options e outros controles compatíveis com o ambiente.
- Automatizar verificações de configuração sempre que possível, utilizando ferramentas de auditoria, baseline de segurança e validação contínua de configurações.
- Utilizar credenciais temporárias, federação de identidade e mecanismos baseados em função, evitando chaves estáticas em arquivos de configuração, código-fonte ou pipelines.

- Utilizar NGFWs e firewalls para bloquear acessos indevidos a serviços que não deveriam estar publicados na internet, especialmente SMB, Telnet, FTP, bancos de dados, painéis de administração e interfaces de IoT.
- Enviar logs de configuração, autenticação e acesso para um SIEM, permitindo a identificação de alterações indevidas, falhas de login, exposição inesperada de serviços e padrões de ataque.

5.4.3. A03 - Software Supply Chain Failures

O OWASP Top 10 Team define falhas de cadeia de suprimentos de software como problemas no processo de construção, distribuição ou atualização de software, incluindo componentes de terceiros vulneráveis, desatualizados ou comprometidos.

Foi a segunda vulnerabilidade mais encontrada em hosts com ativos expostos no Brasil, mais precisamente devido ao uso de componentes ou protocolos obsoletos, muitos destes com vulnerabilidades confirmadas.

Mitigações:

- Manter um processo formal de gerenciamento de atualizações e correções de segurança, priorizando vulnerabilidades conhecidas com exploração pública ou alto impacto.
- Inventariar continuamente versões de sistemas operacionais, servidores web, bancos de dados, bibliotecas, frameworks, firmwares de IoT, plugins e dependências.
- Utilizar SBOM (Software Bill of Materials) para mapear componentes diretos e transitivos utilizados nos sistemas.
- Remover dependências, bibliotecas, componentes, arquivos, documentação e funcionalidades não utilizadas, reduzindo a superfície de ataque.
- Monitorar fontes como CVE, NVD e OSV para identificar vulnerabilidades nos componentes utilizados.
- Utilizar ferramentas de análise de dependências e componentes, como OWASP Dependency-Track, OWASP Dependency-Check e retire.js.

- Obter componentes apenas de fontes oficiais e confiáveis, preferencialmente com pacotes assinados, reduzindo o risco de bibliotecas adulteradas ou maliciosas.
- Atualizar regularmente ferramentas de desenvolvimento, IDEs, extensões, pipelines CI/CD, registries de containers, repositórios de código e servidores de build.
- Proteger repositórios e pipelines com MFA, controle de acesso, separação de funções, proteção de branches, logs imutáveis e revisão de código.
- Evitar atualização simultânea de todos os sistemas críticos; quando possível, utilizar staged rollout ou canary deployment para reduzir impacto caso uma atualização apresente falha.
- Quando a correção imediata não for possível, aplicar controles compensatórios, como virtual patching, regras de WAF, IPS/IDS e monitoramento reforçado em SIEM.
- Em dispositivos IoT, impressoras, câmeras, roteadores e equipamentos legados, manter firmware atualizado e substituir equipamentos que não recebem mais suporte do fabricante.

5.4.4. A04 - Cryptographic Failures

Conforme o OWASP Top 10 Team, falhas criptográficas envolvem ausência de criptografia, uso de algoritmos fracos, má gestão de chaves, vazamento de chaves e proteção insuficiente de dados sensíveis.

Embora seja mais difícil de se confirmar de forma passiva, a utilização de HTTP sem TLS ou SSL assim como Telnet já indica que esta falha está presente devido ao transporte de informações não ser seguro nestes hosts.

Mitigação:

- Substituir HTTP por HTTPS em sistemas web, principalmente em páginas de login, painéis administrativos, APIs e serviços que trafegam dados sensíveis.
- Utilizar TLS em versões atuais e seguras. A OWASP recomenda TLS 1.2 ou superior, com cifras adequadas e forward secrecy.

