

MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



qualitytraining
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

Security OSI Layer : **MNDP** (MikroTik Neighbor Discovery protocol)

- MikroTik Neighbor Discovery protocol (MNDP) и LLDP позволяют "найти" другие устройства с MNDP и CDP (Cisco Discovery Protocol) или LLDP в Layer2 broadcast domain.
- показывает за каким интерфейсом находятся какие соседи, показывает его IP / MAC-адреса и несколько дополнительных параметров, связанных с оборудованием
- Список только для чтения.
- Начиная с ROS v6.45 количество записей Neighbor ограничено (общий объем ОЗУ в мегабайтах) * 16 на интерфейс, чтобы избежать исчерпания памяти.
- по умолчанию включен для всех Ethernet-like интерфейсов
- используется протокол UDP и порт 5678*

Security OSI Layer : **MNDP** (MikroTik Neighbor Discovery protocol)

```
[admin@MikroTik] /ip neighbor> print
```

#	INTERFACE	ADDRESS	MAC-ADDRESS	IDENTITY	VERSION	BOARD
0	ether13	192.168.33.2	00:0C:42:00:38:9F	MikroTik	5.99	RB1100AHx2
1	ether11	1.1.1.4	00:0C:42:40:94:25	test-host	5.8	RB1000
2	Local	10.0.11.203	00:02:B9:3E:AD:E0	c2611-r1	Cisco I...	
3	Local	10.0.11.47	00:0C:42:84:25:BA	11.47-750	5.7	RB750
4	Local	10.0.11.254	00:0C:42:70:04:83	tsys-sw1	5.8	RB750G
5	Local	10.0.11.202	00:17:5A:90:66:08	c7200	Cisco I...	

```
/ip neighbor> print detail
```

```
interface=ether3 address=192.168.200.121 address4=192.168.200.121 mac-address=4C:5E:0C:E0:59:BE  
identity="Kossb" platform="MikroTik" version="6.43.13 (long-term)" unpack=none age=37s uptime=1w3d13h48m20s  
software-id="J2VP-oG9o" board="RB951Ui-2HnD" ipv6=no interface-name="bridge1" system-caps=""  
system-caps-enabled=""
```

Security OSI Layer : **MNDP** (MikroTik Neighbor Discovery protocol)* 6.44*

discovery
protocol

L3,4 - UDP

output: in:(none) out:ether1, proto **UDP**, 22.1.1.102:36896->**255.255.255.255:5678**, len 117

output: in:(none) out:ether1, proto **UDP**, 22.1.1.101:46840->**255.255.255.255:5678**, len 119

discovery
protocol

L3,4 - UDP

L2 -
MNDP,
CDP,
LLDP

multicast
output: in:(unknown 0) out:ether1, src-mac xxx, dst-mac **01:00:0c:cc:cc:cc**, eth-proto 0062

multicast
output: in:(unknown 0) out:ether1, src-mac xxx, dst-mac **01:80:c2:00:00:0e**, eth-proto 88c

L2 -
MNDP,
CDP,
LLDP

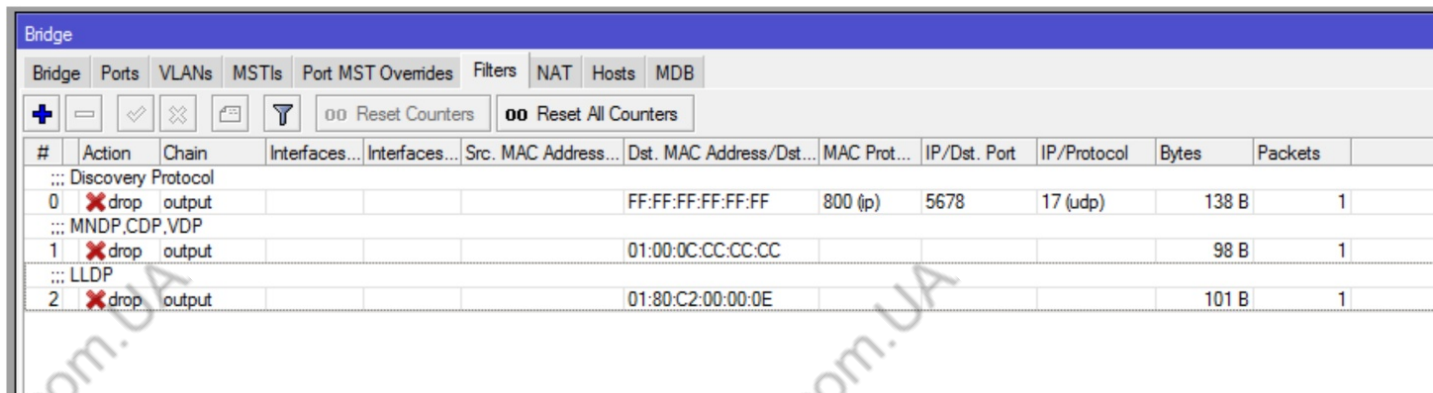
Bridge Filter need in chain OUTPUT: (above 6.44)

output: in:(unknown 0) out:ether1, src-mac 50:00:00:02:00:00, dst-mac ff:ff:ff:ff:ff:ff, eth-proto 0800, **UDP**, 22.1.1.102:5678->**255.255.255.255:5678**, len 138

output: in:(unknown 0) out:ether1, src-mac 50:00:00:02:00:00, dst-mac **01:00:0c:cc:cc:cc**, eth-proto 0062

output: in:(unknown 0) out:ether1, src-mac 50:00:00:02:00:00, dst-mac **01:80:c2:00:00:0e**, eth-proto 88c

Security OSI Layer : **MNDP** (MikroTik Neighbor Discovery protocol)



#	Action	Chain	Interfaces...	Interfaces...	Src. MAC Address...	Dst. MAC Address/Dst...	MAC Prot...	IP/Dst. Port	IP/Protocol	Bytes	Packets
::: Discovery Protocol											
0	✖ drop	output				FF:FF:FF:FF:FF:FF	800 (p)	5678	17 (udp)	138 B	1
::: MNDP, CDP, VDP											
1	✖ drop	output				01:00:0C:CC:CC:CC				98 B	1
::: LLDP											
2	✖ drop	output				01:80:C2:00:00:0E				101 B	1

/interface bridge filter (above 6.44)

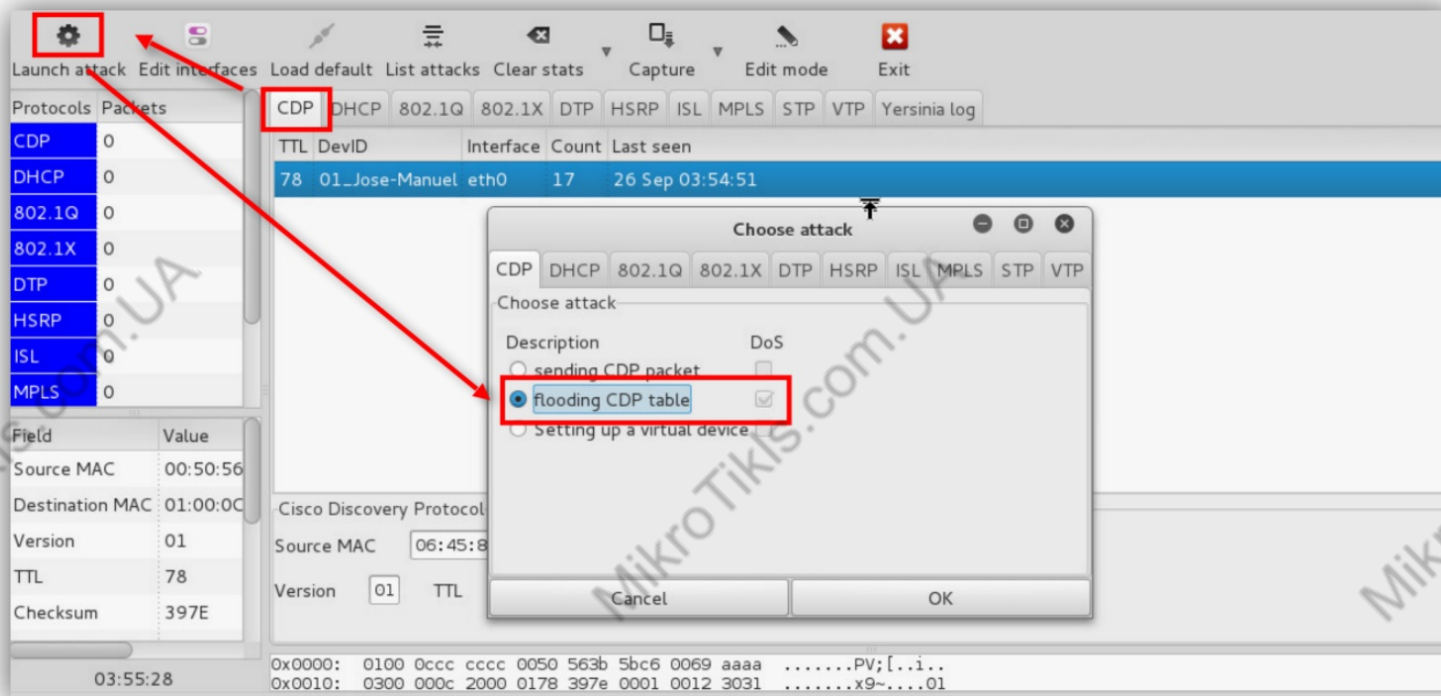
add action=drop chain=output comment="Discovery Protocol" dst-mac-address=FF:FF:FF:FF:FF:FF/FF:FF:FF:FF:FF:FF
dst-port=5678 ip-protocol=udp mac-protocol=ip

add action=drop chain=output comment=MNDP, CDP, VDP dst-mac-address=01:00:0C:CC:CC:CC/FF:FF:FF:FF:FF:FF

add action=drop chain=output comment=LLDP dst-mac-address=01:80:C2:00:00:0E/FF:FF:FF:FF:FF:FF

