

Metasploit

Autor: Morris Tichy

Inhaltsverzeichnis

1. Metasploit Scan	2
1.1. Nmap Scan	2

1. Metasploit Scan

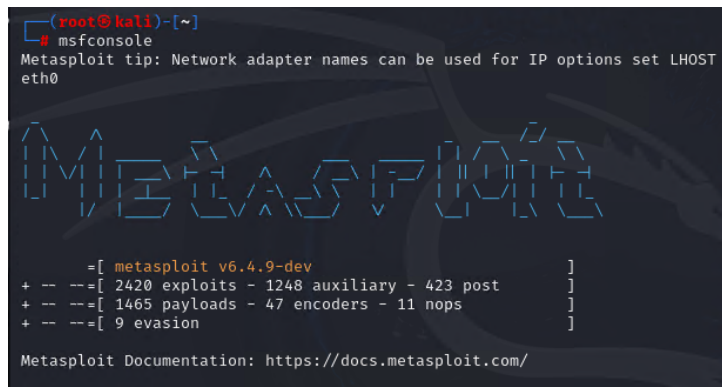
Als zweiten Schritt soll mithilfe von Metasploit ein Scan durchgeführt werden. Zuerst erfolgt aber die Installation von Metasploit. Da Metasploit in der Regel auf Kali Linux vorinstalliert ist, verwenden wir dieses. In dem Root terminal werden folgende Befehle ausgeführt, damit Metasploit gestartet wird. Zuerst wird ein Database Server installiert damit alle ergebnisse gespeichert werden können.

```
1 sudo systemctl start postgresql
2 sudo msfdb init
```

bash

Anschließend wird Metasploit gestartet mit `msfconsole`.

Sobald Metasploit geladen ist, werden Sie die folgende Eingabeaufforderung in Ihrem Terminal sehen - die Startbildschirme sind zufällig, machen Sie sich also keine Sorgen, wenn Ihrer anders aussieht:



```
(root@kali)~[~]
msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST eth0

Metasploit

  = [ metasploit v6.4.9-dev ]
+ -- --[ 2420 exploits - 1248 auxiliary - 423 post ]
+ -- --[ 1465 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Abbildung 1: „Metasploit Ausgabe“

Mit dem Befehl `search portscan` wird eine Liste aller verfügbaren Portscannern zurückgeliefert.

1.1. Nmap Scan

Mit dem Befehl `db_nmap -v -sV 192.168.50.0/24` wird ein Nmap Scan durchgeführt. Dieser Scan zeigt alle offenen Ports und die Versionen der Dienste, die auf diesen Ports laufen.

```
msf6 > db_nmap -v -sV 192.168.50.0/24
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-20 17:48 EST
[*] Nmap: NSE: Loaded 46 scripts for scanning.
[*] Nmap: Initiating ARP Ping Scan at 17:48
[*] Nmap: Scanning 255 hosts [1 port/host]
[*] Nmap: Completed ARP Ping Scan at 17:48, 5.23s elapsed (255 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 6 hosts. at 17:48
[*] Nmap: Completed Parallel DNS resolution of 6 hosts. at 17:48, 9.20s elapsed
```

Abbildung 2: „Metasploit nmap Scan“

Der Befehl `hosts` zeigt eine Liste an aller Geräte die im Netz gefunden worden sind.

```
Hosts
=====
```

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
192.168.50.1	00:0c:29:d2:4e:10		Unknown			device		
192.168.50.2	00:0c:29:7f:99:ca		Unknown			device		
192.168.50.3	00:0c:29:ff:a7:cb		Unknown			device		
192.168.50.4	00:0c:29:db:37:88		Unknown			device		
192.168.50.5	00:0c:29:66:38:99		Unknown			device		
192.168.50.12	00:0c:29:5b:67:f9		Unknown			device		
192.168.50.133			Unknown			device		

Abbildung 3: „Hosts im Netz“

Mit dem Befehl `services` können alle gefunden und offen Ports angezeigt werden.

```
192.168.50.2 3268 tcp ldap open Microsoft Windows Active Directory LDAP Domain: AvangerHQ.at0., Site: Site-1-AvangerHQ
192.168.50.2 3269 tcp ssl/ldap open Microsoft Windows Active Directory LDAP Domain: AvangerHQ.at0., Site: Site-1-AvangerHQ
192.168.50.3 80 tcp http open Microsoft IIS httpd 10.0
192.168.50.3 135 tcp msrpc open Microsoft Windows RPC
192.168.50.3 443 tcp ssl/http open Microsoft IIS httpd 10.0
192.168.50.3 445 tcp microsoft-ds open
192.168.50.4 135 tcp msrpc open Microsoft Windows RPC
192.168.50.4 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
192.168.50.4 445 tcp microsoft-ds open
192.168.50.5 135 tcp msrpc open Microsoft Windows RPC
192.168.50.5 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
192.168.50.5 445 tcp microsoft-ds open
192.168.50.5 3389 tcp ms-wbt-server open Microsoft Terminal Services
192.168.50.12 135 tcp msrpc open Microsoft Windows RPC
192.168.50.133 22 tcp ssh open OpenSSH 9.7p1 Debian 7 protocol 2.0
```

Abbildung 4: „Hosts im Netz“