- Ativar HSTS em aplicações web, evitando downgrade de HTTPS para HTTP.
- Descontinuar protocolos inseguros ou sem criptografia, como Telnet e FTP, substituindo-os por SSH, SFTP, FTPS ou VPN, conforme a necessidade do ambiente.
- Criptografar dados sensíveis em repouso, especialmente credenciais, informações pessoais, dados de saúde, dados financeiros, segredos de negócio e informações reguladas.
- Não armazenar dados sensíveis sem necessidade. Quando possível, aplicar truncamento, tokenização ou descarte seguro.
- Utilizar algoritmos criptográficos confiáveis e implementações bem estabelecidas, evitando MD5, SHA-1, ECB, CBC inseguro e esquemas criptográficos próprios.
- Armazenar chaves sensíveis em HSM físico ou serviço HSM/KMS de nuvem, com rotação, controle de acesso e auditoria.
- Não salvar chaves criptográficas, tokens, senhas ou certificados diretamente em repositórios de código, arquivos de configuração expostos ou pipelines.
- Armazenar senhas com algoritmos próprios para hashing de senhas, como Argon2, yescrypt, scrypt ou PBKDF2-HMAC-SHA-512, conforme indicado pela OWASP.
- Utilizar certificados digitais válidos, emitidos por autoridades confiáveis, e monitorar vencimentos para evitar interrupções ou configurações inseguras de emergência.
- Em sistemas legados que não suportam criptografia adequada, priorizar substituição ou isolamento por VPN e segmentação de rede.

5.4.5. A07 - Authentication Failures

O OWASP Top 10 Team descreve falhas de autenticação como situações em que um atacante consegue fazer o sistema reconhecer um usuário inválido como legítimo.

Embora mais difícil de verificar utilizando ferramentas de observação passivas como no caso do presente trabalho, a ausência de autenticação ou a autenticação anônima em diversos serviços, muitas vezes em órgãos governamentais e empresas no Brasil é algo preocupante e deve ser corrigido o mais rápido possível.

Mitigações:

- Implementar MFA sempre que possível, especialmente em painéis administrativos, VPNs, interfaces remotas, contas privilegiadas, serviços de nuvem e sistemas críticos.
- Remover credenciais padrão de qualquer aplicação, servidor, banco de dados, roteador, câmera, impressora, dispositivo IoT ou serviço administrativo antes de sua exposição em rede.
- Bloquear senhas fracas, previsíveis ou presentes em listas comuns, como “admin”, “123456”, “password” e variações simples.
- Validar novas senhas e alterações de senha contra listas de credenciais vazadas. A OWASP cita o uso de bases como Have I Been Pwned para esse tipo de verificação.
- Incentivar ou exigir o uso de gerenciadores de senha, reduzindo reutilização de credenciais e uso de senhas fracas.
- Evitar políticas antigas de troca periódica obrigatória de senha sem evidência de comprometimento. A OWASP recomenda alinhar políticas de senha às diretrizes modernas do NIST SP 800-63B.
- Implementar bloqueio progressivo, atraso incremental ou limitação de tentativas de login, tomando cuidado para não criar negação de serviço contra usuários legítimos.
- Registrar falhas de login e gerar alertas quando houver indícios de força bruta, password spraying, credential stuffing ou enumeração de usuários.
- Evitar mensagens de erro que permitam enumeração de contas. Respostas como “usuário não encontrado” e “senha incorreta” devem ser substituídas por mensagens genéricas, como “usuário ou senha inválidos”.
- Utilizar gerenciamento de sessão seguro, com identificadores aleatórios, alta entropia, cookies seguros, invalidação após logout e expiração por inatividade.

- Armazenar segredos, tokens de API, chaves SSH, credenciais de banco de dados e certificados em cofres de segredos, e não em arquivos de configuração, scripts ou repositórios.
- Centralizar armazenamento, provisionamento, auditoria, rotação e gestão de segredos utilizando soluções próprias para secret management.
- Monitorar credenciais vazadas associadas aos domínios da organização e forçar redefinição de senha quando houver indício de comprometimento.
- Utilizar WAFs e regras de limitação de taxa em endpoints de autenticação, reduzindo a viabilidade de ataques automatizados contra páginas de login.
- Utilizar SIEMs como Microsoft Sentinel, Splunk Enterprise Security ou IBM QRadar SIEM para correlacionar eventos de autenticação, detectar padrões de ataque e apoiar resposta a incidentes.