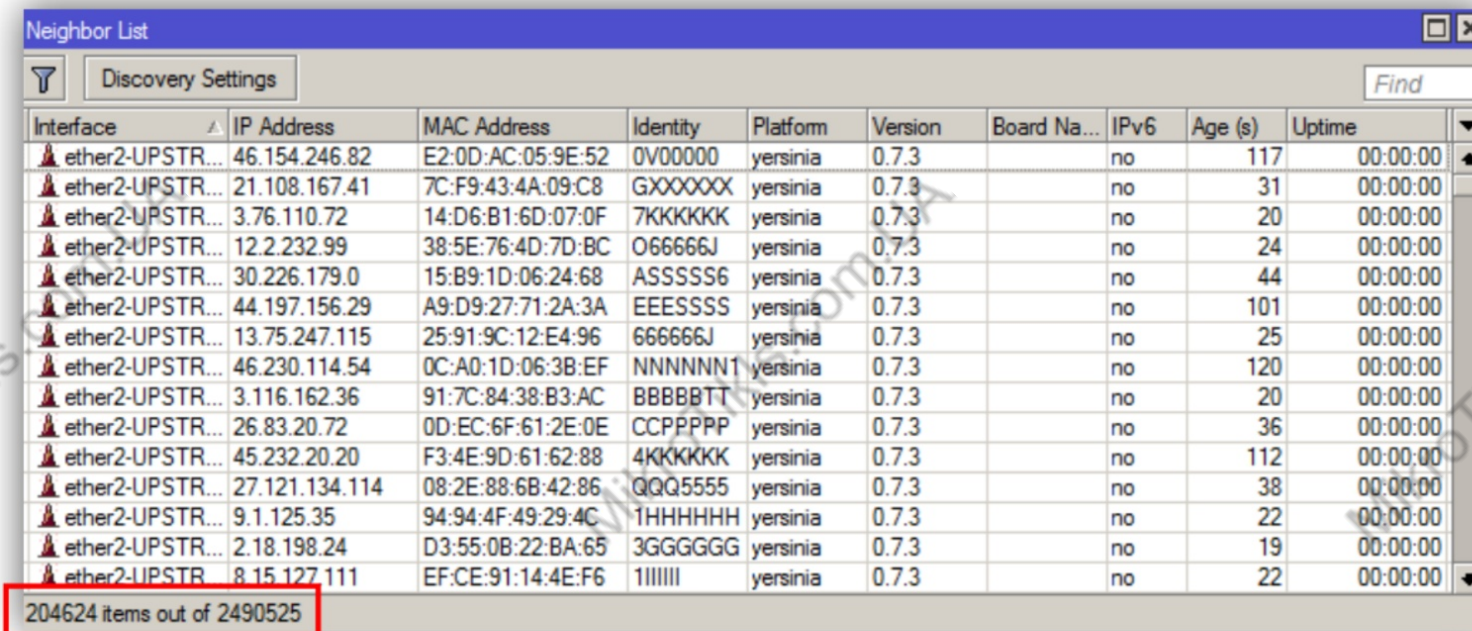
Security OSI Layer : **MNDP - Attack**

Посылка “фейковых” CDP соседей на устройство MikroTik, Cisco и т.д.



Security OSI Layer : **MNDP - Attack**

MikroTik получает сотни тысяч «фальшивых» соседей с рандомной информацией.

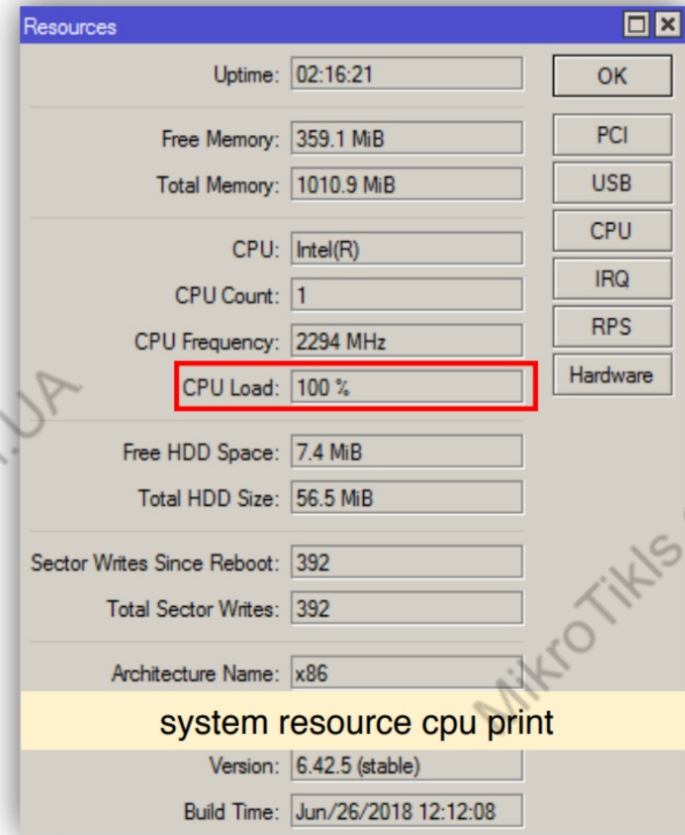
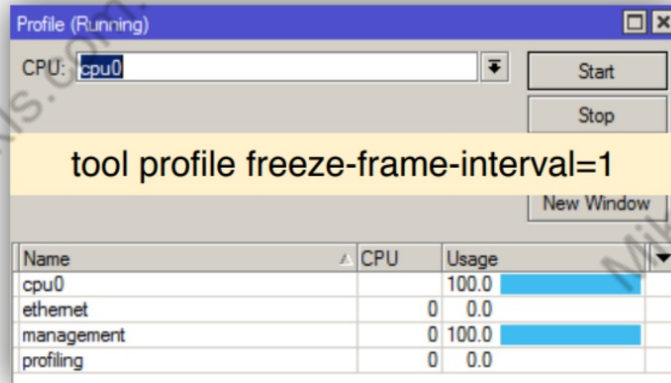


Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
ether2-UPSTR...	46.154.246.82	E2:0D:AC:05:9E:52	0V00000	yersinia	0.7.3		no	117	00:00:00
ether2-UPSTR...	21.108.167.41	7C:F9:43:4A:09:C8	GXXXXXX	yersinia	0.7.3		no	31	00:00:00
ether2-UPSTR...	3.76.110.72	14:D6:B1:6D:07:0F	7KKKKKK	yersinia	0.7.3		no	20	00:00:00
ether2-UPSTR...	12.2.232.99	38:5E:76:4D:7D:BC	O66666J	yersinia	0.7.3		no	24	00:00:00
ether2-UPSTR...	30.226.179.0	15:B9:1D:06:24:68	ASSSSS6	yersinia	0.7.3		no	44	00:00:00
ether2-UPSTR...	44.197.156.29	A9:D9:27:71:2A:3A	EESSSSS	yersinia	0.7.3		no	101	00:00:00
ether2-UPSTR...	13.75.247.115	25:91:9C:12:E4:96	666666J	yersinia	0.7.3		no	25	00:00:00
ether2-UPSTR...	46.230.114.54	0C:A0:1D:06:3B:EF	NNNNNN1	yersinia	0.7.3		no	120	00:00:00
ether2-UPSTR...	3.116.162.36	91:7C:84:38:B3:AC	BBBBBTT	yersinia	0.7.3		no	20	00:00:00
ether2-UPSTR...	26.83.20.72	0D:EC:6F:61:2E:0E	CCPPPPP	yersinia	0.7.3		no	36	00:00:00
ether2-UPSTR...	45.232.20.20	F3:4E:9D:61:62:88	4KKKKKK	yersinia	0.7.3		no	112	00:00:00
ether2-UPSTR...	27.121.134.114	08:2E:88:6B:42:86	QQQ5555	yersinia	0.7.3		no	38	00:00:00
ether2-UPSTR...	9.1.125.35	94:94:4F:49:29:4C	1HHHHHH	yersinia	0.7.3		no	22	00:00:00
ether2-UPSTR...	2.18.198.24	D3:55:0B:22:BA:65	3GGGGGG	yersinia	0.7.3		no	19	00:00:00
ether2-UPSTR...	8.15.127.111	EF:CE:91:14:4E:F6	1IIIIII	yersinia	0.7.3		no	22	00:00:00

