Relatório de Reconhecimento - ReconX

Alvo: ex.tv.br

Data da Análise: 2025-07-08

Análise da IA (Gemini)

Análise Técnica do Relatório de Pentest

Este relatório apresenta uma análise técnica das informações coletadas por meio de ferramentas de pentest, como Nmap, WhatWeb e Amass, direcionadas ao domínio `ex.tv.br`. O objetivo é identificar possíveis vulnerabilidades e fornecer uma avaliação da postura de segurança do alvo.

1. Nmap (Mapeamento de Portas e Serviços)

* **Visão Geral:** O Nmap foi utilizado para identificar portas abertas, os serviços em execução e, possivelmente, o sistema operacional do servidor.
* **Resultados:**
  * **Portas Abertas:** 80 (HTTP), 82 (desconhecida), 443 (HTTPS), 445 (microsoft-ds?)
    * A presença da porta 80 e 443 indica que o site está acessível via HTTP e HTTPS.
    * A porta 445, geralmente associada ao SMB (Server Message Block), é potencialmente preocupante e requer investigação adicional, a principio pode indicar um compartilhamento de arquivos ativo.
    * A porta 82 não foi identificada.
  * **Porta Filtrada:** 3389 (ms-wbt-server)
    * A porta 3389 filtrada sugere que o RDP (Remote Desktop Protocol) pode estar sendo usado, mas está protegido por um firewall.
  * **Serviço Desconhecido:** O Nmap não conseguiu identificar os serviços nas portas 80 e 443 com precisão, apesar de receber dados. Os fingerprints gerados podem ser submetidos ao Nmap para melhorar a identificação futura. No entanto, a resposta HTTP 403 Forbidden indica que um servidor web está respondendo, mas o acesso está restrito.
  * **Detecção de SO:** O Nmap tentou adivinhar o sistema operacional, com maior probabilidade para F5 BIG-IP Local Traffic Manager load balancer (TMOS 11.6) e OpenBSD. Isso sugere o uso de um balanceador de carga e/ou firewall, o que é uma boa prática de segurança.
* **Implicações e Recomendações:**
  * **Porta 445:** Investigar a necessidade e a configuração da porta 445. Se não for essencial, considerar fechá-la para mitigar riscos associados a vulnerabilidades SMB.
  * **Serviços Desconhecidos:** Analisar as respostas HTTP 403 Forbidden para entender as restrições de acesso e garantir que estejam configuradas corretamente.
    * **Detecção de SO:** A detecção imprecisa do sistema operacional pode dificultar a identificação de vulnerabilidades específicas. É importante identificar o sistema operacional correto para uma avaliação de vulnerabilidades mais precisa.
  * **Firewall:** A porta 3389 filtrada indica que o acesso RDP está sendo controlado por um firewall. Revisar as regras do firewall para garantir que o acesso seja restrito apenas a fontes confiáveis.

2. WhatWeb (Identificação de Tecnologias Web)

* **Visão Geral:** O WhatWeb identifica as tecnologias utilizadas no site, como servidores web, frameworks, linguagens de programação e sistemas de gerenciamento de conteúdo (CMS).
* **Resultados:**

* **Redirecionamento:** O site redireciona de HTTP para HTTPS e, em seguida, para `https://www.ex.tv.br/`, indicando uma configuração de segurança para forçar o uso de HTTPS.
* **Servidor Web:** O servidor web é identificado como "Pepyaka", o que pode ser uma configuração personalizada ou um proxy/CDN que ofusca o servidor real.
* **Tecnologias:** O site utiliza HTML5, JavaScript, e é construído com o Wix.com Website Builder.
* **Cookies:** Uso de cookies `ssr-caching`.
* **Cabeçalhos de Segurança:** O cabeçalho `Strict-Transport-Security` (HSTS) está configurado com `max-age=86400`, o que ajuda a proteger contra ataques Man-in-the-Middle (MitM).
* **Emails:** Encontrou diversos emails de `sentry.wixpress.com`

