RELATÓRIO DE RECONHECIMENTO RECONX

ALVO DE RECONHECIMENTO: 192.168.18.1

Data da Análise: 14/07/2025

ANÁLISE DE INTELIGÊNCIA ARTIFICIAL (RECONX)

Análise Técnica do Relatório de Pentest

Este relatório apresenta os resultados de um pentest básico realizado em um dispositivo na rede 192.168.18.0/24, especificamente no endereço 192.168.18.1. As ferramentas utilizadas foram Nmap, WhatWeb e Amass.

1. Nmap (Mapeamento de Portas e Serviços):

* **Resumo:** O Nmap revela que o host 192.168.18.1 está ativo e responde em menos de 8ms. Detectou algumas portas abertas e filtradas. A detecção de sistema operacional sugere um sistema Linux baseado no kernel 3.5, o que indica uma versão potencialmente desatualizada.

* **Detalhes e Implicações de Segurança:**

    * **Portas Filtradas (21, 22, 23):** As portas FTP (21), SSH (22) e Telnet (23) aparecem como "filtered". Isso significa que um firewall está bloqueando ou descartando ativamente pacotes enviados para essas portas. Embora isso aumente a segurança, é importante verificar a configuração do firewall e garantir que essas portas sejam bloqueadas por uma razão válida. O bloqueio de Telnet é uma boa prática, pois é um protocolo inseguro. SSH deve ser protegido por chaves, e o FTP deve ser substituído por SFTP.

    * **Porta 53 (DNS):** A porta 53 (DNS) está aberta e retornando respostas. No entanto, a resposta indica "SERVFAIL", o que sugere um problema com o servidor DNS. Isso pode indicar uma falha no servidor DNS local, uma configuração incorreta ou um ataque DoS. É crucial investigar a causa do SERVFAIL, pois um servidor DNS defeituoso pode comprometer a resolução de nomes e afetar a funcionalidade da rede. O script do Nmap sugere uma requisição "VersionBindReqTCP" que pode ser usada para determinar a versão do BIND (se aplicável) ou outra implementação de DNS.

    * **Porta 80 (HTTP/HTTPS):** A porta 80 está aberta e detectada como "ssl/http", sugerindo que o servidor web pode estar configurado para usar HTTPS (SSL/TLS). No entanto, a nomenclatura "ssl/http" sugere uma configuração que pode não ser ideal. O ideal seria que a porta 80 redirecionasse para a porta 443 (HTTPS). É fundamental verificar a configuração do certificado SSL/TLS para garantir que seja válido e que a versão do protocolo TLS seja forte (TLS 1.2 ou superior).

    * **Fingerprint de Serviço Desconhecido:** O Nmap não conseguiu identificar o serviço na porta 53 com precisão, solicitando o envio de um fingerprint. Isso pode indicar um serviço não padrão ou uma versão modificada de um serviço conhecido. Investigar esse fingerprint pode revelar informações valiosas sobre o serviço em execução.

    * **Detecção de Sistema Operacional:** A detecção de Linux 3.5 é uma preocupação, pois essa versão do kernel é antiga e provavelmente possui vulnerabilidades conhecidas. É crucial verificar qual distribuição Linux está sendo usada e considerar a atualização para uma versão mais recente e suportada.

* **Endereço MAC:** O endereço MAC C0:FF:A8:60:CE:19 revela que o dispositivo é fabricado pela Huawei Technologies.

2. WhatWeb (Identificação de Tecnologia Web):

* **Resumo:** O WhatWeb identificou diversas tecnologias utilizadas no servidor web acessível pela porta 80.

* **Detalhes e Implicações de Segurança:**

* **JQuery:** A detecção de JQuery indica o uso dessa biblioteca JavaScript. É importante verificar se a versão do JQuery utilizada é a mais recente, pois versões antigas podem conter vulnerabilidades conhecidas.

* **PasswordField:** A detecção de vários campos de senha (confirm_password, new_password, etc.) sugere a presença de funcionalidades de gerenciamento de usuários ou autenticação. É crucial garantir que esses campos estejam devidamente protegidos contra ataques como brute-force e injeção de código. O uso de nomes de campo comuns como "txt_Password" pode facilitar ataques direcionados.