204624 items out of 2490525

Security OSI Layer : **MNDP - Attack**

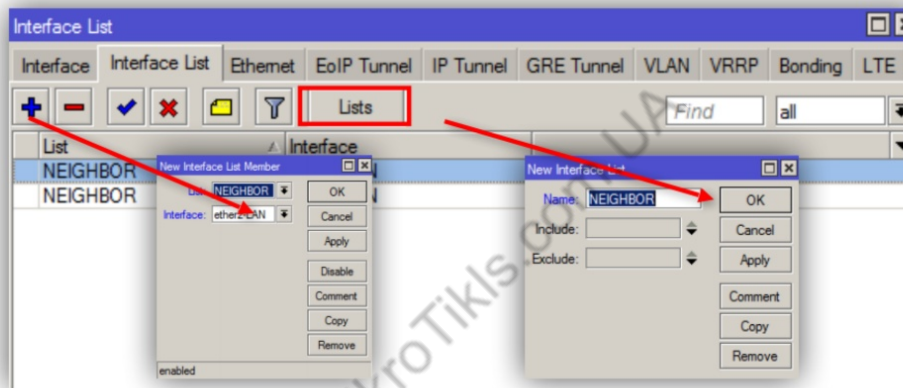
Это тратит ресурсы
роутера и влияет на
производительность



Security OSI Layer : **MNDP - Attack**

Для предотвращения такого рода атак мы должны избирательно выбирать какие интерфейсы могут общаться используя MNDP / CDP / LLDP протоколы.

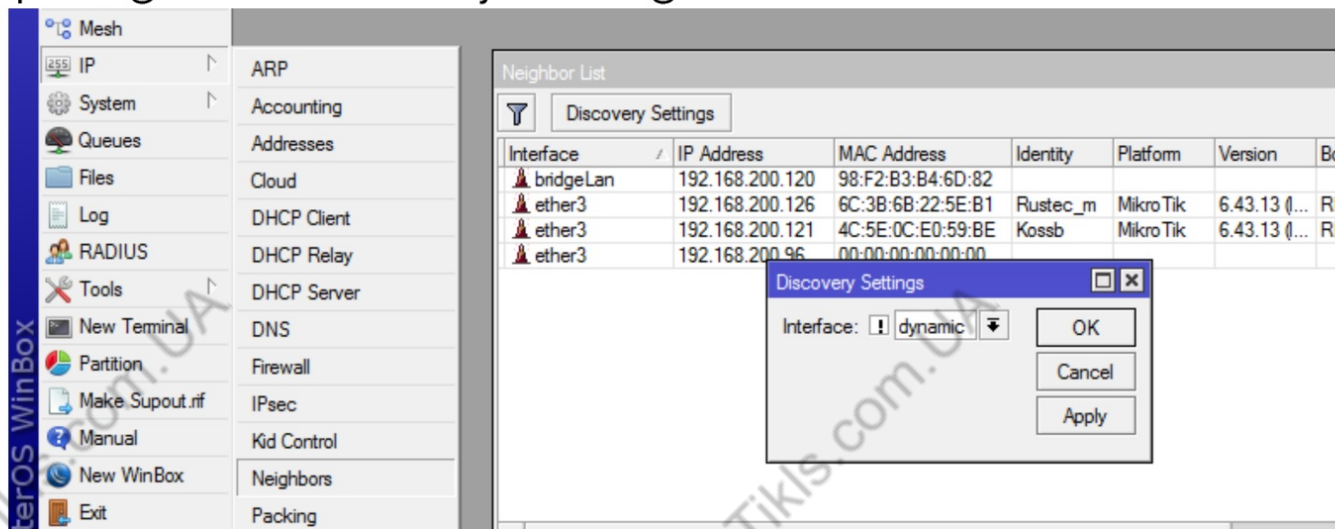
Создайте «Interface List» и выберите интерфейсы, которым разрешено использовать эти протоколы



```
/interface list add name=NEIGHBOR
/interface list member
add interface=etherX list=NEIGHBOR
add interface=etherY list=NEIGHBOR
```


Security OSI Layer : **MNDP** (MikroTik Neighbor Discovery protocol)

/ip neighbor discovery-settings



- В этом меню можно изменить состояние интерфейса независимо от того, участвует он в обнаружении соседей или нет
- Удаление интерфейса из этой конфигурации меню отключит как обнаружение соседей на этом интерфейсе, так и возможность обнаружения самого устройства на этом интерфейсе.
- ваши роутеры все равно будут уязвимы к данной атаке. Почему? Анализ и защита:= Demo+ LAB

MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



qualitytraining
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

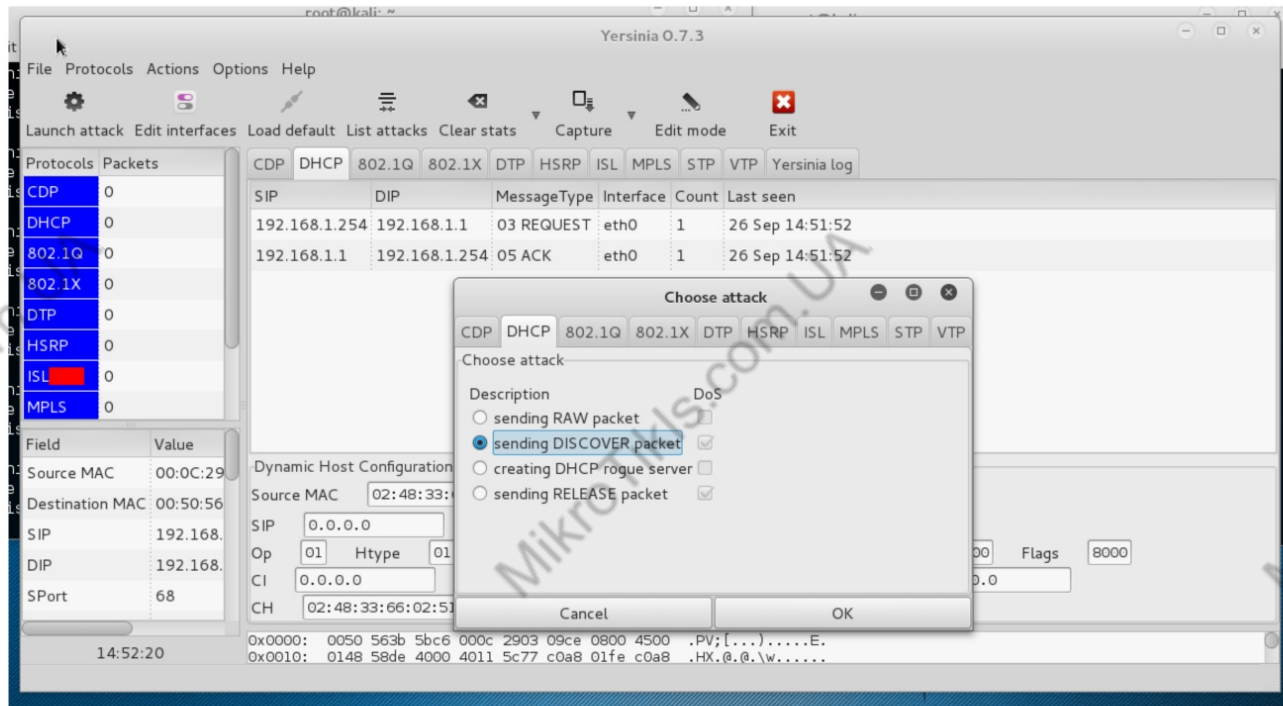
DHCP Starvation Attack

DHCP Starvation

- Атака, осуществляемая при помощи протокола DHCP. DHCP-пул, из которого клиенты получают IP-адреса, ограничен. Например, это может быть 253 адреса (при маске 255.255.255.0)
- Атакующее устройство запрашивает себе IP-адрес у DHCP-сервера и "получает" его
- MAC-адрес атакующего устройства изменяется и оно запрашивает следующий, уже другой IP-адрес, маскируясь под нового клиента
- Такие действия повторяются до тех пор, пока весь пул IP-адресов на сервере не будет исчерпан.