5.5. Medidas complementares para protocolos e ativos expostos analisados

Devido ao volume de uso de protocolos obsoletos e problemático, migrações e ações adicionais são necessárias para sanar problemas que muitas vezes são características do próprio protocolo e não são sanáveis por meio de configurações adicionais ou atualizações periódicas.

HTTP:

- Migrar HTTP para HTTPS, principalmente em páginas de login, APIs, painéis administrativos e sistemas que trafegam dados sensíveis.
- Aplicar TLS 1.2 ou superior, configurar HSTS e remover suporte a algoritmos criptográficos fracos.
- Utilizar WAF para reduzir ataques automatizados contra aplicações web expostas.
- Atualizar servidores web, frameworks, CMS, plugins e bibliotecas.
- Restringir interfaces administrativas por VPN, proxy autenticado, whitelist de IP ou rede interna.

SMB:

- Não expor SMB diretamente à internet.

- Restringir acesso por VPN, firewall, ACL ou rede interna
- Desabilitar autenticação anônima.
- Aplicar atualizações de segurança, principalmente em hosts Windows vulneráveis.
- Bloquear portas 445 e 139 quando não houver necessidade de exposição.
- Monitorar tentativas de acesso SMB por logs e SIEM.

FTP:

- Substituir FTP por SFTP ou FTPS.
- Desativar login anônimo.
- Restringir acesso por IP, VPN ou rede interna.
- Remover servidores FTP sem manutenção.
- Monitorar tentativas de autenticação, upload indevido e acesso a diretórios sensíveis.

Telnet:

- Substituir Telnet por SSH.
- Quando a substituição não for possível, limitar o uso a redes internas isoladas.
- Impedir exposição direta à internet.
- Utilizar VPN e regras rígidas de firewall para qualquer acesso remoto.
- Substituir equipamentos legados que dependam exclusivamente de Telnet quando houver alternativa viável.

SSH:

- Manter o serviço SSH atualizado.
- Desabilitar login direto de root.
- Usar autenticação por chaves em vez de senhas sempre que possível.
- Aplicar MFA em ambientes críticos.
- Restringir acesso por IP, VPN ou bastion host.
- Monitorar tentativas de força bruta, password spraying e acessos fora do padrão.

IoT:

- Trocar credenciais padrão.
- Atualizar firmware.
- Desabilitar serviços desnecessários, como Telnet, FTP, UPnP e interfaces administrativas públicas.
- Impedir exposição direta à internet.
- Segmentar a rede de IoT, separando câmeras, impressoras, sensores e dispositivos administrativos de redes corporativas sensíveis.
- Restringir acesso a câmeras, impressoras e sensores somente a usuários e dispositivos autorizados.
- Substituir dispositivos sem suporte ou sem atualização de segurança.

Interfaces de login:

- Remover exposição pública sempre que possível.
- Exigir VPN, proxy autenticado ou solução de acesso remoto segura.
- Aplicar MFA.
- Implementar limitação de tentativas de login.
- Monitorar credenciais vazadas.
- Bloquear senhas fracas e reutilizadas.
- Registrar e analisar falhas de autenticação em SIEM.
- Evitar mensagens que permitam enumeração de usuários.

Ativos críticos:

- Priorizar correção por criticidade, principalmente em órgãos públicos, instituições acadêmicas, tribunais, empresas de energia, segurança pública e serviços essenciais.
- Criar inventário contínuo de ativos expostos.
- Reduzir a superfície de ataque por meio de firewall, NGFW, VPN, segmentação de rede e remoção de serviços desnecessários.
- Corrigir vulnerabilidades antigas com exploração pública conhecida.
- Enviar logs de autenticação, rede, aplicação e sistema operacional para SIEM.
- Criar alertas para exposição inesperada de portas, falhas repetidas de login, uso de credenciais vazadas e alterações de configuração.

- Estabelecer rotina formal de atualização, revisão de configuração e resposta a incidentes.

