NMAP

Script

Sommario

Traccia esercizio principale

Scansione delle vulnerabilità con Nmap

Si richiede allo studente di effettuare delle scansioni di vulnerabilità sul target Metasploitable (target e attaccante su stessa rete o su reti diverse), tramite gli script:

- Vuln
- Vulners

Analizzare 3 vulnerabilità identificate a scelta.

Spiegare le differenze tra i due script.

Traccia esercizio facoltativo

Ripetere le stesse operazione sul target Windows.

Configurazione del laboratorio virtuale

Sono principalmente 2 reti distinti gestite da pfSense: 192.168.1.0/24 su Kali e 192.168.50.0/24 su Meta e Windows 7.

Svolgimento esercizio principale

Scansione con il modulo vuln

Utilizzare il comando **nmap --script vuln -sV -p- 192.168.50.100**

Cosa fa questo comando:

- --script vuln: lancia lo script Nmap vuln, che cerca vulnerabilità nei servizi.
- -sV: effettua una rilevazione delle versioni dei servizi.
- -p-: scansiona tutte le porte, dalla 1 alla 65535.
- 192.168.50.100: IP del target Metasploitable.

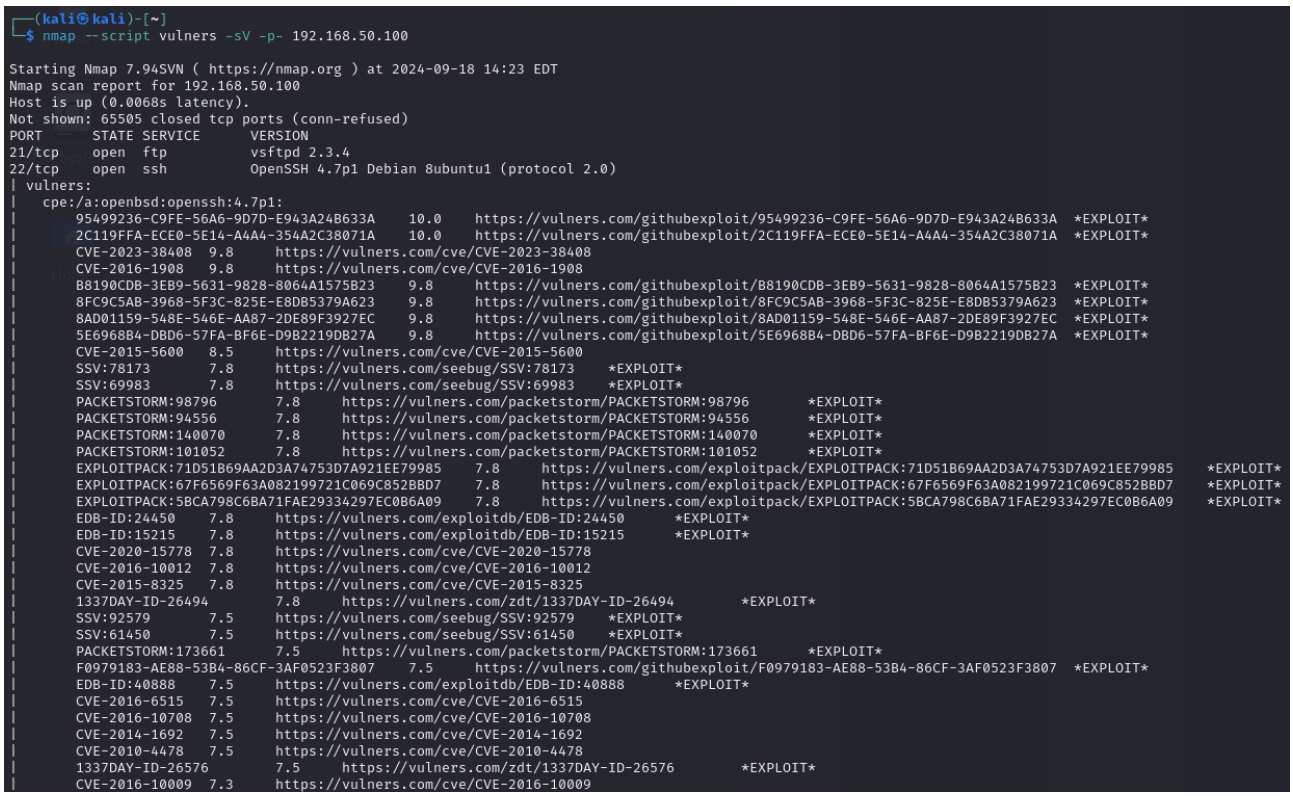
```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln -sV -p- 192.168.50.100

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-18 14:10 EDT
Nmap scan report for 192.168.50.100
Host is up (0.027s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       SSV:78173       7.8     https://vulners.com/seebug/SSV:78173    *EXPLOIT*
|       SSV:69983       7.8     https://vulners.com/seebug/SSV:69983    *EXPLOIT*
|       PACKETSTORM:98796       7.8     https://vulners.com/packetstorm/PACKETSTORM:98796       *EXPLOIT*
|       PACKETSTORM:94556       7.8     https://vulners.com/packetstorm/PACKETSTORM:94556       *EXPLOIT*
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       PACKETSTORM:101052      7.8     https://vulners.com/packetstorm/PACKETSTORM:101052      *EXPLOIT*
|       EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    7.8     https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    *EXPLOIT*
|       EXPLOITPACK:67F6569F63A082199721C069C852BBD7    7.8     https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852BBD7    *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    *EXPLOIT*
|       EDB-ID:24450    7.8     https://vulners.com/exploitdb/EDB-ID:24450      *EXPLOIT*
```

