Übung – Erkennen von Bedrohungen und Schwachstellen

Zielsetzung

Sie verwenden Nmap, einen Port-Scanner und ein Tool für das Netzwerk-Mapping, zum Erkennen von Bedrohungen und Schwachstellen auf einem System.

Hintergrund/Szenario

Nmap (Network Mapper) ist ein Open-Source-Programm, das für die Netzwerkanalyse und das Sicherheits-Auditing genutzt wird. Administratoren können mit Nmap auch Hosts überwachen oder Zeitpläne für Service-Upgrades verwalten. Mit Nmap wird ermittelt, welche Hosts in einem Netzwerk verfügbar sind sowie welche Services, Betriebssysteme und Paketfilter oder Firewalls ausgeführt werden.

Erforderliche Ressourcen

- PC mit Ubuntu 16.0.4 LTS, auf einer VMware-Workstation installiert

Schritt 1: Öffnen Sie in Ubuntu ein Terminalfenster.

a. Melden Sie sich mit den folgenden Anmeldeinformationen in Ubuntu an:

Benutzer: **cisco**

Kennwort: **password**

b. Klicken Sie auf das Symbol **Terminal**, um ein Terminal zu öffnen.

© 2017 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

Schritt 2: Führen Sie Nmap aus.

Geben Sie in der Eingabeaufforderung den folgenden Befehl ein, um einen grundlegenden Scan dieses Ubuntu-Systems durchzuführen:

```
cisco@ubuntu:~$ nmap localhost
```

```
cisco@ubuntu:~$ nmap localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:43 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
cisco@ubuntu:~$
```

Die Ergebnisse sind ein Scan der ersten 1.024 TCP-Ports.

Welche TCP-Ports sind geöffnet?

Schritt 3: Benutzen Sie NMAP mit Administratorrechten.

a. Geben Sie im Terminal den folgenden Befehl ein, um die UDP-Ports des Computers zu scannen (bedenken Sie, dass bei Ubuntu die Groß- und Kleinschreibung beachtet wird), und geben Sie bei entsprechender Aufforderung das Kennwort **password** ein:

```
cisco@ubuntu:~$ sudo nmap -sU localhost
```

```
cisco@ubuntu:~$ sudo nmap -sU localhost
[sudo] password for cisco:

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
cisco@ubuntu:~$
```

Welche UDP-Ports sind geöffnet?

© 2017 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.

b. Geben Sie im Terminal den folgenden Befehl ein:

```
cisco@ubuntu:~$ nmap –sV localhost
```

```
cisco@ubuntu:~$ nmap -sV localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:53 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet  Linux telnetd
Service Info: OS: 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 0.97 seconds
cisco@ubuntu:~$
```

Wenn Sie den Switch **–sV** in Verbindung mit dem Befehl **nmap** verwenden, wird eine Versionserkennung durchgeführt, die Sie für die Recherche hinsichtlich Schwachstellen einsetzen können.

Schritt 4: Erfassen Sie die SSH-Schlüssel.

Geben Sie im Terminal den folgenden Befehl ein, um einen Skript-Scan zu starten:

```
cisco@ubuntu:~$ nmap –A localhost
```

```
cisco@ubuntu:~$ nmap -A localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:56 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 83:35:a7:81:c7:04:47:d4:6b:b4:87:b3:e3:5b:c7:ab (RSA)
|_  256 78:97:1f:92:cf:38:63:90:c3:7f:d5:ff:85:43:e6:2f (ECDSA)
23/tcp open  telnet  Linux telnetd
Service Info: OS: 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 1.16 seconds
cisco@ubuntu:~$
```

Sie haben die SSH-Schlüssel für das Hostsystem erfasst. Durch den Befehl werden verschiedene in Nmap integrierte Skripte zum Testen bestimmter Schwachstellen ausgeführt.

Referenzen

Nmap: https://nmap.org/

© 2017 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Dieses Dokument enthält öffentliche Informationen von Cisco.