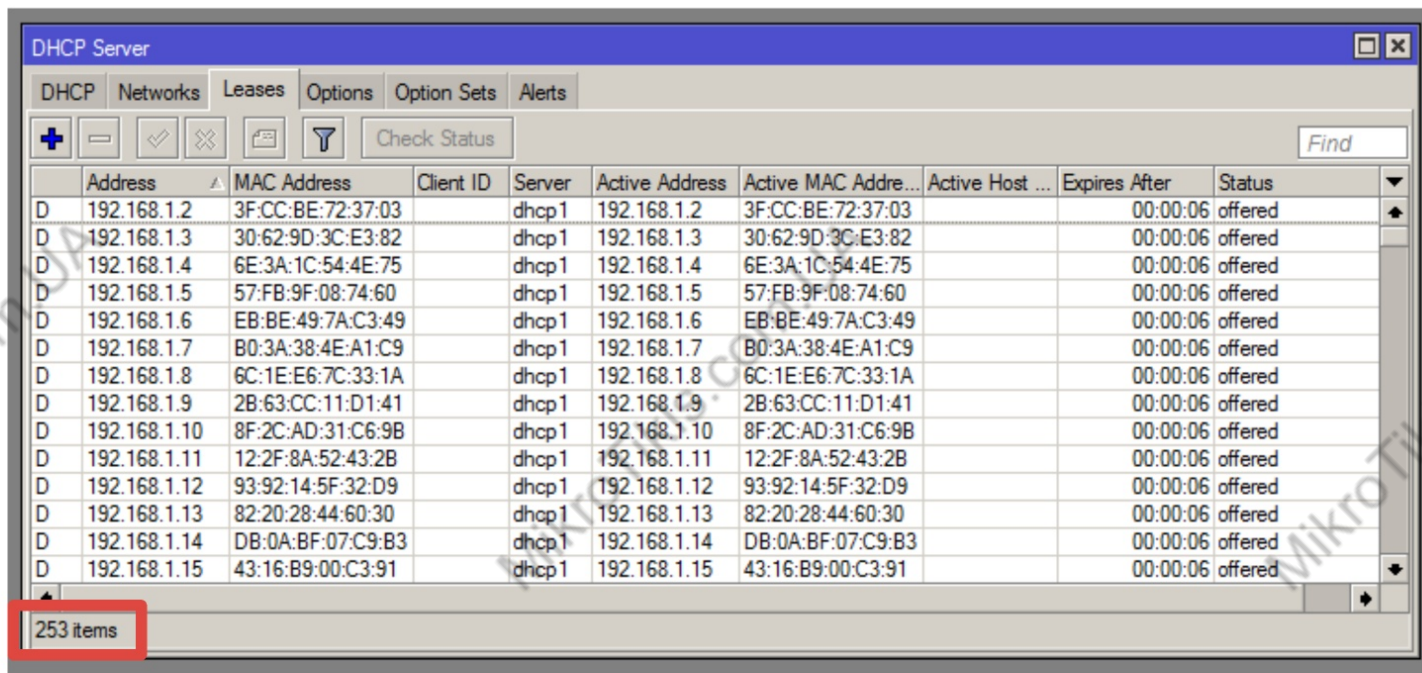
DHCP Starvation

К примеру, той же утилитой (yersinia) посылается множество “fake” DHCP requests (запросов) на роутер(DHCP-server)



DHCP Starvation

Злоумышленник исчерпывает весь pool (DHCP leases) множественными dhcp запросами к роутеру. И продолжает посылать дальше Discovery...



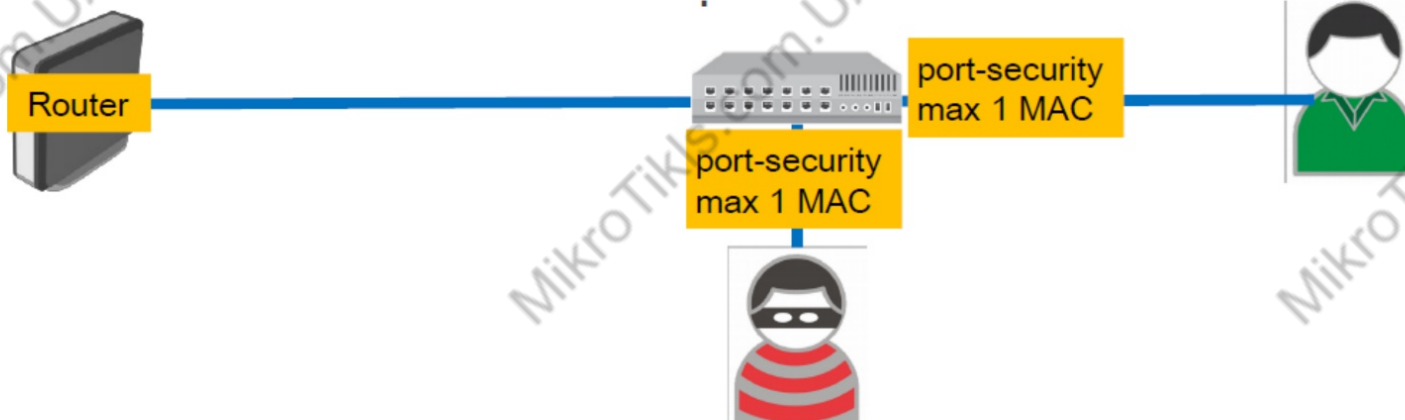
	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host	Expires After	Status
D	192.168.1.2	3F:CC:BE:72:37:03		dhcp1	192.168.1.2	3F:CC:BE:72:37:03		00:00:06	offered
D	192.168.1.3	30:62:9D:3C:E3:82		dhcp1	192.168.1.3	30:62:9D:3C:E3:82		00:00:06	offered
D	192.168.1.4	6E:3A:1C:54:4E:75		dhcp1	192.168.1.4	6E:3A:1C:54:4E:75		00:00:06	offered
D	192.168.1.5	57:FB:9F:08:74:60		dhcp1	192.168.1.5	57:FB:9F:08:74:60		00:00:06	offered
D	192.168.1.6	EB:BE:49:7A:C3:49		dhcp1	192.168.1.6	EB:BE:49:7A:C3:49		00:00:06	offered
D	192.168.1.7	B0:3A:38:4E:A1:C9		dhcp1	192.168.1.7	B0:3A:38:4E:A1:C9		00:00:06	offered
D	192.168.1.8	6C:1E:E6:7C:33:1A		dhcp1	192.168.1.8	6C:1E:E6:7C:33:1A		00:00:06	offered
D	192.168.1.9	2B:63:CC:11:D1:41		dhcp1	192.168.1.9	2B:63:CC:11:D1:41		00:00:06	offered
D	192.168.1.10	8F:2C:AD:31:C6:9B		dhcp1	192.168.1.10	8F:2C:AD:31:C6:9B		00:00:06	offered
D	192.168.1.11	12:2F:8A:52:43:2B		dhcp1	192.168.1.11	12:2F:8A:52:43:2B		00:00:06	offered
D	192.168.1.12	93:92:14:5F:32:D9		dhcp1	192.168.1.12	93:92:14:5F:32:D9		00:00:06	offered
D	192.168.1.13	82:20:28:44:60:30		dhcp1	192.168.1.13	82:20:28:44:60:30		00:00:06	offered
D	192.168.1.14	DB:0A:BF:07:C9:B3		dhcp1	192.168.1.14	DB:0A:BF:07:C9:B3		00:00:06	offered
D	192.168.1.15	43:16:B9:00:C3:91		dhcp1	192.168.1.15	43:16:B9:00:C3:91		00:00:06	offered

253 items

Preventing DHCP Starvation Attacks

Защитить сеть от данной атаки можно с помощью настройки портов коммутатора

- Злоумышленник использует новый MAC-адрес для запроса нового адреса
- Следовательно, необходимо ограничить количество MAC-адресов на портах Switch
- Злоумышленник не сможет арендовать больше IP-адресов, чем разрешенное кол-во MAC адресов на порту