* **UncommonHeaders:** A presença do header "content-security-policy" é uma boa prática, pois ajuda a mitigar ataques XSS (Cross-Site Scripting). A configuração do CSP deve ser revisada para garantir que seja restritiva o suficiente para proteger contra ataques.

* **X-Frame-Options: SAMEORIGIN:** Este header protege contra ataques de clickjacking, permitindo que a página seja incorporada apenas em iframes do mesmo domínio.

* **X-XSS-Protection: 1; mode=block:** Este header habilita a proteção contra XSS no navegador.

3. Amass (Enumeração de Subdomínios):

* **Resumo:** O Amass não encontrou nenhum ativo adicional (subdomínios) associado ao domínio.

* **Implicações de Segurança:** A falta de subdomínios descobertos pode indicar uma superfície de ataque menor. No entanto, é importante lembrar que o Amass pode não detectar todos os subdomínios existentes.

Recomendações Gerais:

* **Atualização do Sistema Operacional:** Priorizar a atualização do sistema operacional Linux para uma versão mais recente e suportada para mitigar vulnerabilidades conhecidas.
* **Análise e Correção do Problema DNS:** Investigar e corrigir a falha do servidor DNS (SERVFAIL) para garantir a resolução de nomes adequada.
* **Fortalecimento da Segurança Web:**
  * Verificar e atualizar a versão do JQuery.
  * Implementar medidas de proteção robustas para os campos de senha, incluindo políticas de senha fortes e proteção contra brute-force.
  * Revisar e fortalecer a configuração do Content Security Policy (CSP).
  * Certificar-se de que o servidor web está configurado para redirecionar HTTP para HTTPS e utilizar uma versão forte do TLS (1.2 ou superior).
* **Investigação do Serviço Desconhecido:** Investigar o serviço não identificado na porta 53 e determinar sua

finalidade e configuração.
* **Auditoria de Firewall:** Revisar as regras do firewall para garantir que as portas bloqueadas (FTP, SSH, Telnet) estejam devidamente protegidas e que não haja regras desnecessárias.
* **Testes Adicionais:** Realizar testes mais aprofundados, incluindo testes de vulnerabilidade e testes de penetração, para identificar e explorar possíveis falhas de segurança.

Conclusão:

O relatório revela algumas preocupações de segurança que precisam ser abordadas. A versão desatualizada do sistema operacional Linux e o problema com o servidor DNS são os pontos mais críticos. Além disso, é importante fortalecer a segurança do servidor web e investigar o serviço desconhecido. A correção dessas vulnerabilidades melhorará significativamente a postura de segurança do dispositivo. Um pentest mais completo, com ferramentas de análise de vulnerabilidade e exploração, é altamente recomendado.

MÓDULO: NMAP

Resultados de NMAP

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-14 02:31 CDT
Nmap scan report for 192.168.18.1
Host is up (0.0074s latency).
Not shown: 995 closed tcp ports (reset)
PORT   STATE    SERVICE  VERSION
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp open     domain   (generic dns response: SERVFAIL)
80/tcp open     ssl/http
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.95%I=7%D=7/14%Time=6874B26D%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x82\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
MAC Address: C0:FF:A8:60:CE:19 (Huawei Technologies)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.5
OS details: Linux 3.5
Network Distance: 1 hop

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 26.95 seconds
```

MÓDULO: WHATWEB

Resultados de WhatWeb

```
[1m [34mhttp://192.168.18.1 [0m [200 OK] [1mCountry [0m[ [0m [22mRESERVED [0m][ [1m [31mZZ [0m],
```

[1mIP [0m[[0m [22m192.168.18.1 [0m], [1mJQuery [0m, [1mPasswordField [0m[[0m [22mconfirm_password,new_password,old_password,ssid1_password,ssid2_password,txt_Password [0m], [1mScript [0m[[0m [22mJavaScript,text/javascript [0m], [1mUncommonHeaders [0m[[0m [22mcontent-security-policy [0m], [1mX-Frame-Options [0m[[0m [22mSAMEORIGIN [0m], [1mX-UA-Compatible [0m[[0m [22mIE=edge [0m], [1mX-XSS-Protection [0m[[0m [22m1; mode=block [0m]

MÓDULO: AMASS

Resultados de AMASS

No assets were discovered

RECOMENDAÇÕES DE SEGURANÇA

Com base na análise realizada, recomendamos as seguintes ações para mitigar riscos identificados: