

Analisi dell'Exploit di Metasploitable 2 - S7/L2

Sommario

Questo report documenta un penetration testing mirato a un ambiente di macchina virtuale Metasploitable 2. Il test si è concentrato sull'identificazione e lo sfruttamento di vulnerabilità nel sistema target utilizzando il Metasploit Framework (MSF). L'analisi ha rivelato uno sfruttamento riuscito dei servizi Telnet, dimostrando la natura insicura di questo protocollo legacy e sottolineando l'importanza di configurazioni di sicurezza adeguate.

Ambiente di Test

- **Sistema Target:** Macchina virtuale Metasploitable 2 (192.168.20.10)
- **Piattaforma di Test:** Kali Linux (2023)
- **Strumento Principale:** Metasploit Framework (MSF6)

```
(kali㉿kali2023)-[~]
$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

File System

.:ok000kdc'      'cdk000ko:.
.x0000000000000c      c0000000000000x.
:000000000000000k,      ,k000000000000000:
'000000000kkkk00000: :00000000000000000'
o00000000.MMMM.o0000o0000l.MMMM,00000000o
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
l00000000.MMMMMMMMMM;d;MMMMMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMMM;MMMM,00000000.
c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000occc0000.MX'x00d.
,kol'M.0000000000000.M'd0k,
:kk;.0000000000000.;Ok:
; k0000000000000000k:
,x0000000000000x,
.l00000000l.
,d0d,
.
```

Metodologia

Il penetration test ha seguito un approccio strutturato:

1. **Accesso Iniziale:** Ottenimento dell'accesso al login della macchina virtuale Metasploitable 2 utilizzando credenziali predefinite
2. **Ricognizione:** Utilizzo di Metasploit per scoprire i servizi disponibili sul sistema target
3. **Scansione delle Vulnerabilità:** Identificazione di servizi Telnet vulnerabili sulla porta 23
4. **Sfruttamento:** Esecuzione dello scanner di versione Telnet per confermare la vulnerabilità e ottenere informazioni sul servizio
5. **Documentazione:** Registrazione dei risultati per l'analisi

```
msf6 > search auxiliary scanner/telnet

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/telnet/brocade_enable_login          normal  No    Brocade Enable Login Check Scanner
1  auxiliary/scanner/telnet/lantronix_telnet_password     normal  No    Lantronix Telnet Password Recovery
2  auxiliary/scanner/telnet/lantronix_telnet_version      normal  No    Lantronix Telnet Service Banner Detection
3  auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass 2021-09-06     normal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
4  auxiliary/scanner/telnet/telnet_ruggedcom              normal  No    RuggedCom Telnet Password Generator
5  auxiliary/scanner/telnet/satel_cmd_exec                2017-04-07     normal  No    Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
6  auxiliary/scanner/telnet/telnet_login                  normal  No    Telnet Login Check Scanner
7  auxiliary/scanner/telnet/telnet_version                normal  No    Telnet Service Banner Detection
8  auxiliary/scanner/telnet/telnet_encrypt_overflow       normal  No    Telnet Service Encryption Key ID Overflow Detection

Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner/telnet/telnet_encrypt_overflow
```

Ricognizione Aggiuntiva

Ulteriori indagini hanno rivelato molteplici moduli di scansione relativi a Telnet disponibili in Metasploit:

- auxiliary/scanner/telnet/brocade_enable_login
- auxiliary/scanner/telnet/lantronix_telnet_password
- auxiliary/scanner/telnet/lantronix_telnet_version
- auxiliary/scanner/telnet/telnet_ruggedcom
- auxiliary/scanner/telnet/satel_cmd_exec
- auxiliary/scanner/telnet/telnet_login
- auxiliary/scanner/telnet/telnet_version
- auxiliary/scanner/telnet/telnet_encrypt_overflow

