

Lab Security - Guideline

Security goals: CIA (confidentiality, integrity and availability)

Vulnerabilities and threats

- 1) Reconnaissance
- 2) Eavesdropping
- 3) Access: Masquerading/IP spoofing, Session replay, Back doors
- 4) Denial of Service (DoS)
- 5) Distributed Denial of Service (DDoS)

Wifi attack learning tool:

http://williams.comp.ncat.edu/IA_visualization_labs/security_visual_tools/wireless_attacks/wireless_attacks_demo.html

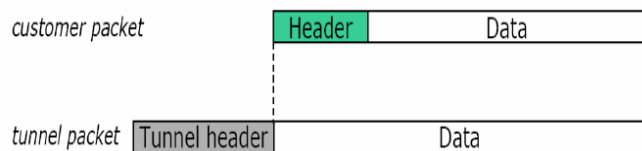
Security solutions

- 1) Firewalls: Packet filtering, NAT
- 2) Intrusion Detection Systems: HIDS, NIDS

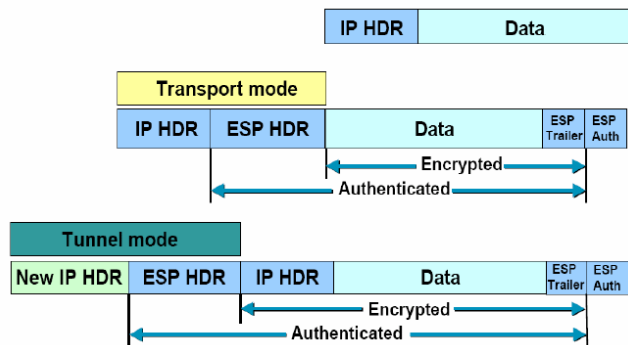
VPN (Virtual Private Network)

- conexiune private peste o rețea publică de date
- Trafic criptat și autentificat

Tunneling



IPSec



Iptables

Tables: filter, nat, mangle

filter

Chains: INPUT, FORWARD, OUTPUT

Targets: ACCEPT, DROP, REJECT, QUEUE, RETURN

Basic Examples:

- lists current rules in iptables:

iptables -L

iptables -L -v

- reset iptables:

iptables -F

iptables -P INPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -P OUTPUT ACCEPT

Usefull tutorial:

<https://help.ubuntu.com/community/IptablesHowTo>

Access lists (ACLs)

1) Standard ACLs

- a) Purpose: identifies traffic based on source IP;

- b) Definition:

Router(config)#access-list access-list-number {deny | permit | remark} source [source-wildcard]

[log]

- access-list-number: 1 – 99, 1300 – 1999

- c) Placing the ACL on an interface:

- i) the standard ACL should be place closed to the traffic destination

- ii) must be applied to the interface (inbound or outbound)

Router(config-if)#ip access-group {access-list-number | access-list-name} {in | out}

Example: block all traffic except that from source 10.1.1.x.

Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255

```
Router(config)#interface fastEthernet0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip access-group 1 in
```

2) Extended ACLs

- a) Purpose: identifies traffic based on several parameters: source addresses, destination address, protocols and port numbers

- b) Definition:

```
Router(config)#access-list access-list-number {deny | permit | remark} protocol source [source-wildcard] [source-port-operator operand] [source-port port-number sau name] destination [destination-wildcard] [destination-port-operator operand] [destination-port port-number sau name] [established]
```

- access-list-number: 100 – 199, 2000 – 2699

- c) Placing the ACL on an interface:

- i) The extended ACL should be place closed to the traffic source
- ii) must be applied to the interface (inbound or outbound)

```
Router(config-if)#ip access-group {access-list-number | access-list-name} {in | out}
```

Example: permit ftp traffic from source 10.1.1.x. to all host inside the network

```
Router(config)# access-list 101 permit tcp 10.1.1.0 0.0.0.255 any eq 21
```

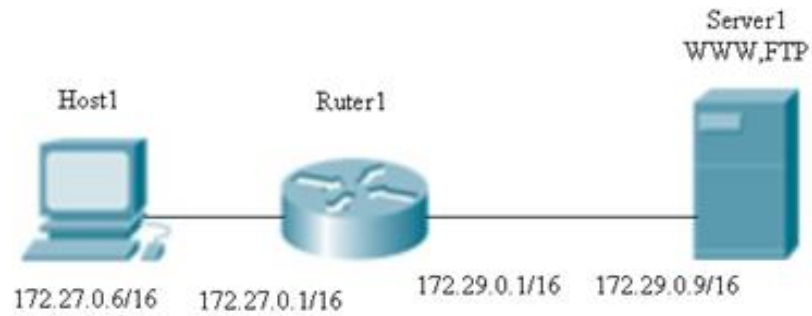
```
Router(config)#interface fastEthernet0/0
```

```
Router(config-if)#ip access-group 101 in
```

Show access lists configuration:

```
Router#show access-lists {access-list-number | access-list-name}
```

Laboratory test configuration:



Requirement1:

- Using a standard ACL block Host1 from accessing Server1

Requirement2:

- delete the previous ACL
- Using an extended ACL block Host1 from accessing the www service on Server1, but permit other services