LABORATÓRIO XIII

HONEYPOTS

Redes de Computadores – Da Teoria à Prática com Netkit

Laboratório XIII – Honeypots

Objetivos do laboratório

- Aprender sobre honeypots e honeynets
- Conhecer ferramentas de criação de potes
- Relacionar potes com footprintings

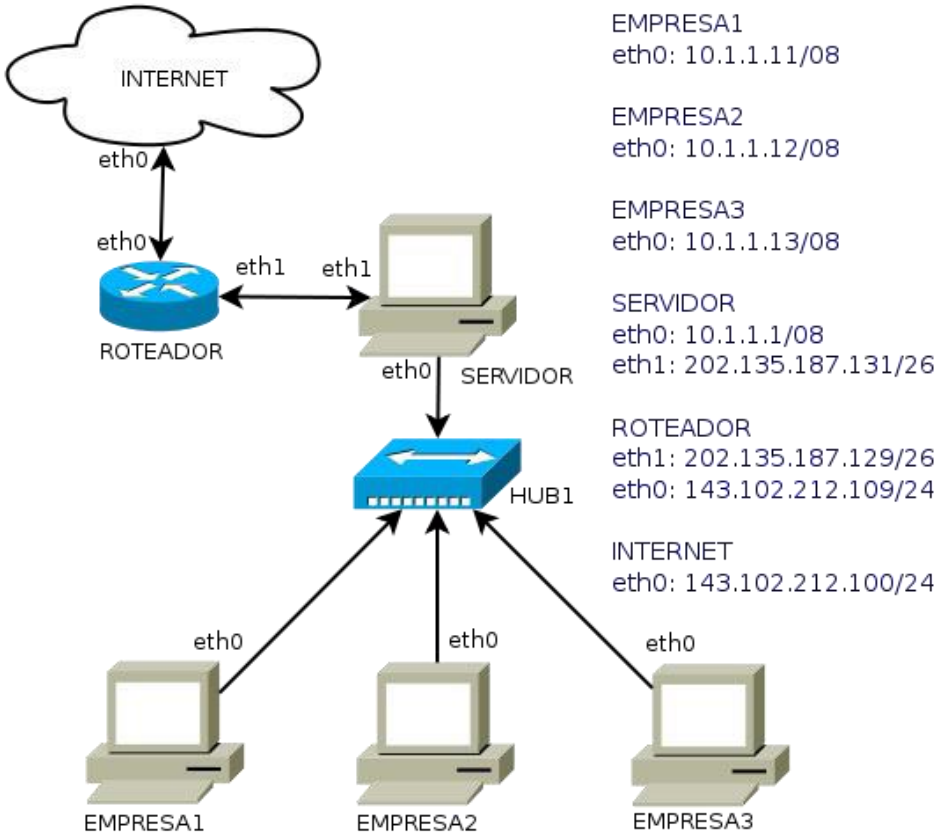
Este experimento utiliza a versão personalizada do filesystem disponível no site. Verifique se a mesma está adequadamente instalada.

Cenário sendo reproduzido

A figura abaixo representa a topologia de rede sendo estudada, sendo a mesma que foi utilizada no laboratório de firewall, representando a infraestrutura de redes da empresa Cosmo Books.

Para o compartilhamento da internet, foi utilizado um servidor montado numa velha máquina do proprietário, um K6-II 500 MHz com 64 MB de RAM, o qual denominamos SERVIDOR. Esta máquina é ligada à internet pelo provedor Fasty. Os computadores são ligados em rede por um hub de 8 portas de 100Mbps e cabos categoria 5, devidamente dimensionados. Os possíveis usuários são **joaquim, manuel**, **maria** e **comprador.**

Em nosso laboratório virtual, o provedor é representado pelo "ROTEADOR" e os números de IPs são mostrados. Ao iniciar o laboratório virtual, SERVIDOR e INTERNET se comunicam à vontade.



Conhecimentos de segurança que você irá adquirir

Diferente do ponto de vista do laboratório de firewall, agora estamos interessados em ataques ativos e passivos que podem ser realizados em uma rede. Uma habilidade importante para um possível atacante é conhecer o alvo. Quanto mais informações o mesmo tiver melhor. Se informação é um dos poderes de um atacante, uma forma de se proteger é fornecer informações faltas de modo que ele pense que a rede tem uma topologia da rede diferente da rede de fato.

A técnica de honeypot se torna interessante pois, ao mesmo tempo que você pode utilizar fornecer informações faltas para o atacante, você pode estudar as cargas e procedimentos que o mesmo utiliza em sua rede, de modo que você pode aprender novas maneiras de ataque e, consequentemente, estudar novas formas de proteger seus sistemas.

Antes de continuar, é importante lembrar que você deve ter feito a instalação do software **Wireshark** que será utilizado neste lab, portanto use os comandos apt-get install wireshark (distribuições debian) ou urpmi wireshark (mandriva) para instalar este software, caso o mesmo não esteja instalado.

