

Esercitazione W10D4

Comandi di scan più utilizzati

Ettore Farris - 12/01/2024

Descrizione sintetica dell'esercitazione

<https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/>

Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report. Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

1) Nmap: scansione -sV

```
(kali㉿kali) ~  
[~$ sudo nmap -sV 192.168.32.101  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-16 13:12 EST  
Nmap scan report for 192.168.32.101  
Host is up (0.030s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet      Linux telnetd  
25/tcp    open  smtp        Postfix smtpd  
53/tcp    open  domain      ISC BIND 9.4.2  
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind     2 (RPC #100000)  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec        netkit-rsh rexecd  
513/tcp   open  login?        
514/tcp   open  shell       Netkit rshd  
1099/tcp  open  java-rmi    GNU Classpath grmiregistry  
1524/tcp  open  bindshell   Metasploitable root shell  
2049/tcp  open  nfs         2-4 (RPC #100003)  
2121/tcp  open  ftp        ProFTPD 1.3.1  
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc         VNC (protocol 3.3)  
6000/tcp  open  X11         (access denied)  
6667/tcp  open  irc         UnrealIRCd  
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)  
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 57.49 seconds
```

La scansione -sV di Nmap restituisce tutte le porte aperte del target. E' interessante notare che, oltre alla porta, è indicata anche la versione del software. Sapendo la versione, si può fare una ricerca per vulnerabilità.

Su Metasploitable ad esempio ci sono dei servizi vulnerabili, come quello della porta 21/tcp in cui gira *vsftpd 2.3.4*. Una semplice ricerca google ci da informazioni sulla vulnerabilità di questa versione e su come sfruttarla.

2) CrackMapExec

```
(kali㉿kali) - (~)
$ crackmapexec ftp 192.168.32.101
FTP 192.168.32.101 21 192.168.32.101 [*] Banner: (vsFTPD 2.3.4)

(kali㉿kali) - (~)
$ crackmapexec ssh 192.168.32.101
SSH 192.168.32.101 22 192.168.32.101 [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

(kali㉿kali) - (~)
$ crackmapexec smb 192.168.32.101
SMB 192.168.32.101 445 METASPLOITABLE [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)

(kali㉿kali) - (~)
$
```


Questo tool serve per valutare la sicurezza di reti che utilizzano, tra le tante, Active Directory. Indicando il target e il protocollo (come smb, ftp, ssh ecc) per il quale effettuare una scansione di sicurezza, questo tool restituisce informazioni preziose, come il banner del servizio.

Confrontando le informazioni ottenute con la scansione -sV di Nmap vista in precedenza, si vede l'attendibilità e l'efficacia di questo tool. Ad esempio, per il servizio FTP, il banner mostrato è sempre *vsftpd 2.3.4*.

3) Netdiscover

```
Currently scanning: 192.168.69.0/16 | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.32.101 08:00:27:2b:56:8f    1     60  PCS Systemtechnik GmbH
192.168.50.1   08:00:27:a8:ab:a8    1     60  PCS Systemtechnik GmbH
```



Netdiscover è un tool utilissimo che serve per la host discovery. Effettuando una scansione generica con comando `sudo netdiscover` (portando metasploitable nella nostra rete interna), si nota che è tra gli host presenti.

Questo tipo di scansione effettua un controllo per tutti gli host appartenenti a diverse sottoreti. In questo caso, kali appartiene alla sottorete 192.168.50.0 mentre metasploitable appartiene a quella 192.168.32.0. Gli host trovati sono pfsense (il default gateway attivo al momento della scansione) e metasploitable.

Tra le informazioni, compare il vendor della NIC, riconosciuto tramite l'indirizzo MAC.