6. CONSIDERAÇÕES FINAIS

Os objetivos estabelecidos no início do trabalho foram plenamente atingidos, a análise de exposição de ativos no Brasil e exame cruzado utilizando dados quantitativos de múltiplas plataformas e as possíveis explorações permitiu alcançar resultados amplos e significativos, tanto do ponto de vista técnico quanto acadêmico.

Foi possível demonstrar de forma quantitativa o nível de exposição de ativos no Brasil, demonstrando também os índices de possíveis vulnerabilidades de muitos dos principais ativos e o impacto que poderiam ter caso explorados. A correlação com o ranking OWASP TOP 10 foi utilizado como uma referência solida para uma avaliação que prioriza vulnerabilidades mais importantes e comuns, mantendo o foco do trabalho em dados observáveis.

É importante notar que o número de ativos encontrados por cada plataforma varia regularmente e que a variação de valores entre elas se dá devido aos métodos utilizados e objetivos de cada plataforma, mas na maioria dos casos, a proporção de ativos encontrados as vulnerabilidades dos hosts e as vulnerabilidades encontradas se mantiveram relativamente estáveis dado às variações drásticas de coleta dos dados.

Foi possível constatar que das vulnerabilidades abordadas pelo presente trabalho, as mais prevalentes em sistemas no Brasil estão ligadas aos itens A03, A04, A01, A02 e A07 respectivamente. Tendo em vista que mais de 50% dos problemas de todos os ativos detectados no Brasil seriam mitigados ou completamente solucionados caso houvesse atualizações periódicas e utilização de protocolos e softwares mais modernos ao invés da utilização atual que em sua maioria consiste de tecnologias obsoletas.

Finalmente, foi possível observar que infelizmente um número alarmante de instituições de grande importância possuem ativos expostos e muitos possuem vulnerabilidades, revelando um risco real à segurança nacional e que devem ser tratados o mais rápido possível.

REFERENCIAS

Open Worldwide Application Security Project. **OWASP Top 10:2025**. 2025. Disponível em: https://owasp.org/Top10/2025/. Acesso em: 10 mar. 2026.

National Institute of Standards and Technology. **NIST SP 800-30 Rev.1**. 2012. Disponivel em: https://doi.org/10.6028/NIST.SP.800-30r1. Acesso em: 19 mar. 2026.

National Institute of Standards and Technology. **Vulnerability Metrics.** 2024. Disponivel em: https://nvd.nist.gov/vuln-metrics/cvss. Acesso em: 19 mar. 2026.

Forum of Incident Response and Security Teams. **Common Vulnerability Scoring System Version 4.0.** 2026. Disponivem em: https://www.first.org/cvss/v4.0/. Acesso em: 19 mar. 2026.

National Institute of Standards and Technology. **NIST SP 1800-26A.** 2020. Disponivem em: https://doi.org/10.6028/NIST.SP.1800-26. Acesso em: 19 mar. 2026.

Blacksmith InfoSec. **Understanding the CIA Triad in Cybersecurity and MSP Compliance**. 2025. Disponivel em: https://blacksmithinfosec.com/understanding-the-cia-triad-in-cybersecurity-and-msp-compliance/. Acesso em: 19 mar. 2026.

Lumos. **CIA Triad: Definition, Importance, and Examples**. 2025. Disponível em: https://www.lumos.com/topic/cia-triad. Acesso em: 19 mar. 2026.

United States Government Accountability Office. **WEAPON SYSTEMS CYBERSECURITY DOD Just Beginning to Grapple with Scale of Vulnerabilities**. 2018. Disponível em: https://www.gao.gov/assets/gao-19-128.pdf. Acesso em: 19 mar. 2026.

National Institute of Standards and Technology. **NIST SP 800-53 Rev5**. 2020. Disponivel em: https://doi.org/10.6028/NIST.SP.800-53r5. Acesso em: 19 mar. 2026.

OWASP. **Attack Surface Analysis Cheat Sheet**. 2026. Disponivel em: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html. Acesso em: 19 mar. 2026.