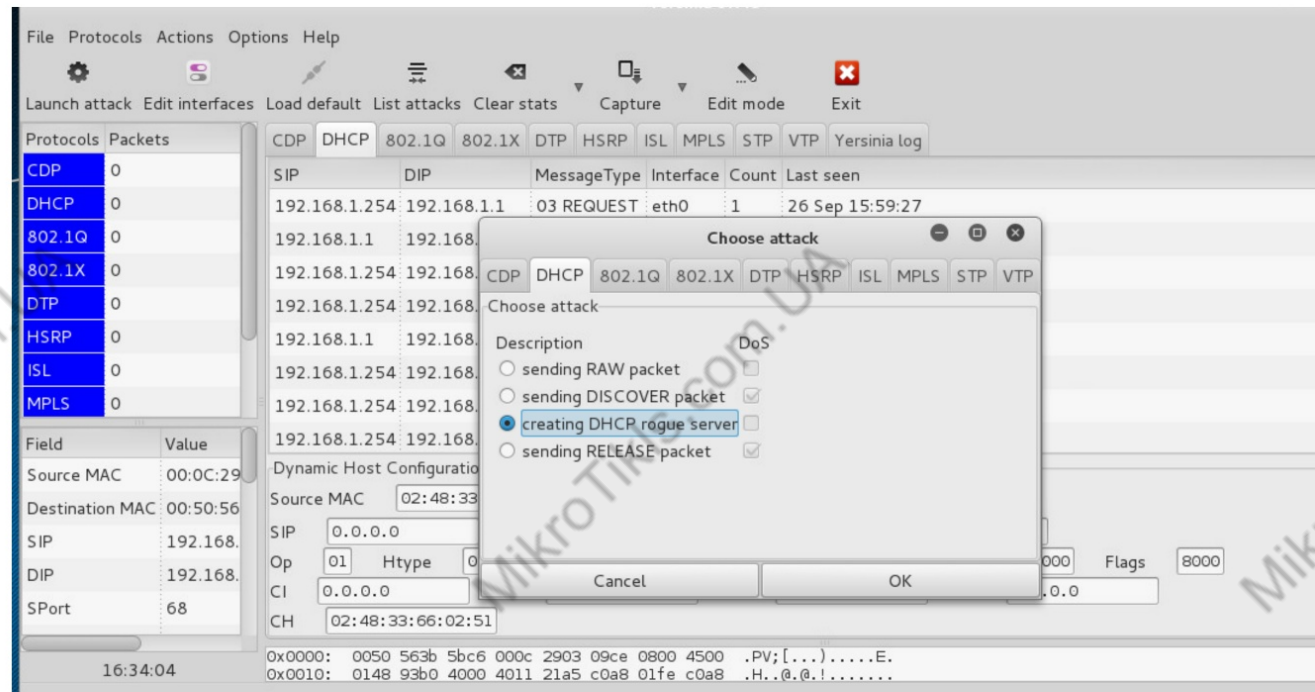


Rogue DHCP Server (DHCP-spoofing)

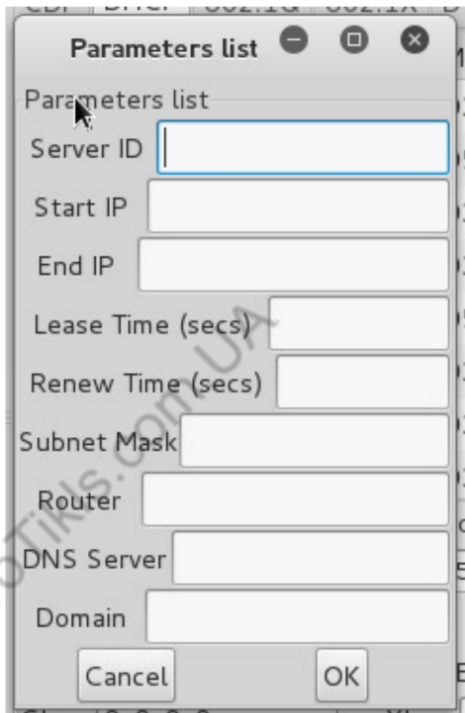
При DHCP-spoofing злоумышленник настраивает в сети ненастоящий DHCP-сервер, чтобы выдавать для клиентов DHCP-адреса. Цель этой атаки – заставить клиентов использовать ложную службу доменных имен (DNS) и Windows-службу имён Internet (сервер WINS), а также использовать узел или устройство злоумышленника в качестве шлюза по умолчанию.

Перед DHCP-spoofing часто используется атака истощения ресурсов DHCP (DHCP Starvation) для отказа обслуживания санкционированного DHCP-сервера, благодаря чему гораздо проще внедрить в сеть фиктивный DHCP-сервер.

Rogue DHCP Server (DHCP-spoofing)



Rogue DHCP Server (DHCP-spoofing)



The image shows a 'Parameters list' dialog box with the following fields:

- Server ID
- Start IP
- End IP
- Lease Time (secs)
- Renew Time (secs)
- Subnet Mask
- Router
- DNS Server
- Domain

At the bottom are 'Cancel' and 'OK' buttons.

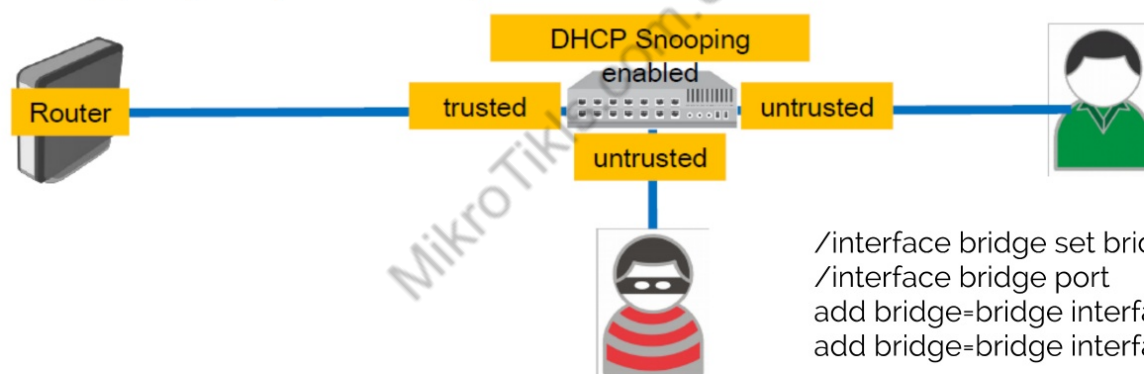
- **Server IP** – the IP server, the name of which will send the answer the DHCP (xxx.xxx.xxx.xxx);
- **Start IP** – initial IP, issued to customers -address address range (xxx.xxx.xxx.xxx);
- **End IP** – IP, issued to customers -address address range (xxx.xxx.xxx.xxx);
- **Time The Lease (secs)** – The time in seconds for which the address is given
- **Time The Renew (secs)** – The time in seconds how many clients must renew the address lease
- **Subnet Mask** – Subnet mask for the clients (xxx.xxx.xxx.xxx);
- **Router** – router address issued to clients (xxx.xxx.xxx.xxx ,the address of a fake router);
- **DNS Server** – DNS server provided to clients (xxx.xxx.xxx.xxx ,the address of a fake DNS server);
- **The Domain** – a domain name in the local area network (abc.def);

Preventing Rogue DHCP Server

включение DHCP snooping ((config)#ip dhcp snooping vlan 20)

настройка доверенных портов на интерфейсах (по умолчанию все порты ненадежные) ((config-if)#ip dhcp snooping trust)

указание адреса доверенного DHCP сервера, который доступен через доверенный порт. ((config)#ip dhcp-server 10.1.1.1)



```
/interface bridge set bridge1 idhcp-snooping=yes  
/interface bridge port  
add bridge=bridge interface=ether1 trusted=yes  
add bridge=bridge interface=ether2
```

https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#DHCP_Snooping_and_DHCP_Option_82

MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



qualitytraining
Succeed with Quality

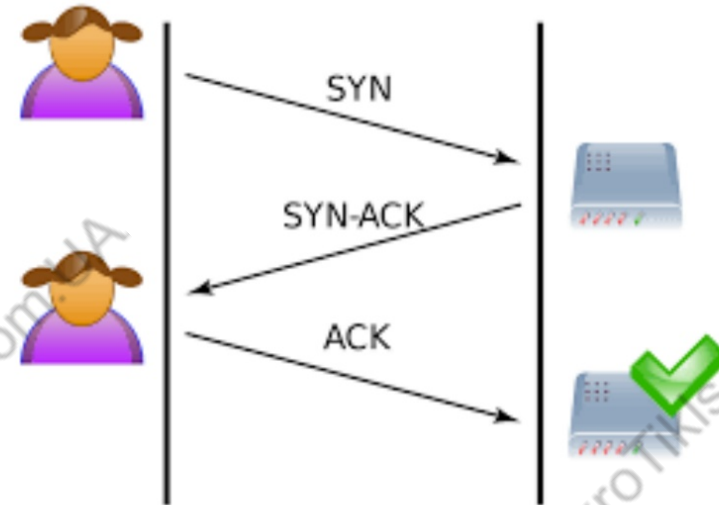
MTI-GROUP LLC / network academy

V.21-01

TCP SYN Attack

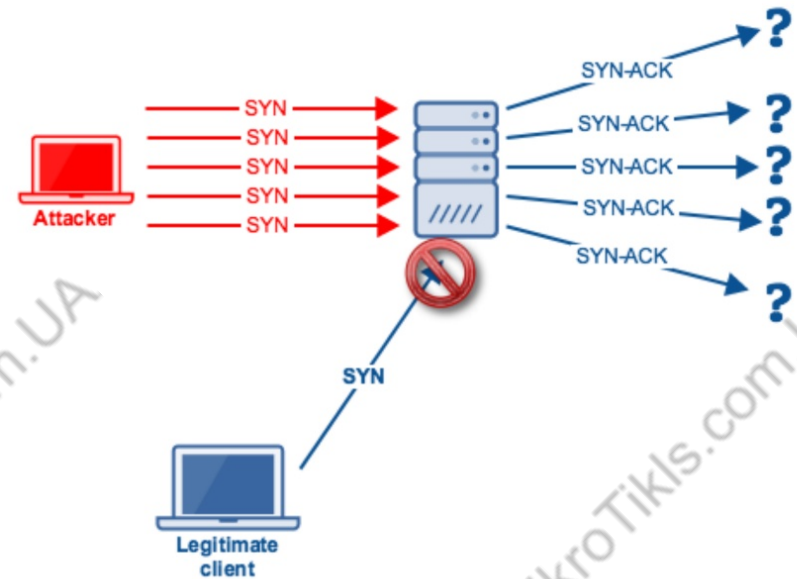
Согласно процессу «трёхкратного рукопожатия» TCP,

- клиент посылает пакет с установленным флагом SYN (synchronize).
- В ответ на него сервер должен ответить комбинацией флагов SYN+ACK (acknowledges).
- После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным.



TCP SYN Attack

- Принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере (цели атаки) очередь на подключения.
- При этом он игнорирует SYN+ACK пакеты цели, не высывая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес.
- В очереди подключений появляются так называемые полуоткрытые соединения (англ. half-open connection), ожидающие подтверждения от клиента. По истечении определенного тайм-аута эти подключения отбрасываются.
- Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений.
- Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь, либо устанавливают её с существенными задержками.



TCP SYN Attack

Scanning available ports on target, commonly used target is 80/http service

```
round-trip min/avg/max = 0.070/0.070/0.0 ms
root@kali:~# nmap 192.168.1.1

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-09-26 04:33 WIB
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
179/tcp    open  bgp
443/tcp    open  https
2000/tcp   open  cisco-sccp
8291/tcp   open  unknown
MAC Address: 00:50:56:3B:5B:C6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
root@kali:~# hping3 --flood --rand-source --udp -p 53 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

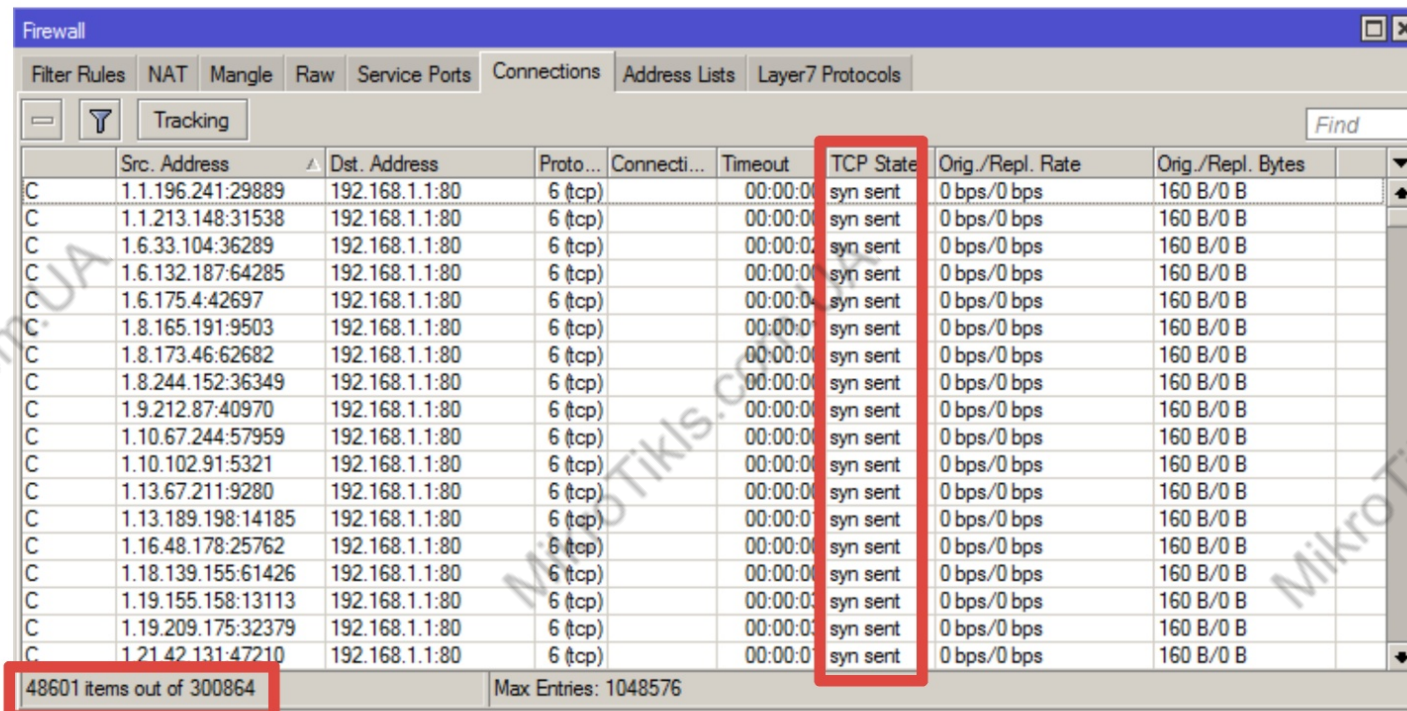
TCP SYN Attack

Download and install "hping3" and run command bellow

```
root@kali:~# hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

TCP SYN Attack

"IP > Firewall > Connections" please observe the "syn sent" from random source addresses



The screenshot shows the Mikrotik WinBox Firewall Connections tab. A list of connections is displayed, all with the state 'syn sent'. The 'TCP State' column is highlighted with a red box. At the bottom left, a status bar indicates '48601 items out of 300864' and 'Max Entries: 1048576', also highlighted with a red box.

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	1.1.196.241:29889	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.1.213.148:31538	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.6.33.104:36289	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.6.132.187:64285	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.6.175.4:42697	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.8.165.191:9503	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.8.173.46:62682	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.8.244.152:36349	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.9.212.87:40970	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.10.67.244:57959	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.10.102.91:5321	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.13.67.211:9280	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.13.189.198:14185	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.16.48.178:25762	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.18.139.155:61426	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.19.155.158:13113	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.19.209.175:32379	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B
C	1.21.42.131:47210	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B

48601 items out of 300864 Max Entries: 1048576

TCP SYN Attack

Torch interface traffic

Torch

Basic

Interface: ether2-UPSTREAM

Entry Timeout: 00:00:03 s

Collect

☒ Src. Address ☒ Src. Address6

☒ Dst. Address ☒ Dst. Address6

☐ MAC Protocol ☒ Port

☒ Protocol ☐ VLAN Id

☐ DSCP

Filters

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Start

Stop

Close

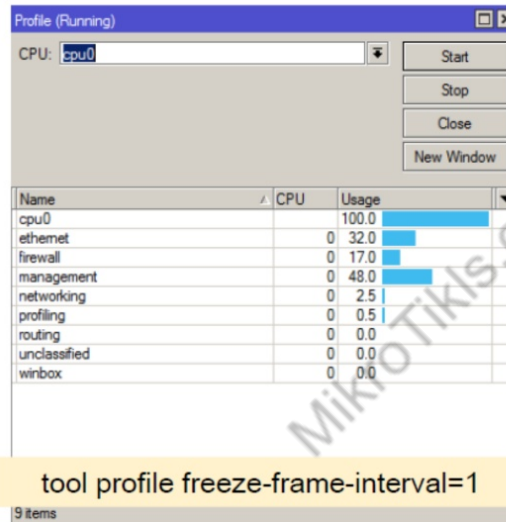
New Window

Et...	Prot...	Src...	Dest...	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pa
800 (ip)	6 (tcp)	1.250.82.222.2059	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.246.185.126.2069	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.6.189.216.2149	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.171.180.16.2161	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.55.102.115.2429	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	4.4.55.160.2464	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.251.194.197.2657	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.63.96.213.2820	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.100.185.79.2878	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.219.212.187.2897	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	4.26.6.116.3019	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.150.129.7.3101	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	1.184.139.122.3135	192.168.1.1:80 (http)			0 bps	1392 bps	0	
800 (ip)	6 (tcp)	3.219.251.220.3280	192.168.1.1:80 (http)			0 bps	1392 bps	0	