* **Implicações e Recomendações:**
* **Servidor Web:** Investigar a identidade do servidor "Pepyaka" para entender sua configuração e possíveis vulnerabilidades.
* **Wix.com:** Estar ciente das considerações de segurança específicas para sites construídos no Wix. O Wix gerencia grande parte da infraestrutura, mas ainda é importante configurar corretamente as opções de segurança oferecidas.
* **HSTS:** O HSTS está habilitado, o que é uma boa prática. Considerar aumentar o valor de `max-age` para um período mais longo (por exemplo, um ano) para melhorar a proteção a longo prazo.
* **Cookies:** Validar o uso de `ssr-caching` nos cookies, para entender melhor como o cache esta sendo utilizado.
* **Emails:** Investigar o motivo dos emails nos metadados, pois pode ser um vazamento de informação.

3. Amass (Enumeração de Subdomínios e Ativos)

* **Visão Geral:** O Amass é usado para descobrir subdomínios, endereços IP associados e outras informações relevantes sobre a infraestrutura do domínio.
* **Resultados:**
* **Subdomínios:** Identificou subdomínios como `pt.ex.tv.br`, `en.ex.tv.br`, `es.ex.tv.br` e `www.ex.tv.br`, indicando versões do site em diferentes idiomas.
* **Servidores DNS:** Utiliza servidores DNS da Wix (`ns4.wixdns.net` e `ns5.wixdns.net`).
* **Servidores MX:** Utiliza servidores MX do Google para gerenciamento de e-mail.
* **Endereços IP:** Aponta para os endereços IP 185.230.63.186, 185.230.63.107 e 185.230.63.171.
* **CDN:** Os subdomínios e `www` utilizam um CDN (`cdn1.wixdns.net`).
* **Implicações e Recomendações:**
* **Subdomínios:** Avaliar a segurança de todos os subdomínios identificados, pois cada um representa uma superfície de ataque potencial.
* **Servidores DNS/MX:** A utilização de serviços DNS e MX de terceiros (Wix e Google) é comum e geralmente segura, desde que as configurações estejam corretas.
* **CDN:** A utilização de um CDN ajuda a proteger o site contra ataques DDoS e melhora o desempenho. Verificar a configuração do CDN para garantir que esteja otimizado para segurança.

4. Análise Geral e Conclusões

* **Postura de Segurança:** A postura de segurança geral do domínio `ex.tv.br` parece razoável, com a utilização de HTTPS, HSTS e um CDN. No entanto, a porta 445 aberta e a identificação imprecisa do servidor web requerem investigação adicional.
* **Vulnerabilidades Potenciais:**
* **Porta 445:** Se a porta 445 não for necessária, fechá-la é a melhor opção. Caso contrário, garantir que esteja devidamente protegida e atualizada contra vulnerabilidades SMB.
* **"Pepyaka":** Identificar o servidor web real por trás de "Pepyaka" e verificar se há vulnerabilidades conhecidas.
* **Subdomínios:** Garantir que todos os subdomínios estejam atualizados e protegidos contra vulnerabilidades.

* **Recomendações:**
  1. Realizar uma análise de vulnerabilidades mais aprofundada nas portas abertas e nos serviços em execução.
  2. Investigar a configuração e a necessidade da porta 445.
  3. Identificar o servidor web real por trás de "Pepyaka" e aplicar as atualizações de segurança necessárias.
  4. Revisar e fortalecer a configuração de segurança do Wix.com.
  5. Monitorar continuamente a superfície de ataque para detectar novas vulnerabilidades e ameaças.
  6. Validar o uso do `ssr-caching` dos cookies.
  7. Investigar o motivo dos emails nos metadados

Observações Finais:

Este relatório fornece uma análise inicial da postura de segurança do domínio `ex.tv.br`. É fundamental realizar testes mais abrangentes e específicos para identificar e corrigir vulnerabilidades com precisão. A segurança deve ser uma preocupação contínua, com monitoramento regular e atualizações de segurança implementadas prontamente.