Devemos lembrar que, os comandos marcados com a tag [real] deverão ser executados no console real. Os demais comandos serão executados dentro das máquinas virtuais. Sempre que exigido a instrução pedirá uma máquina virtual específica.

Execução do laboratório

Importante: Antes de executar este lab, você desejará se preparar com os seguintes requisitos: Este lab requer diversas janelas. Use um ambiente de trabalho com vários espaços, preferencialmente 4 deles. Gnome, Kde, Xfce tem quatro espaços por padrão.

Sobre as pastas:
Em seu computador pessoal, o caminho ideal é /home/seu_nome/nklabs/
Se você está executando estas práticas em um laboratório restrito, como o da universidade, utilize a pasta /tmp. (Lembrando que o conteúdo entre execuções será apagado ao finalizar a máquina).

1. [real] Salve o arquivo netkit_lab12.tar.gz na sua pasta de labs. (/pasta_dos_labs). (Isso mesmo, vamos usar o arquivo do lab12 para executar o tutorial 13.)

2. [real] Acesse a pasta nklabs a partir do terminal
```
[seu_nome@suamaquina tmp]$ cd /pasta_dos_labs
```

3. [real] Use o comando:
```
[seu_nome@suamaquina tmp]$ tar -xf netkit_lab12.tar.gz
```

Será criada a pasta lab12 dentro da sua pasta nklabs.

4. [real] Use o comando a seguir:
```
[seu_nome@suamaquina tmp]$ lstart -d /pasta_dos_labs/lab12
```

As seis máquinas virtuais serão iniciadas com as interfaces de rede devidamente configuradas. A internet não está distribuída para os computadores da empresa e os serviços de rede ainda não estão inicializados.

5. [real] Organize suas janelas de modo a localizar qualquer uma delas rapidamente. É recomendável que você utilize duas áreas de trabalho, para deixar as janelas com certa largura, pois algumas linhas de saída dos comandos deste tutorial são longas.

6. O primeiro passo é colocar a rede em funcionamento. Faça os seguintes comandos para realizar o compartilhamento da internet, no SERVIDOR. Sim, queremos que você reforce seus conhecimentos em iptables, seu professor deverá cobrar na prova.

```
SERVIDOR:~$ echo 1 > /proc/sys/net/ipv4/ip_forward
SERVIDOR:~$ iptables –F
SERVIDOR:~$ iptables -F -t nat
SERVIDOR:~$ iptables -F -t mangle
SERVIDOR:~$ iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

7. Tente executar um ping de INTERNET para EMPRESA2.
```
INTERNET:~$ ping 10.1.1.12
```

   O resultado esperado é que a rede não pode ser alcançada. Lembre-se de interromper o ping com o comando Ctrl+C após algumas entradas.

8. Tente executar um ping à partir do SERVIDOR para INTERNET
```
SERVIDOR:~$ ping 143.102.212.100
```

   O resultado esperado é sucesso na comunicação

9. Tente fazer o mesmo da EMPRESA1 para a INTERNET
```
EMPRESA1:~$ ping 143.102.212.100
```

   O resultado esperado é sucesso na comunicação.

Devemos lembrar que cada computador permite o acesso de 4 usuários, maria, joaquim, manuel e comprador. As senhas são 123mar, 123joa, 123man e 123com respectivamente. Estes passos são repetitivos com a prática anterior justamente para maior fixação.

10. Nos computadores EMPRESA1 acione os serviços de SSH, FTP, DNS, PROXY e HTTP com os seguintes comandos:
```
EMPRESA1:~$ cd /etc/init.d
EMPRESA1:~$ ./apache2 start
EMPRESA1:~$ ./squid start
EMPRESA1:~$ ./bind start
EMPRESA1:~$ ./proftpd start
EMPRESA1:~$ ./ssh start
```

11. Repita o procedimento anterior com os computadores EMPRESA2 e

EMPRESA3.

12. Verifique os processos em execução no computador EMPRESA1 com o comando ps aux | more.
```
EMPRESA1:~$ ps aux | more
```

O comando more permite fazer pausas na saída do comando ps aux. O comando ps aux exibe uma lista de processos detalhada. Para avançar páginas sobre uma saída sendo exibida com more, utilize a barra de espaços.

13. No computador EMPRESA1, execute o seguinte comando e tome nota da saída.
```
EMPRESA1:~$ netstat -nap
```

Observe a saída atentamente.

14. Execute o comando a seguir no SERVIDOR para ativar a captura de pacotes. Atenção para não executá-lo duas vezes.
```
SERVIDOR:~$ tcpdump -i eth0 -w /hosthome/lab13.pcap &
```

Atenção ao & comercial no final do comando que irá permitir que o tcpdump execute em background. Ao executar o comando, será necessário pressionar ENTER uma vez mais para que o *"prompt de comando"* seja devolvido.

Até o momento você iniciou os serviços dos vários computadores internos, como fez no laboratório passado. Com os conhecimentos das práticas 5 e 12 anteriores, você poderia fazer os redirecionamentos de porta, ports scans para averiguar as portas abertas.

Neste momento, vamos incrementar nossa rede com mais alguns computadores através do pacote especial honeyd que cria potes de mel. Se você estiver usando um PC real ao invés do Netkit para essa prática, utilize

15. No computador SERVIDOR, crie um arquivo de configuração chamado **mel.conf,** na pasta /etc/honeypot: *(não erre ao digitar*)
```
SERVIDOR:~$ vim mel.conf
```

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block

create template
set template personality "Microsoft Windows XP Professional SP1"
set template uptime 1728650
set template maxfds 35
set template default tcp action reset
add template tcp port 135 open
add template tcp port 139 open
add template tcp port 445 open

set template ethernet "00:00:11:1c:3c:01"
bind 10.1.1.100 template
```