Cornell University. **arXiv:2308.09019 - Smart Bulbs can be Hacked to Hack into your Household**. 2023. Disponivel em: https://doi.org/10.48550/arXiv.2308.09019. Acesso em: 19 mar. 2026

The Verge. **The DJI Romo robovac had security so poor, this man remotely accessed thousands of them.** 2026. Disponivel em: https://www.theverge.com/tech/879088/dji-romo-hack-vulnerability-remote-control-camera-access-mqtt. Acesso em: 19 mar. 2026.

Techspot. **A developer accidentally gained control of more than 10,000 DJI devices.** 2026. https://www.techspot.com/news/111443-developer-accidentally-gained-control-more-than-10000-dji.html. Acesso em: 19 mar. 2026.

Cloudflare. **What is an attack surface?**. 2025. Disponível em: https://www.cloudflare.com/learning/security/what-is-an-attack-surface/. Acesso em: 19 mar. 2026.

FortifyData. **What is an External Attack Surface and Why It Matters**. 2025. Disponível em: https://fortifydata.com/blog/what-is-an-external-attack-surface/. Acesso em: 20 mar. 2026.

Fortinet. **What Is A DMZ Network?**. 2025. Disponivel em: https://www.fortinet.com/resources/cyberglossary/what-is-dmz. Acesso em: 20 mar. 2026.

Paloalto Networks. **What is Zero Trust Architecture (ZTA)?**. 2025. Disponivel em: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture. Acesso em: 20 mar. 2026.

National Institute of Standards and Technology. **NIST SP 800-77 Rev. 1.** 2020. Disponível em: https://doi.org/10.6028/NIST.SP.800-77r1. Acesso em: 20 mar. 2026.

Hong Kong Computer Emergency Response Team. **Personal VPN Security Guideline.** 2020. Disponível em: https://www.hkcert.org/security-guideline/personal-vpn-security-guideline. Acesso em: 20 mar. 2026.

National Cyber Security Centre. **External attack surface management (EASM) buyer's guide.** 2025. Disponível em: https://www.ncsc.gov.uk/guidance/external-attack-surface-management-buyers-guide. Acesso em: 20 mar. 2026.

IBM. **What is shadow IT?.** Disponível em: https://www.ibm.com/think/topics/shadow-it. Acesso em: 23 mar. 2026.

Port Swigger. **Insecure direct object references (IDOR).** Disponivel em: https://portswigger.net/web-security/access-control/idor. Acesso em: 24 mar. 2026.

Shodan. **What is Shodan?.** Disponivel em: https://help.shodan.io/the-basics/what-is-shodan. Acesso em: 25 mar. 2026.

Censys. **What is Censys?**.Disponível em: https://about.censys.io/. Acesso em: 25 mar. 2026.

Netlas. **Netlas vs Shodan: Platforms Comparison.** 2024. Disponível em: https://netlas.io/blog/netlas_vs_shodan/. Acesso em: 25 mar. 2026.

Censys. **State Of The Internet Report**. 2023. Disponivel em: https://go.censys.io/rs/120-HWT-117/images/2023StateoftheInternetReport.pdf. Acesso em: 25 mar. 2026.

Censys. **State Of The Internet Report**. 2025. Disponivel em: https://50081908.fs1.hubspotusercontent-

na1.net/hubfs/50081908/Reports/2025%20SOTIR_250919.pdf. Acesso em: 25 mar. 2026.

Security Week. **8,000 New WordPress Vulnerabilities Reported in 2024.** 2025**.** Disponivel em: https://www.securityweek.com/8000-new-wordpress-vulnerabilities-reported-in-2024/. Acesso em: 25 mar. 2026.

Kaspersky Daily. **Vulnerabilities in WordPress themes and plugins: how to protect your site.** 2025. Disponivel em: https://www.kaspersky.com/blog/vulnerable-wordpress-plugins-and-themes/54228/. Acesso em: 25 mar. 2026.

National Institute of Standards and Technology. **NIST SP 800-175B.** 2020. Disponível em: https://doi.org/10.6028/NIST.SP.800-175Br1. Acesso em: 25 mar. 2026.

National Institute of Standards and Technology. **NIST SP 800-38A.** 2001. Disponível em: https://doi.org/10.6028/NIST.SP.800-38A. Acesso em: 07 abr. 2026.