Ci sono troppe vulnerabilità che si possono sfruttare.

Scansione con il modulo vulners

Lo script vulners è simile, ma più specifico. Usa il database Vulners per identificare vulnerabilità note, in base alle versioni dei software rilevati sul target: **nmap --script vulners -sV -p- 192.168.50.100**



```
┌──(kali㉿kali)-[~]
└─$ nmap --script vulners -sV -p- 192.168.50.100

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-18 14:23 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0068s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       SSV:78173       7.8     https://vulners.com/seebug/SSV:78173    *EXPLOIT*
|       SSV:69983       7.8     https://vulners.com/seebug/SSV:69983    *EXPLOIT*
|       PACKETSTORM:98796       7.8     https://vulners.com/packetstorm/PACKETSTORM:98796       *EXPLOIT*
|       PACKETSTORM:94556       7.8     https://vulners.com/packetstorm/PACKETSTORM:94556       *EXPLOIT*
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       PACKETSTORM:101052      7.8     https://vulners.com/packetstorm/PACKETSTORM:101052      *EXPLOIT*
|       EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    7.8     https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    *EXPLOIT*
|       EXPLOITPACK:67F6569F63A082199721C069C852BBD7    7.8     https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852BBD7    *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    *EXPLOIT*
|       EDB-ID:24450    7.8     https://vulners.com/exploitdb/EDB-ID:24450      *EXPLOIT*
|       EDB-ID:15215    7.8     https://vulners.com/exploitdb/EDB-ID:15215      *EXPLOIT*
|       CVE-2020-15778  7.8     https://vulners.com/cve/CVE-2020-15778
|       CVE-2016-10012  7.8     https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325   7.8     https://vulners.com/cve/CVE-2015-8325
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       SSV:61450       7.5     https://vulners.com/seebug/SSV:61450    *EXPLOIT*
|       PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       EDB-ID:40888    7.5     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2016-6515   7.5     https://vulners.com/cve/CVE-2016-6515
|       CVE-2016-10708  7.5     https://vulners.com/cve/CVE-2016-10708
|       CVE-2014-1692   7.5     https://vulners.com/cve/CVE-2014-1692
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       CVE-2016-10009  7.3     https://vulners.com/cve/CVE-2016-10009
```

Ci sono troppe vulnerabilità che si possono sfruttare.

Differenze tra vuln e vulners

- **vuln**: è un insieme generico di script che cercano vulnerabilità comuni nei servizi esposti. Fornisce una panoramica generale sulle vulnerabilità, con controlli che coprono un'ampia gamma di problematiche di sicurezza.
- **vulners**: è più focalizzato. Confronta le versioni dei software rilevati con un database esterno (Vulners), restituendo le vulnerabilità note con riferimenti a CVE. È più accurato nella correlazione con vulnerabilità specifiche e note.

