Configurações iniciais

Linux1

```
auto eth0

iface eth0 inet static
        address 192.0.2.100
        netmask 255.255.255.0
        gateway 192.0.2.1
```

Linux2

```
auto eth0

iface eth0 inet static
        address 203.0.113.100
        netmask 255.255.255.0
        gateway 203.0.113.1
```

Mikrotik

```
ip address add address=192.0.2.1/24 interface=ether1
ip address add address=203.0.113.1/24 interface=ether2
```

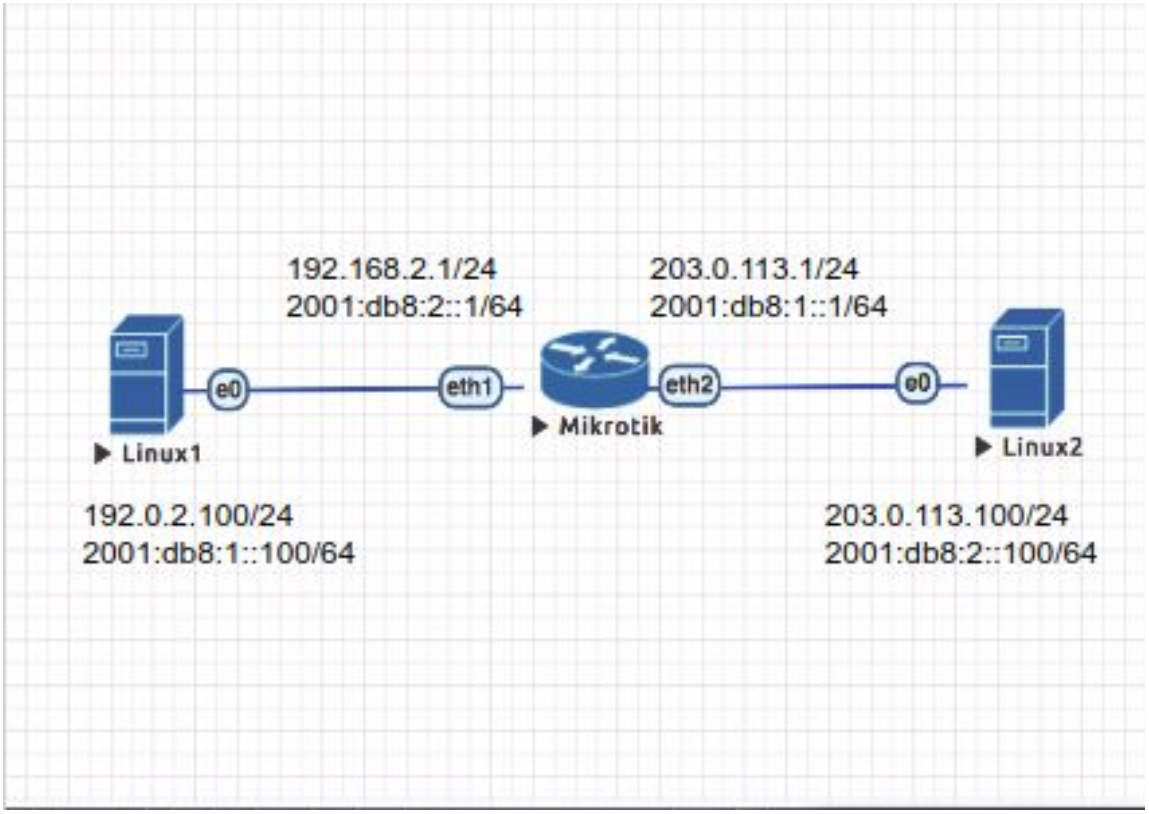
Experiência Zero - Como o Eve funciona?