Twingate. **Vastaamo Data Breach: What & How It Happened?.** 2024. Disponível em: https://www.twingate.com/blog/tips/Vastaamo-data-breach. Acesso em: 07 abr. 2026.

Wikipedia. **Vastaamo Data Breach**. Disponível em: https://en.wikipedia.org/wiki/Vastaamo_data_breach. Acesso em: 07 abr. 2026.

WorldFence. **GoDaddy Breached – Plaintext Passwords – 1.2M Affected.** 2021. Disponível em: https://www.wordfence.com/blog/2021/11/godaddy-breach-plaintext-passwords. Acesso em: 07 abr. 2026.

Malwarebytes. **Facebook and Instagram passwords were stored in plaintext, Meta fined.** 2024. Disponível em: https://www.malwarebytes.com/blog/news/2024/10/facebook-and-instagram-passwords-were-stored-in-plaintext-meta-fined. Acesso em: 07 abr. 2026.

Data Protection Commission. **Inquiry into Meta Platforms Ireland Limited.** 2024. Disponível em: https://www.dataprotection.ie/en/dpc-guidance/law/decisions-made-under-data-protection-act-2018/inquiry-into-meta-platforms-ireland-limited-september-2024. Acesso em: 07 abr. 2026.

National Institute of Standards and Technology. **NIST SP 800-63B-4.** 2025. Disponível em: https://doi.org/10.6028/NIST.SP.800-63b-4. Acesso em: 14 abr. 2026.

Uber Blog. **Security Update**. 2022. Disponivel em: https://www.uber.com/pt/en/newsroom/security-update/. Acesso em: 14 abr. 2026.

23andMe blog. **Addressing Data Security Concerns – Action Plan**. 2023. Disponivel em: https://blog.23andme.com/articles/addressing-data-security-concerns. Acesso em: 14 abr. 2026.

Upguard. **What Caused the Uber Data Breach in 2022?.** 2025. Disponivel em: https://www.upguard.com/blog/what-caused-the-uber-data-breach. Acesso em: 14 abr. 2026.

The HIPAA journal. **6.9 Million 23andMe Users Affected by Data Breach.** 2023. Disponível em: https://www.hipaajournal.com/6-9-million-23andme-users-affected-by-data-breach/**.** Acesso em: 14 abr. 2026.

The Guardian. **DNA testing firm 23andMe fined £2.3m by UK regulator for 2023 data Hack**. 2025. Disponível em: https://www.theguardian.com/technology/2025/jun/17/dna-testing-firm-23andme-fined-23m-by-uk-regulator-for-2023-data-hack. Acesso em: 14 abr. 2026.

IBM. **What is open source intelligence (OSINT)?**. Disponível em: https://www.ibm.com/think/topics/osint. Acesso em: 15 abr. 2026.

Exploit Database. **About The Exploit Database**. Disponível em: https://www.exploit-db.com/about-exploit-db. Acesso em: 16 abr. 2026.

National Vulnerability Database. **NVD Home**. Disponível em: https://nvd.nist.gov/. Acesso em: 17 abr. 2026.

Exploit Database. **Exploit Database Submissions Guidelines**. Disponível em: https://www.exploit-db.com/submit. Acesso em: 17 abr. 2026.

National Vulnerability Database. **CVE-2020-0796 Detail.** 2020. Disponível em: https://nvd.nist.gov/vuln/detail/cve-2020-0796. Acesso em: 13 mai. 2026.

Tech Radar. **50,000 printers hacked to promote YouTuber.** 2018. Disponível em: https://www.techradar.com/news/50000-printers-hacked-to-promote-youtuber. Acesso em: 17 mai. 2026.

Check Point. **IoT Botnet**. Disponível em: https://www.checkpoint.com/cyber-hub/network-security/what-is-iot/iot-botnet/. Acesso em: 17 mai. 2026.

The Hacker News. **DoJ Disrupts 3 Million-Device IoT Botnets Behind Record 31.4 Tbps Global DDoS Attacks.** 2026. https://thehackernews.com/2026/03/doj-disrupts-3-million-device-iot.html. Acesso em: 17 mai. 2026.