Svolgimento esercizio facoltativo

Scansione con il modulo vuln

Questo script esegue una scansione per individuare vulnerabilità comuni.

nmap --script vuln -oX vuln_scan.xml 192.168.50.101

Spiegazione:

- --script vuln: Usa il set di script vuln di Nmap per cercare vulnerabilità comuni.
- -oX vuln_scan.xml: Esporta i risultati in formato XML nel file vuln_scan.xml.
- 192.168.50.101: Indirizzo IP del target (Windows 7).

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln -oX vuln_scan.xml 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-18 19:35 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0043s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 99.11 seconds
```

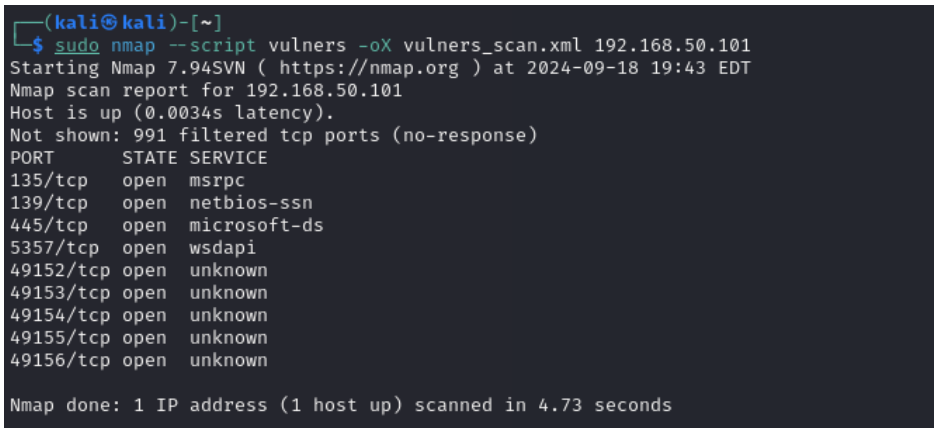
Scansione con il modulo vulners

Questo script utilizza il database di vulnerabilità CVE per fornire dettagli più specifici su eventuali vulnerabilità.

nmap --script vulners -oX vulners_scan.xml 192.168.50.101

Spiegazione:

- --script vulners: Esegue lo script vulners per identificare vulnerabilità basate su CVE.
- -oX vulners_scan.xml: Esporta i risultati in formato XML nel file vulners_scan.xml.
- 192.168.50.101: Indirizzo IP del target (Windows 7).



Differenze tra vuln e vulners

- **vuln**: Questo script esegue controlli generici per vulnerabilità note sui servizi che sono aperti e accessibili sul target.
- **vulners**: Questo script è più specifico e utilizza un database di vulnerabilità (come CVE) per fornire riferimenti precisi a problemi noti con dettagli aggiuntivi.

Vulnerabilità di Windows 7 scoperta

La vulnerabilità **CVE-2017-0143** è una falla di sicurezza nota anche come **EternalBlue**, che è stata scoperta in Microsoft Windows. È stata resa pubblica nel 2017 e sfruttata in vari attacchi, tra cui il famigerato attacco **WannaCry**.

Dettagli sulla vulnerabilità:

- **Tipo**: Esecuzione di codice remoto (RCE).
- **Piattaforme colpite**: Versioni vulnerabili di Microsoft Windows, in particolare Windows 7, Windows Server 2008 e versioni precedenti.
- **Meccanismo**: La vulnerabilità risiede nel protocollo **Server Message Block (SMB)**, utilizzato per la condivisione di file e stampanti. Un attaccante potrebbe inviare pacchetti appositamente progettati a un sistema vulnerabile e ottenere il controllo remoto del dispositivo.

Implicazioni:

- **Esecuzione di codice**: Gli attaccanti possono eseguire codice arbitrario sul sistema vulnerabile, permettendo loro di installare malware, esfiltrare dati o compromettere ulteriormente la rete.
- **Ampia diffusione**: La vulnerabilità ha avuto un impatto significativo, con molti dispositivi non aggiornati che sono stati facilmente compromessi.

Mitigazioni:

Microsoft ha rilasciato patch per correggere questa vulnerabilità. È consigliato a tutti gli utenti di Windows applicare le ultime aggiornamenti di sicurezza e disabilitare SMBv1, se non necessario.