Dicas do **vim**. A tecla insert ou i passa para o modo de edição. Todo comando é iniciado com : (dois pontos). :q para sair, :w para gravar e :q! para sair sem salvar as alterações. É útil saber alguns comandos básicos deste editor, pois pode ser a única coisa que você tenha a mão.

16. Inicie o serviço de honeypot do servidor com o seguinte comando:
```
SERVIDOR:~$ honeyd -i eth0 -d -f /etc/honeypot/mel.conf
```

17. No computador EMPRESA1, faça um portscan para verificar as portas abertas do ip 10.1.1.1.
```
EMPRESA1:~$ nmap -p 21,22,53,80 10.1.1.1
```

18. Faça o mesmo agora com o ip inexistente 10.1.1.100, porém com as portas dos serviços que ativamos.
```
EMPRESA1:~# nmap -p 135,139,445,80 10.1.1.100
```

Observe a interessante saída do portscan. Vejamos como o honeypot pode ser uma ferramenta interessante.

19. No computador SERVIDOR, altere o arquivo mel.conf para acrescentar logo acima da configuração do mac ethernet as linhas:

```
add template tcp port 80 "sh /usr/share/honeyd/scripts/win32/web.sh"
add template tcp port 22 "/usr/share/honeyd/scripts/test.sh $ipsrc $dport"
```

20. A partir do computador EMPRESA1, utilize o lynx para verificar uma página de um computador inexistente.
```
EMPRESA1:~# lynx 10.1.1.200
```

Observe que a saída é que o computador não pode ser encontrado. Faça o mesmo com o IP de nosso pote de mel agora. O passo a seguir pode falhar uma vez que a versão presente do honeyd neste fs do Netkit é um pouco lenta e demora à responder.

21. Tente visualizar a página http do pote de mel utilizando o lynx:
```
EMPRESA1:~# lynx 10.1.1.100
```

22. Interrompa a captura do arquivo de captura no servidor. Para isso execute o comando a seguir com dois enters.
```
SERVIDOR:~# fg tcpdump
```

23. Estude atenciosamente o pacote no wireshark. Ele está em sua pasta home com o nome de lab13.pcap.

24. No SERVIDOR, vá para a pasta /usr/share/honeyd/scripts e observe seu conteúdo. Estude alguns dos scripts presentes.

25. [real] Faça os exercícios propostos antes de parar o laboratório nos labs seguintes.

26. [real] Use o comando a seguir para encerrar a execução do laboratório:
```
[seu_nome@suamaquina ~]$ lhalt -d /pasta_dos_labs/lab13
```

27. [real] Use o comando a seguir para apagar os enormes arquivos.disk:
```
[seu_nome@suamaquina ~]$ lclean -d /pasta_dos_labs/lab13
```

Formule as teorias

Lembrando seus conhecimentos adquiridos até agora.

1. Altere o arquivo de configuração mel.conf para aceitar uma nova máquina. Use a personalidade “Linux 2.4.7 (X86)”.
2. Quais as vantagens de usar o honeypot baseado em aplicação? Qual desvantagem foi percebida?
3. Proponha uma solução para a criação de uma honeynet.
4. Porque o uso de honeypots ou honeynets é interessante? E as saídas produzidas pelo honeyd (ou seus logs)?

Aprendendo um pouco sobre linux

Utilizamos um software chamado honeyd que é um daemon para a criação de potes de mel e honeynets. Seu uso é bastante simples, pois requer apenas um arquivo de configuração, embora alterar os scripts pode permitir gerar resultados poderosos e interessantes, levando o atacante a realmente acreditar que está conseguindo informações privilegiadas.

É interessante vocẽ observar que o próprio Netkit oferece uma solução que pode ser utilizada para montagem de honeynets com os serviços funcionais, entretanto, a medida que as máquinas forem acessadas de fato, um script ou executável que puder ser executado, pode comprometer o processamento do hospedeiro.