Resultados do Módulo: NMAP

Starting Nmap 7.95 (https://nmap.org) at 2025-07-08 15:33 CDT
Nmap scan report for ex.tv.br (185.230.63.171)
Host is up (0.087s latency).
Other addresses for ex.tv.br (not scanned): 185.230.63.186 185.230.63.107
rDNS record for 185.230.63.171: unalocated.63.wixsite.com
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http
82/tcp open xfer?
443/tcp open ssl/https Pepyaka
445/tcp open microsoft-ds?
3389/tcp filtered ms-wbt-server
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.95%I=7%D=7/8%Time=686D808D%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,79,"HTTP/1\.0\x20403\x20Forbidden\r\nX-Seen-By:\x20pmHZlB45NPy7b1
SF:VBAukQrewfbs\+7qUVAqsIx00yI78k=\r\nConnection:\x20close\r\nContent-Leng
SF:th:\x200\r\n\r\n")%r(HTTPOptions,79,"HTTP/1\.0\x20403\x20Forbidden\r\nX
SF:-Seen-By:\x20AHc3TXLcXOul\+t9LIbGg9ciHE4dbw\+wewoJ5nvKoyjE=\r\nConnecti
SF:on:\x20close\r\nContent-Length:\x200\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.95%T=SSL%I=7%D=7/8%Time=686D8096%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,79,"HTTP/1\.0\x20403\x20Forbidden\r\nX-Seen-By:\x20AHc3TXL
SF:cXOul\+t9LIbGg9ciHE4dbw\+wewoJ5nvKoyjE=\r\nConnection:\x20close\r\nCont
SF:ent-Length:\x200\r\n\r\n")%r(HTTPOptions,79,"HTTP/1\.0\x20403\x20Forbid
SF:den\r\nX-Seen-By:\x20VtqAe8Wu9wvSsl49B/X4\+ewfbs\+7qUVAqsIx00yI78k=\r\n
SF:Connection:\x20close\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequ
SF:est,79,"HTTP/1\.0\x20403\x20Forbidden\r\nX-Seen-By:\x20VtqAe8Wu9wvSsl49
SF:B/X4\+ewfbs\+7qUVAqsIx00yI78k=\r\nConnection:\x20close\r\nContent-Lengt
SF:h:\x200\r\n\r\n")%r(RTSPRequest,79,"HTTP/1\.0\x20403\x20Forbidden\r\nX-

Relatório de Reconhecimento - ReconX

SF:Seen-By:\x20jKB0KR2wTEE1MYSdxvKSbciHE4dbw\+wewoJ5nvKoyjE=\r\nConnection
SF::\x20close\r\nContent-Length:\x200\r\n\r\n");
Device type: load balancer|general purpose|firewall
Running (JUST GUESSING): F5 Networks TMOS 11.6.X|11.4.X (91%), OpenBSD 5.X|4.X|6.X|3.X|7.X (90%), FreeBSD 7.X (85%)
OS CPE: cpe:/o:f5:tmos:11.6 cpe:/o:openbsd:openbsd:5.8 cpe:/o:f5:tmos:11.4 cpe:/o:openbsd:openbsd:4.4 cpe:/o:openbsd:openbsd:6 cpe:/o:openbsd:openbsd:3.9 cpe:/o:openbsd:openbsd:7.1 cpe:/o:freebsd:freebsd:7.0
Aggressive OS guesses: F5 BIG-IP Local Traffic Manager load balancer (TMOS 11.6) (91%), OpenBSD 5.8 (90%), F5 BIG-IP AFM firewall (89%), OpenBSD 4.4 - 4.5 (87%), OpenBSD 4.5 (87%), OpenBSD 6.0 - 6.4 (87%), OpenBSD 6.1 (87%), OpenBSD 3.9 (87%), OpenBSD 4.0 (87%), OpenBSD 4.2 - 4.4 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.68 seconds