La scoperta di questi moduli indica le diffuse vulnerabilità associate alle implementazioni Telnet su varie piattaforme hardware e software.

```
msf6 > search auxiliary scanner/telnet/telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/telnet/telnet_version  normal         No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version
```

Esecuzione del Metasploit Framework

Il penetration test ha sfruttato il Metasploit Framework (MSF6) con i seguenti moduli:

1. Rilevamento Banner Telnet:

- Modulo: **auxiliary/scanner/telnet/telnet_version**
- Target: **192.168.20.10:23**
- Scopo: Rilevare e raccogliere informazioni sul servizio Telnet in esecuzione sul target

2. Configurazione del Modulo:

- RHOSTS: **192.168.20.10** (Indirizzo IP target)
- RPORT: **23** (Porta Telnet predefinita)
- THREADS: **1** (Thread di esecuzione)
- TIMEOUT: **30 secondi**

```
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  -  -  -  -
  PASSWORD  no              no       The password for the specified username
  RHOSTS     yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      23              yes       The target port (TCP)
  THREADS    1               yes       The number of concurrent threads (max one per host)
  TIMEOUT    30              yes       Timeout for the Telnet probe
  USERNAME   no              no       The username to authenticate as

View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.20.10
RHOSTS => 192.168.20.10
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.20.10:23 - 192.168.20.10:23 TELNET
a
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
[*] 192.168.20.10:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

[illegible]

Risultati dell'Exploitation

Lo scanner di versione Telnet è stato eseguito con successo contro il target, rivelando:

1. **Banner del Servizio:** Il servizio Telnet è stato identificato positivamente sulla porta 23
2. **Informazioni di Autenticazione:** Il banner ha esposto informazioni sulle credenziali di login
3. **Informazioni di Contatto:** Il sistema ha rivelato dettagli di contatto amministrativi
4. **Completamento della Scansione:** Scansione riuscita di 1 host target (100% completato)

Implicazioni di Sicurezza

I risultati dimostrano diverse criticità di sicurezza:

1. **Credenziali Predefinite:** L'uso di combinazioni nome utente/password predefinite (msfadmin/msfadmin) rappresenta un rischio significativo per la sicurezza negli ambienti di produzione
2. **Protocollo in Chiaro:** Telnet trasmette tutti i dati, comprese le credenziali di autenticazione, in chiaro, rendendolo vulnerabile allo sniffing di rete
3. **Perdita di Informazioni dal Banner:** Il servizio Telnet ha esposto informazioni sensibili del sistema attraverso il suo banner
4. **Mancanza di Controlli di Accesso:** Non erano presenti restrizioni evidenti sull'accesso remoto o protezioni contro attacchi a forza bruta

Raccomandazioni

Sulla base dei risultati del penetration test, si raccomandano le seguenti misure di sicurezza:

1. **Disabilitare Telnet:** Sostituire Telnet con alternative sicure come SSH per l'amministrazione remota
2. **Implementare Autenticazione Forte:** Applicare politiche di password complesse e considerare l'autenticazione a più fattori
3. **Segmentazione della Rete:** Limitare l'accesso ai servizi amministrativi solo alle reti di gestione fidate
4. **Rafforzamento dei Banner:** Rimuovere informazioni sensibili dai banner di servizio
5. **Scansione Regolare delle Vulnerabilità:** Implementare scansioni di routine per identificare e risolvere vulnerabilità simili
6. **Gestione delle Patch:** Mantenere aggiornate le patch di sicurezza per tutti i servizi di rete

Conclusione

Il penetration test ha dimostrato con successo lo sfruttamento dei servizi Telnet sul target Metasploitable 2. Questo esercizio evidenzia l'importanza di proteggere i protocolli legacy e implementare misure di sicurezza a più livelli. Le vulnerabilità osservate, sebbene intenzionali in questo ambiente di formazione, rappresentano lacune di sicurezza comuni trovate in sistemi di produzione configurati in modo improprio.

Data del Report: 13 maggio 2025