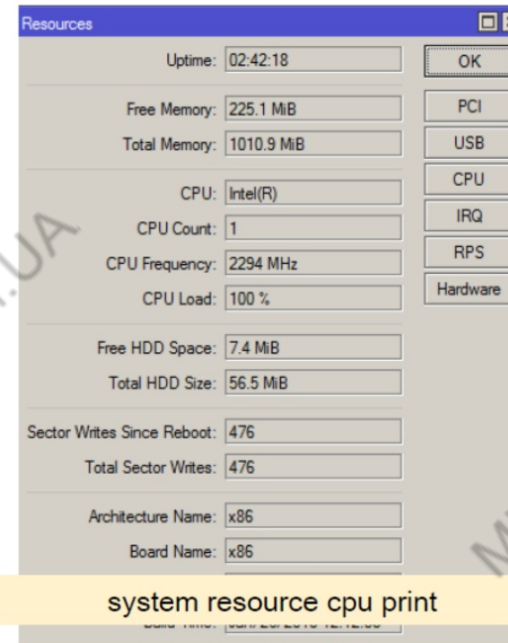
13320 items Total Tx: 0 bps Total Rx: 38.5 Mbps Total Tx Packet: 0 Total Rx Packet: 27 691

TCP SYN Attack

The attack is exhausting the resources of the router and impacting the performance



tool profile freeze-frame-interval=1



system resource cpu print

Preventing TCP SYN Attack

- Rate-limiting for each new tcp connection
- Reduce syn-received timer
- And setup tcp syn-cookies

Preventing TCP SYN Attack

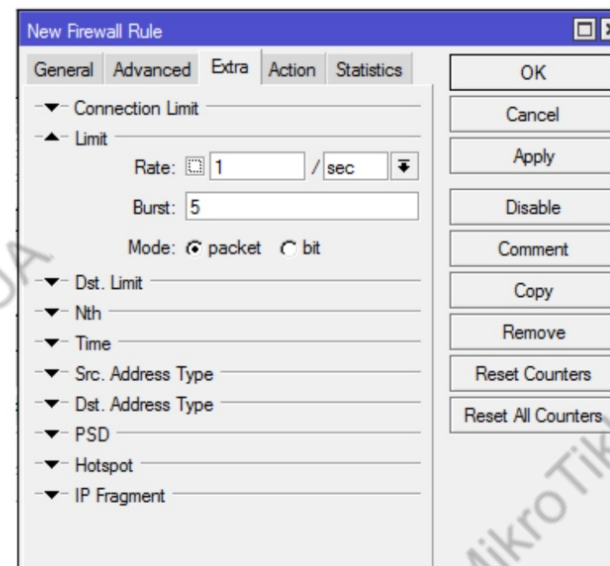
ip firewall filter (extra limit)

Предназначено для ограничения количества передаваемых пакетов:

Rate – количество пакетов в секунду (минуту/час).

Burst – Количество неучитываемых пакетов (пакетов не входящих в packet rate).

Extra - Limit



Rate Limit and ICMP or other

The screenshot displays the Mikrotik WinBox Firewall configuration interface. On the left, the 'Firewall' tab is active, showing a list of filter rules. On the right, the 'Firewall Rule' configuration window is open, showing the 'General' tab.

Firewall Rule Configuration (General Tab):

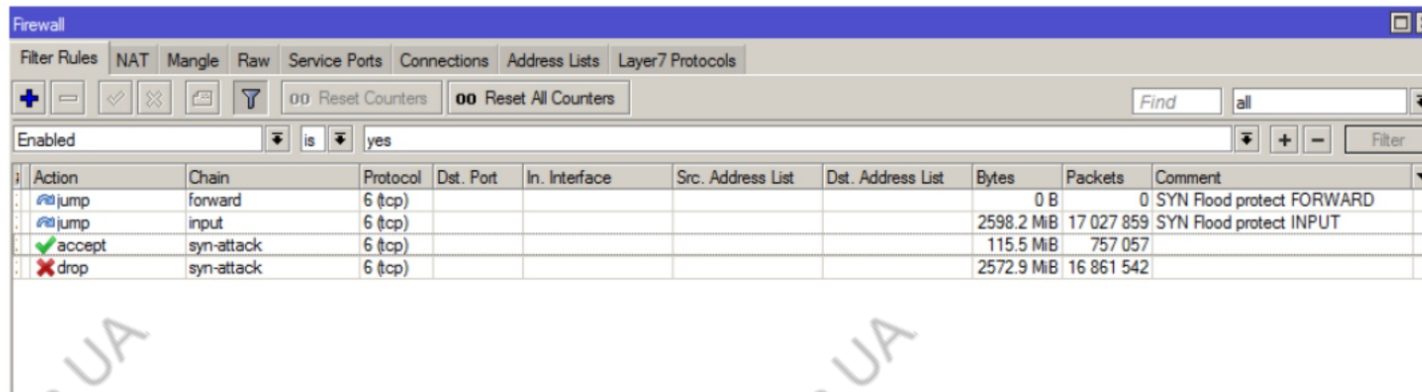
- Connection Limit: ☐ (unchecked)
- Limit: ☐ (checked)
 - Rate: 1 / sec
 - Burst: 5
- Dst. Limit: ☐ (unchecked)
- Nth: ☐ (unchecked)

Firewall Rule List:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✓ acc...	input			1 (icmp)					22.0 KB	15
1	✗ drop	input			1 (icmp)					10.3 KB	7

Preventing TCP SYN Attack

- Creating firewall for preventing tcp SYN flood



Action	Chain	Protocol	Dst. Port	In. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
jump	forward	6 (tcp)					0 B	0	SYN Flood protect FORWARD
jump	input	6 (tcp)					2598.2 MiB	17 027 859	SYN Flood protect INPUT
accept	syn-attack	6 (tcp)					115.5 MiB	757 057	
drop	syn-attack	6 (tcp)					2572.9 MiB	16 861 542	

/ip firewall filter

```
add action=jump chain=forward comment="SYN Flood protect FORWARD" connection-state=new  
jump-target=syn-attack protocol=tcp tcp-flags=syn
```

```
add action=jump chain=input comment="SYN Flood protect INPUT" connection-state=new jump-  
target=syn-attack protocol=tcp tcp-flags=syn
```

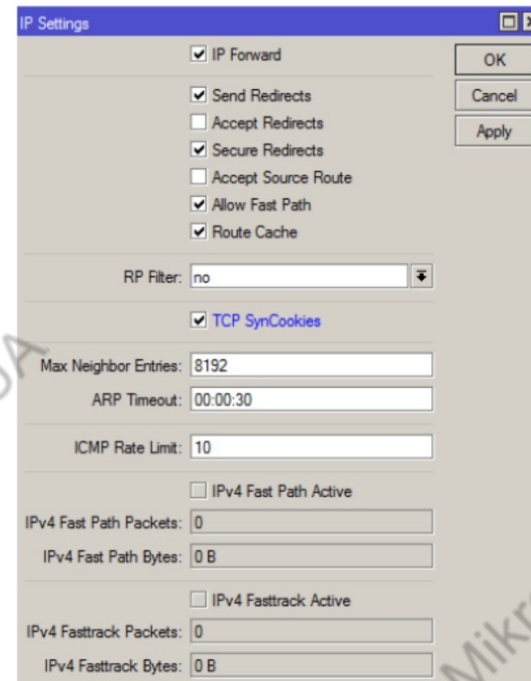
```
add action=accept chain=syn-attack connection-state=new limit=400,5:packet protocol=tcp tcp-  
flags=syn
```

```
add action=drop chain=syn-attack connection-state=new protocol=tcp tcp-flags=syn
```

use RAW if not use conntrack!