Resultados do Módulo: WhatWeb

[1m [34mhttp://ex.tv.br [0m [301 Moved Permanently] [1mIP [0m[[0m [22m185.230.63.107 [0m], [1mRedirectLocation [0m[[0m [22mhttps://ex.tv.br/ [0m], [1mUncommonHeaders [0m[[0m [22mx-seen-by [0m]
[1m [34mhttps://ex.tv.br/ [0m [301 Moved Permanently] [1mHTTPServer [0m[[1m [36mPepyaka [0m], [1mIP [0m[[0m [22m185.230.63.186 [0m], [1mRedirectLocation [0m[[0m [22mhttps://www.ex.tv.br/ [0m], [1mStrict-Transport-Security [0m[[0m [22mmax-age=86400 [0m],
[1mUncommonHeaders [0m[[0m [22mx-wix-cache-control,x-wix-request-id,server-timing,x-seen-by,x-content-type-options [0m]
[1m [34mhttps://www.ex.tv.br/ [0m [200 OK] [1mContent-Language [0m[[0m [22mpt-BR [0m], [1mCookies [0m[[0m [22mssr-caching [0m], [1mCountry [0m[[0m [22mUNITED STATES [0m][[1m [31mUS [0m], [1mEmail [0m[[0m [22m2062d0a4929b45348643784b5cb39c36@sentry.wixpress.com,271e9fa3230b4eec94b02bf95780f5f2@sentry.wixpress.com,460ff4620fa44cba8df530afde949785@sentry.wixpress.com,605a7baede844d278b89dc95ae0a9123@sentry-next.wixpress.com,8eb368c655b84e029ed79ad7a5c1718e@sentry.wixpress.com,bcea6319e2dd4b1aaecfde5bec98f9ed@sentry.wixpress.com,ed436f5053144538958ad06a5005e99a@sentry.wixpress.com [0m], [1mHTML5 [0m, [1mHTTPServer [0m[[1m [36mPepyaka [0m], [1mIP [0m[[0m [22m34.149.87.45 [0m], [1mMetaGenerator [0m[[0m [22mWix.com Website Builder [0m], [1mOpen-Graph-Protocol [0m[[1m [32mwebsite [0m][[1m [36makeloficial [0m],
[1mScript [0m[[0m [22mapplication/json,application/ld+json,text/javascript,wix/htmlEmbeds [0m],
[1mStrict-Transport-Security [0m[[0m [22mmax-age=86400 [0m], [1mTitle [0m[[1m [33mAKEL | Filosofia X [0m], [1mUncommonHeaders [0m[[0m [22mlink,html-cacheable,x-content-type-options,x-served-by,server-timing,x-wix-request-id,x-seen-by,glb-x-seen-by,alt-svc [0m], [1mVia-Proxy [0m[[0m [22m1.1 google [0m], [1mX-UA-Compatible [0m[[0m [22mIE=edge [0m]

Resultados do Módulo: AMASS

ex.tv.br (FQDN) --> ns_record --> ns5.wixdns.net (FQDN)
ex.tv.br (FQDN) --> ns_record --> ns4.wixdns.net (FQDN)
ex.tv.br (FQDN) --> mx_record --> alt4.aspmx.l.google.com (FQDN)
ex.tv.br (FQDN) --> mx_record --> alt1.aspmx.l.google.com (FQDN)
ex.tv.br (FQDN) --> mx_record --> alt2.aspmx.l.google.com (FQDN)

