

Definição de ambiente de Pentest aplicado a redes abertas

Resumo

As configurações apresentadas foram fundamentais para a execução deste trabalho, uma vez que a ferramenta Kali Linux, é um sistema operacional baseado em Linux voltado para a segurança cibernética, e oferece um conjunto de ferramentas destinadas a testes de intrusão. Entre essas ferramentas destacam-se o Escaneamento de Redes, o Monitoramento de Dispositivos, o uso de protocolos como Nmap e ARP entre outras funcionalidades. Essas ferramentas permitem identificar, explorar e corrigir vulnerabilidades presentes em sistemas e redes, contribuindo para a segurança da infraestrutura tecnológica.

Kali Linux

- Kali Linux é uma distribuição GNU/Linux baseada no Debian, considerado o sucessor do Back Track. O projeto apresenta várias melhorias, além de mais aplicativos. É voltado principalmente para auditoria e segurança de computadores em geral. É desenvolvido e mantido pelo *Offensive Security Ltd*. Desde 21 de janeiro de 2016, é uma distribuição “rolling-release”.
- O Kali Linux dispõe de numerosos softwares pré-instalados, incluindo o Nmap (port scanner), Aircrack-ng (software para testes de segurança em rede de computadores).

Instalação

O Kali Linux permite a instalação em arquiteturas i386, amd64 e ARM (armel e armhf), para a arquitetura i386, a imagem do Kai, traz um kernel PAE por padrão, podendo assim ser executado em sistemas com mais de 4 GB de RAM. O sistema pode ser instalado a partir de um DVD ou um Live USB, também permite a instalação via rede.

Ferramentas

- Escaneamento das redes
- Monitoramento da rede
- Leitura dos dispositivos conectados à rede
- Nmap (portscan)
- ARP

Essas ferramentas podem ser usadas para inúmeros propósitos, a maioria envolve exploração de falhas em uma rede de computadores ou aplicação, realização de descoberta de computadores na rede, ou escaneamento de um alvo específico na rede pelo endereço IP. Muitas ferramentas da versão passada foram eliminadas para focar nas mais populares e efetivas para testes de segurança.

Escaneamento das redes

- Busca mostrar todas as redes locais disponíveis.
- Comando: **airodump-ng**

```
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
D8:C6:78:E0:D4:38 -88 2 0 0 6 130 WPA2 CCMP PSK VIVOFIBRA-D438
8C:9B:68:96:0C:15 -83 4 0 0 11 195 WPA2 CCMP PSK 2G_ISABELLA
90:75:8C:93:84:69 -88 4 0 0 10 130 WPA2 CCMP PSK Ferreiras 2Ghz
92:75:8C:C3:84:69 -82 5 0 0 10 130 WPA2 CCMP PSK <length: 0>
60:7E:CD:6A:83:68 -66 10 0 0 11 270 WPA2 CCMP PSK 8360_Fibra_2.4G
80:D0:4A:97:AF:60 -49 20 1 0 11 195 WPA2 CCMP PSK Varago.A
48:B2:5D:1A:0B:08 -65 14 0 0 4 130 WPA2 CCMP PSK PODEMAIS
C0:3D:D9:86:52:C8 -64 13 0 0 6 130 WPA2 CCMP PSK VIVOFIBRA-52C8
B8:5F:B0:1D:09:04 -68 14 0 0 8 130 WPA2 CCMP PSK Poiati
1C:9D:72:86:6B:90 -56 13 1 0 1 195 WPA2 CCMP PSK GABRIEL_2G
D8:33:B7:30:F1:AE -50 15 0 0 1 260 WPA2 CCMP PSK Damico09

BSSID STATION PWR Rate Lost Frames Notes Probes
D8:33:B7:30:F1:AE 42:9B:93:1D:61:0A -35 0 - 1e 0 2
D8:33:B7:30:F1:AE B2:CC:23:EC:1C:59 -37 0 - 1 3 9
Quitting ...
Notice: You specified "-bssid". Did you mean "--bssid" instead?
```

Monitoramento da rede

- Mostrar quais dispositivos estão conectados e quais vão se conectar
- Comando: **airodump-ng -c**

```
(root@kali)-[~/home/kali/Downloads/naive-hashcat]
└─# airodump-ng -c 1 --bssid D8:33:B7:30:F1:AE -w /media/kali/persistence wlan0
ioctl(SIOCSIWMODE) failed: Device or resource busy
15:36:24 Created capture file "/media/kali/persistence-01.cap".

CH 1 ][ Elapsed: 36 s ][ 2024-04-11 15:37 ][ WPA handshake: D8:33:B7:30:F1:AE

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
D8:33:B7:30:F1:AE 14 96 360 70 0 1 260 WPA2 CCMP PSK Damico09

BSSID STATION PWR Rate Lost Frames Notes Probes
D8:33:B7:30:F1:AE B2:CC:23:EC:1C:59 25 1e- 1 0 101 EAPOL
D8:33:B7:30:F1:AE 42:9B:93:1D:61:0A 24 1e- 1e 9 118 EAPOL Damico09
D8:33:B7:30:F1:AE 00:D7:6D:4A:F8:DA 28 0 - 6e 0 473
Quitting ...
```

Leitura dos dispositivos conectados à rede

- Leitura limpa e apresenta os IPs associados
- Comando: **netdiscover -r**

```
Currently scanning: Finished! | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
192.168.0.1  d8:33:b7:30:f1:ad  1     60  Sagemcom Broadband SAS
192.168.0.3  3c:e5:b4:18:54:1f  1     60  KIDASEN INDUSTRIA E COMERCIO DE ANTENAS LTDA
192.168.0.5  72:4c:35:f2:c6:83  1     60  Unknown vendor

(kali@kali)-[~]
└─$ sudo netdiscover -r 192.168.0.1/24
```

Nmap(portscan)

- Mostrar as portas do servidor online
- Comando: **nmap scanme.nmap.org**

```
(kali@kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 14:38 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 10.35 seconds
```