1. Como logar no EVE
2. Como criar uma pasta
3. Como criar uma experiência
    a. Add New Lab
    b. Colocar duas máquinas ligadas
        i. Add an object -> Node
        ii. Selecionar Linux -> Linux Kali
        iii. Renomear para HostA
        iv. Add an object -> Node
        v. Selecionar Linux -> Linux Kali
        vi. Renomear para HostB
        vii. Conectar HostA com HostB.
    c. Ligar as máquinas
    d. Mostrar o processamento
    e. Acessar uma máquina e mostrar como ela está operando.
    f. Desligar a experiência

Pré Experiência - Configurando IPv6

1. Acessar o eve-ng (eve-ng.in.ceptro.br)
    a. login: lacnicXX
    b. senha: labgrupoXX
2. Acessar **Linux1** (mesmo usuário e senha no outro linux)
    a. login: root
    b. senha: toor
3. Configurar IPv6 em **Linux1**
    a. #ip -6 address add 2001:db8:2::100/64 dev eth0
    b. #ip -6 route add default via 2001:db8:2::1
4. Configurar IPv6 em **Linux2**
    a. #ip -6 address add 2001:db8:1::100/64 dev eth0
    b. #ip -6 route add default via 2001:db8:1::1
5. Habilitar IPv6 em **Mikrotik**
    a. /system package enable ipv6
    b. /system reboot
6. Configurar IPv6 em **Mikrotik**
    a. /ipv6 address add address=2001:db8:2::1/64 interface=ether1 advertise=no
    b. /ipv6 address add address=2001:db8:1::1/64 interface=ether2 advertise=no

Topologia final:



Primeira Experiência - Observando pacotes com o Wireshark

1. Acessar **Linux1**
2. Abrir o wireshark
3. No wireshark capturar a interface eth0
4. No terminal realizar um ping IPv4 para Linux2
    a. #ping -c4 203.0.113.100
5. No terminal realizar um ping IPv6 para Linux2
    a. #ping6 -c4 2001:db8:1::100
6. No terminal realizar um NMAP TCP SYN scan IPv4
    a. #nmap -sS 203.0.113.100
7. No terminal realizar um NMAP UDP scan IPv4
    a. #nmap -sU 203.0.113.100
    b. parar com o CTRL+C
8. No terminal realizar um NMAP TCP SYN scan IPv6
    a. #nmap -6 -sS 2001:db8:1::100
9. No terminal realizar um NMAP UDP scan IPv6
    a. #nmap -6 -sU 2001:db8:1::100

b. parar com CTRL+C

Segunda experiência - ataque de dicionário

1. Acessar **Mikrotik**
2. Trocar a senha do usuário default (sem senha por padrão)
    a. /user set 0 password=mk123
3. Acessar **Linux1**
4. Verificar arquivo rockyou.txt (uma lista de 14 milhões de senhas que já foram quebradas)
    a. #gzip -d /usr/share/wordlists/rockyou.txt.gz
    b. #grep senha /usr/share/wordlists/rockyou.txt
5. No terminal gerar palavras em letras minúsculas de tamanho 1 a
    a. #crunch 1 3
6. No terminal colocar essas palavras em um arquivo palavras.txt
    a. #crunch 1 3 -o palavras.txt
7. No terminal gerar palavras de 5 a 8 caracteres
    a. #crunch 5 8
8. No terminal gerar palavras de 5 a 8 caracteres com os caracteres "a", "b" e "c”
    a. #crunch 5 8 abc
9. No terminal mostrar o arquivo com lista de caracteres disponíveis no crunch
    a. #cat /usr/share/rainbowcrack/charset.txt
10. No terminal gerar palavras de 8 caracteres com letras minúsculas terminadas em 2705
    a. #crunch 8 8 -t @@@@2705
11. No terminal gerar palavras de 8 caracteres com letras minúsculas iniciadas em "edu"
    a. #crunch 8 8 -t edu@@@@@
12. No terminal gerar palavras de 3 caracteres com a permutação de caracteres "e", "d" e "u"
    a. #crunch 3 3 -p edu
13. No terminal gerar o arquivo de senhas para o ataque
    a. #crunch 5 5 0123456789 -t mk@@@ -o password.txt
14. No terminal gerar o arquivo de usuários para o ataque
    a. #echo “admin” > user.txt

15. No terminal executar o programa "patator" para realizar o ataque
    a. #patator ssh_login host=192.0.2.1 user=FILE0 password=FILE1 0=/root/user.txt 1=/root/password.txt -x ignore:mesg='Authentication failed.'