Relatório de Reconhecimento - ReconX

ex.tv.br (FQDN) --> mx_record --> aspmx.l.google.com (FQDN)
ex.tv.br (FQDN) --> mx_record --> alt3.aspmx.l.google.com (FQDN)
ex.tv.br (FQDN) --> node --> pt.ex.tv.br (FQDN)
ex.tv.br (FQDN) --> node --> en.ex.tv.br (FQDN)
ex.tv.br (FQDN) --> node --> es.ex.tv.br (FQDN)
pt.ex.tv.br (FQDN) --> cname_record --> cdn1.wixdns.net (FQDN)
en.ex.tv.br (FQDN) --> cname_record --> cdn1.wixdns.net (FQDN)
es.ex.tv.br (FQDN) --> cname_record --> cdn1.wixdns.net (FQDN)
ex.tv.br (FQDN) --> a_record --> 185.230.63.186 (IPAddress)
ex.tv.br (FQDN) --> a_record --> 185.230.63.107 (IPAddress)
ex.tv.br (FQDN) --> a_record --> 185.230.63.171 (IPAddress)
ex.tv.br (FQDN) --> node --> www.ex.tv.br (FQDN)
ns5.wixdns.net (FQDN) --> a_record --> 216.239.38.101 (IPAddress)
ns4.wixdns.net (FQDN) --> a_record --> 216.239.36.101 (IPAddress)
www.ex.tv.br (FQDN) --> cname_record --> cdn1.wixdns.net (FQDN)
alt4.aspmx.l.google.com (FQDN) --> aaaa_record --> 2a00:1450:4025:c01::1a (IPAddress)
alt4.aspmx.l.google.com (FQDN) --> a_record --> 142.250.147.27 (IPAddress)
alt1.aspmx.l.google.com (FQDN) --> a_record --> 173.194.76.27 (IPAddress)
alt1.aspmx.l.google.com (FQDN) --> aaaa_record --> 2a00:1450:400c:c00::1a (IPAddress)
alt2.aspmx.l.google.com (FQDN) --> a_record --> 142.250.102.26 (IPAddress)
alt2.aspmx.l.google.com (FQDN) --> aaaa_record --> 2a00:1450:4025:402::1a (IPAddress)
aspmx.l.google.com (FQDN) --> aaaa_record --> 2800:3f0:4003:c00::1b (IPAddress)
aspmx.l.google.com (FQDN) --> a_record --> 142.251.0.27 (IPAddress)
alt3.aspmx.l.google.com (FQDN) --> a_record --> 192.178.156.26 (IPAddress)
alt3.aspmx.l.google.com (FQDN) --> aaaa_record --> 2a00:1450:4013:c1c::1b (IPAddress)
216.239.32.0/20 (Netblock) --> contains --> 216.239.38.101 (IPAddress)
216.239.32.0/20 (Netblock) --> contains --> 216.239.36.101 (IPAddress)
185.230.60.0/22 (Netblock) --> contains --> 185.230.63.186 (IPAddress)
185.230.60.0/22 (Netblock) --> contains --> 185.230.63.107 (IPAddress)
185.230.60.0/22 (Netblock) --> contains --> 185.230.63.171 (IPAddress)
142.250.146.0/23 (Netblock) --> contains --> 142.250.147.27 (IPAddress)
192.178.0.0/15 (Netblock) --> contains --> 192.178.156.26 (IPAddress)
15169 (ASN) --> managed_by --> GOOGLE - Google LLC (RIROrganization)
15169 (ASN) --> announces --> 216.239.32.0/20 (Netblock)
15169 (ASN) --> announces --> 142.250.146.0/23 (Netblock)
15169 (ASN) --> announces --> 192.178.0.0/15 (Netblock)
58182 (ASN) --> managed_by --> WIX_COM (RIROrganization)
58182 (ASN) --> announces --> 185.230.60.0/22 (Netblock)
2800:3f0:4003::/48 (Netblock) --> contains --> 2800:3f0:4003:c00::1b (IPAddress)
142.250.102.0/24 (Netblock) --> contains --> 142.250.102.26 (IPAddress)
2a00:1450::/32 (Netblock) --> contains --> 2a00:1450:4025:c01::1a (IPAddress)
2a00:1450::/32 (Netblock) --> contains --> 2a00:1450:4025:402::1a (IPAddress)
2a00:1450::/32 (Netblock) --> contains --> 2a00:1450:400c:c00::1a (IPAddress)
2a00:1450::/32 (Netblock) --> contains --> 2a00:1450:4013:c1c::1b (IPAddress)
142.251.0.0/24 (Netblock) --> contains --> 142.251.0.27 (IPAddress)
15169 (ASN) --> announces --> 2800:3f0:4003::/48 (Netblock)
15169 (ASN) --> announces --> 142.250.102.0/24 (Netblock)
15169 (ASN) --> announces --> 2a00:1450::/32 (Netblock)
15169 (ASN) --> announces --> 142.251.0.0/24 (Netblock)