

## 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:

- Vulners
- Vuln

Analizzare 3 vulnerabilità identificate a scelta. Spiegare le differenze tra i due script.

### Vulners:

```
C:\home\kali> nmap --script vulners 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 08:06
Nmap scan report for 192.168.50.101
Host is up (0.020s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
```

### Vuln:

```

C:\home\kali> nmap -script vuln 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 08:06 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 81.97% done; ETC: 08:07 (0:00:02 remaining)
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.61% done; ETC: 08:08 (0:00:11 remaining)
Stats: 0:03:20 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.72% done; ETC: 08:10 (0:00:06 remaining)
Stats: 0:03:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.72% done; ETC: 08:10 (0:00:06 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0041s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523 BID:48539
|       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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://www.securityfocus.com/bid/48539
|         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
|_ 22/tcp    open  ssh
|_ 23/tcp    open  telnet
|_ 25/tcp    open  smtp
|   smtp-vuln-cve2010-4344:
|     The SMTP server is not Exim: NOT VULNERABLE
|_ 53/tcp    open  domain
|_ 80/tcp    open  http
|   http-trace: TRACE is enabled
|   http-fileupload-exploiter:
|
|_ Couldn't find a file-type field.
|_ http-sql-injection:
|   Possible sql_i for queries:
|     http://192.168.50.101:80/dav/?C=M&3BOX3DAK27%20OR%20sqlspider
|     http://192.168.50.101:80/dav/?C=S&3BOX3DAK27%20OR%20sqlspider
|     http://192.168.50.101:80/dav/?C=D&3BOX3DAK27%20OR%20sqlspider
|     http://192.168.50.101:80/dav/?C=N&3BOX3DD&27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.50.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

```

3 vulnerabilità che si possono identificare da quest'ultimo screen sono:

### VSFTPD version 2.3.4 backdoor (CVE-2011-2523):

Presente nel servizio FTP in esecuzione sulla porta 21/tcp, questa versione contiene una backdoor che consente a un utente malintenzionato di ottenere accesso root al sistema dopo aver stabilito una connessione FTP. Sono evidenziati anche vari link che indicano exploit pubblici per sfruttare questa vulnerabilità

### HTTP - SQL Injection (porta 80/tcp):

Viene rilevata una potenziale vulnerabilità di **SQL Injection** in vari URL, un attaccante potrebbe eseguire query non autorizzate sul database, potenzialmente estraendo, modificando o cancellando dati.

Sono elencate molteplici pagine vulnerabili, inclusi script PHP presenti nel contesto di **Mutillidae**, una web app deliberatamente vulnerabile.

### HTTP TRACE Abilitato (porta 80/tcp):

La scansione segnala che la funzione TRACE è abilitata sul server HTTP.

Potrebbe esporre il server a vulnerabilità di tipo Cross-Site Tracing (XST), che può essere utilizzato in combinazione con altre vulnerabilità per rubare dati dell'utente o sessioni di autenticazione.

**Differenza tra i due script:**

La scansione **Vulners** è più veloce e non comporta traffico extra per il target, mostra solo le porte aperte potenzialmente vulnerabili e non tenta di verificare o sfruttare alcuna vulnerabilità, mentre la scansione **Vuln** invece tenta di scoprire la presenza di vulnerabilità particolari testando direttamente il servizio scoperto, ha un alto grado di fiducia e nessun falso positivo