16. **Segurança Mikrotik**
17. Acessar **Mikrotik**
18. Trocar a senha e o usuário default
    a. /user set 0 password=Umasenhaseguraeumasenhaextensa name=BackupAdmin comment=BACKUP
19. Adicionar grupo específico
20. /user group add name=tecnico policy=ssh,ftp,reboot,read,write,policy
21. Adicionar outro usuário
    a. /user add name=eduardo password=Naodevemosusaramesmasenha group=tecnico comment=consultor
22. Acessar **Linux1**
23. No terminal adicionar chave rsa para o ssh
    a. #ssh-keygen -t rsa
    b. password=Senhadousuariolinux1
24. No terminal transferir a chave pública para o Mikrotik
    a. #scp .ssh/id_rsa.pub BackupAdmin@192.0.2.1:eduardo.pub
25. No **Mikrotik** importar e criptografar a chave transferida
    a. /user ssh-keys import public-key-file=eduardo.pub user=eduardo
    b. /ip ssh set strong-crypto=yes
26. Acessar **Linux1**
27. No terminal testar o acesso ssh IPv4 de Linux1 para Mikrotik
    a. #ssh eduardo@192.0.2.1
28. No terminal testar o acesso ssh IPv6 de Linux1 para Mikrotik
    a. #ssh -6 eduardo@2001:db8:2::1
29. No **Mikrotik** verificar o log (habilitado por padrão)
    a. /log print

b. /export compact

Terceira experiência - Ataque de Sniffing de pacotes em protocolos sem segurança

1. Acessar **Linux1**
2. Abrir o wireshark
3. No wireshark capturar a interface eth0
4. No terminal realizar uma conexão via telnet ao Mikrotik
    a. #telnet 192.0.2.1
    b. user: BackupAdmin
    c. password: Umasenhaseguraeumasenhaextensa
5. No wireshark observar a senha trafegada
6. No terminal realizar os seguintes NMAP para descobrir as portas abertas em TCP e UDP em IPv4 e IPv6
7. NMAP TCP SYN IPv4
    a. #nmap -sS 192.0.2.1
8. NMAP UDP IPv4
    a. #nmap -sU 192.0.2.1
9. NMAP TCP SYN IPv6
    a. #nmap -6 -sS 2001:db8:2::1
10. NMAP UDP IPv6
    a. #nmap -6 -sU 2001:db8:2::1

11. **Segurança Mikrotik**
12. Acessar **Mikrotik**
13. Listar todos os serviços habilitados
    a. /ip service print
14. Desabilitar todos os serviços não utilizados
    a. /ip service disable telnet (desabilita o telnet)
    b. /ip service disable ftp (desabilita o ftp)
    c. /ip service disable www (desabilita o HTTP)
    d. /ip service disable www-ssl (desabilita o HTTPS - **no emulador veio desabilitado por padrão**)

e. /ip service disable api (desabilita a opção de pegar informações do roteador por api)
f. /ip service disable api-ssl (desabilita a opção de pegar informações do roteador por api)
g. /tool bandwidth-server set enabled=no (desabilita o testador de banda)
h. /ip dns set allow-remote-requests=no (**desabilita o mikrotik de atuar como um servidor DNS cache - no emulador veio desabilitado por padrão**)
i. /ip socks set enabled=no **(desabilita acesso via sockets no mikrotik - no emulador veio desabilitado por padrão**)
j. /tool mac-server set allowed-interface-list=none (desabilita o acesso via lan sem IP definido)
k. /tool mac-server mac-winbox set allowed-interface-list=none (desabilita o acesso via lan sem IP definido)
l. /tool mac-server ping set enabled=no (desabilita a descoberta na lan)
m. /tool romon set enabled=no (desabilita Router Management Overlay Network para diminuir a interface de ataque - **no emulador veio desabilitado por padrão**)
n. /ip neighbor discovery-settings set discover-interface-list=none (desabilita o MNDP, CDP e LLDP que ficam procurando roteadores na rede)
o. /ip proxy set enabled=no (desabilita o proxy - **no emulador veio desabilitado por padrão**)
p. /ip upnp set enabled=no (desabilita o upnp - **no emulador veio desabilitado por padrão**)
q. ip dhcp-client set 0 disabled=yes (desabilita o cliente dhcp da interface ether1)

15. Listar todos os Pacote habilitados
    a. /system package print
16. Desabilitar os pacotes não utilizados
    a. /system package disable wireless
    b. /system reboot
17. Listar as interfaces

a. /interface print

18. Desabilitar a interfaces que não estão em uso
    a. /interface set 2,3 disabled=yes

Quarta experiência - Ataque nos hashes vazados

1. Acessar **Linux1**
2. No terminal adicionar novo usuário
    a. #adduser edu
    b. password=123abc
    c. Full Name= Eduardo
    d. Room Number= 123
    e. Work Phone= 0000-0000
    f. Home Phone= 1111-1111
    g. Other= abc
3. No terminal verificar as informações desse usuário
    a. #cat /etc/passwd
4. No terminal verificar arquivo de senhas
    a. #cat /etc/shadow
5. No terminal juntar os arquivos passwd e shadow no arquivo quebrahash.txt
    a. #unshadow /etc/passwd /etc/shadow > quebrahash.txt
6. No terminal executar o programa John The Ripper (programa que encontra senhas em arquivos)
    a. #john --wordlist=/usr/share/john/password.lst quebrahash.txt
7. No terminal verificar senhas descobertas pelo John The Ripper
    a. #john --show quebrahash.txt (mostra todos os hashes quebrados pelo programa)

8. **Segurança Mikrotik**
9. Acessar **Mikrotik**
10. Fazer backup das suas configurações
    a. /export file=configuracao
    b. /system backup save name=configuracaoHash
    c. /file print
11. Acessar **Linux1**
12. No terminal baixar as configurações do Mikrotik de forma segura através do sftp
    a. #sftp eduardo@192.0.2.1:configuracao.rsc

b. #sftp eduardo@[2001:db8:2::1]:configuracao.rsc

obs: o sftp utilizar a mesma chave do ssh, portanto é necessário ter feito a transferência da chave rsa anteriormente. Além disso é preciso tomar cuidado com as permissões do usuário: pode desativar o ftp mas não pode tirar a permissão do usuário de usar ftp

Quinta experiência - Spoofing

1. **Ataque Linux**
2. Acessar **Linux2**
3. Abrir o wireshark de capturar a interface eth0
4. Acessar **Linux1**
5. Abrir o wireshark e capturar a interface eth0
6. No terminal executar o hping3 com o endereço de origem falsificado com destino ao **Linux2**
    a. #hping3 -a 192.168.1.3 203.0.113.100 --interface eth0
7. Para falsificar um pacote IPv6, podemos utilizar o comando nping. No entanto para isso é necessário saber o mac address da interface eth0 do Linux e da interface ether1 do Mikrotik
8. No Mikrotik listar o mac address do Mikrotik
    a. /interface print detail
9. No terminal listar o mac address do Linux1
    a. #ip address show
10. No terminal executar o nping com o endereço de origem falsificado com destino ao **Linux2**
    a. #nping -6 -S 3000::1 --dest-ip 2001:db8:1::100 --dest-mac 50:29:00:03:00:00 --source-mac 00:50:00:00:01:00

11. **Segurança Mikrotik**
12. Acessar **Mikrotik**
13. Habilitar o rpf filter IPv4
    a. /ip settings set rp-filter=strict
14. Como não há rpf filter para IPv6 no Mikrotik, aplicar filtros manuais
    a. /ipv6 firewall address-list add address=2001:db8:2::/64 list=CLIENTE-V6
    b. /ipv6 firewall filter add chain=forward in-interface=ether1 src-address-list=CLIENTE-V6
    c. /ipv6 firewall filter add action=drop chain=forward in-interface=ether1
15. Acessar **Linux1**

16. No terminal executar o hping3 com o endereço de origem falsificado com destino ao **Linux2**
    a. #hping3 -a 192.168.1.3 203.0.113.100 --interface eth0
17. No terminal executar o nping com o endereço de origem falsificado com destino ao **Linux2**
    a. #nping -6 -S 3000::1 --dest-ip 2001:db8:2::100 --dest-mac 50:29:00:03:00:00 --source-mac 00:50:00:00:01:00