Preventing TCP SYN Attack

- IP > Settings and enable “TCP SynCookies”



```
/ip settings set tcp-syncookies=yes
```

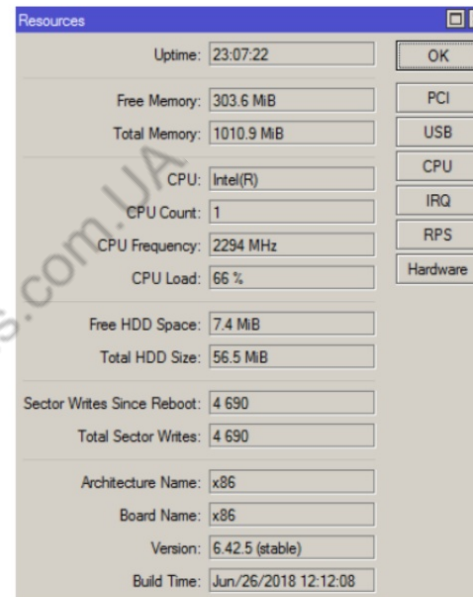
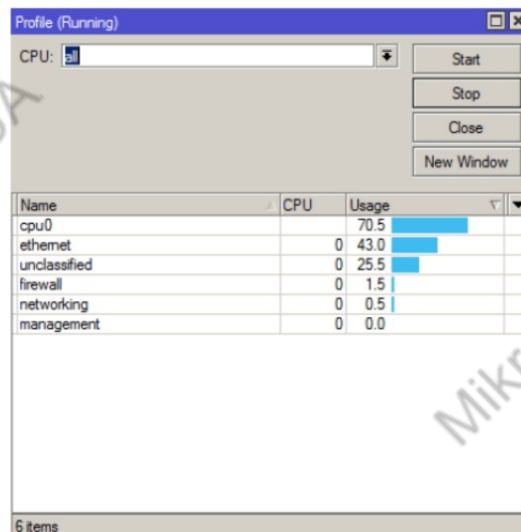
Preventing TCP SYN Attack

запустим снова hping3

```
root@kali:~# hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.1  
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 120 data bytes  
hping in flood mode, no replies will be shown
```


Preventing TCP SYN Attack

- These rules are stopping the tcp SYN attack, but still affecting the CPU resources. (*need more powerful router for preventing*)



MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



qualitytraining
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

UDP flood

- UDP flood – сетевая атака типа «отказ в обслуживании», использующая бессеансовый режим протокола UDP
- Заключается в отправке множества UDP-пакетов на определённые или случайные номера портов удалённого хоста, который для каждого полученного пакета должен определить соответствующее приложение, убедиться в отсутствии его активности и отправить ответное ICMP-сообщение «адресат недоступен»
- В итоге атакуемая система окажется перегруженной: в протоколе UDP механизм предотвращения перегрузок отсутствует, поэтому после начала атаки паразитный трафик быстро захватит всю доступную полосу пропускания, и полезному трафику останется лишь малая её часть
- Подменив IP-адреса источников в UDP-пакетах, злоумышленник может перенаправить поток ICMP-ответов и тем самым сохранить работоспособность атакующих хостов, а также обеспечить их анонимность
- Частным случаем является атака UDP Flood DNS, использующая порт 53 и загружающая сервер DNS UDP-запросами о его домене или IP-адресе несуществующего домена – объём ответов при этом значительно превышает объём запросов

UDP flood attack

- Scanning available port on target, commonly used target is 53/dns service

```
root@kali:~# nmap 192.168.1.1
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-09-26 04:33 WIB
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
179/tcp   open  bgp
443/tcp   open  https
2000/tcp  open  cisco-scp
8291/tcp  open  unknown
MAC Address: 00:50:56:3B:5B:C6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```

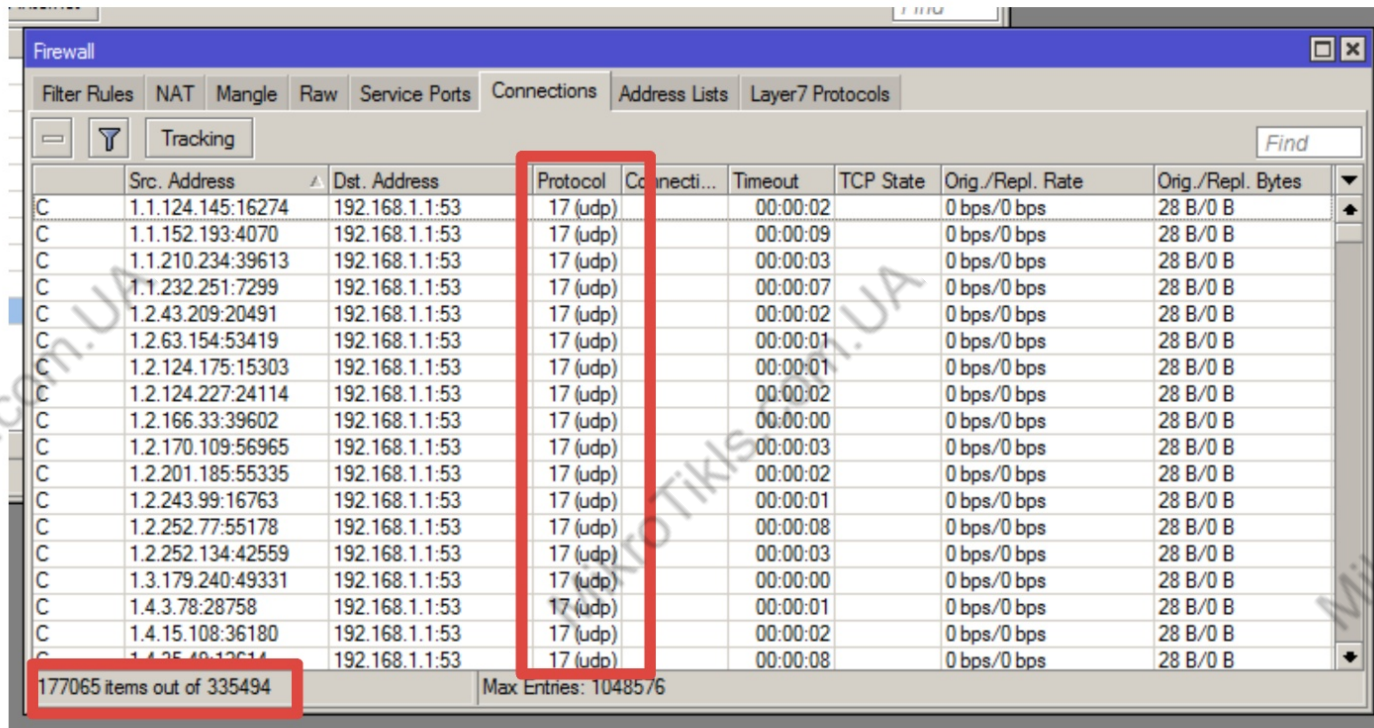
UDP flood attack

- Start attacking UDP protocol port 53(dns) with hping3

```
root@kali:~# hping3 --flood --rand-source --udp -p 53 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```


UDP flood attack

"IP > Firewall > Connections" please observe "udp" protocol from random source addresses



The screenshot shows the Mikrotik WinBox Firewall Connections tab. A red rectangle highlights the 'Protocol' column, which contains '17 (udp)' for all entries. Another red rectangle highlights the status bar at the bottom left, which reads '177065 items out of 335494'. The table below shows a list of connections from various source IP addresses to 192.168.1.1:53.

	Src. Address	Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	1.1.124.145:16274	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.1.152.193:4070	192.168.1.1:53	17 (udp)		00:00:09		0 bps/0 bps	28 B/0 B
C	1.1.210.234:39613	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B
C	1.1.232.251:7299	192.168.1.1:53	17 (udp)		00:00:07		0 bps/0 bps	28 B/0 B
C	1.2.43.209:20491	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.2.63.154:53419	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.2.124.175:15303	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.2.124.227:24114	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.2.166.33:39602	192.168.1.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	1.2.170.109:56965	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B
C	1.2.201.185:55335	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.2.243.99:16763	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.2.252.77:55178	192.168.1.1:53	17 (udp)		00:00:08		0 bps/0 bps	28 B/0 B
C	1.2.252.134:42559	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B
C	1.3.179.240:49331	192.168.1.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	1.4.3.78:28758	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B
C	1.4.15.108:36180	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.4.25.40:12614	192.168.1.1:53	17 (udp)		00:00:08		0 bps/0 bps	28 B/0 B

177065 items out of 335494 Max Entries: 1048576

UDP flood attack

Torch interface traffic

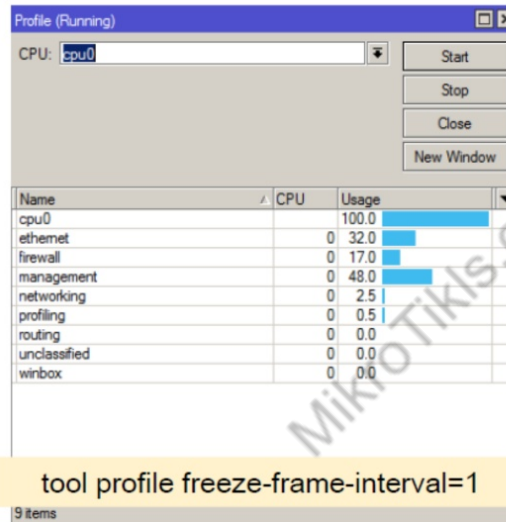
The screenshot shows the Torch application window. The 'Basic' tab is selected, showing the interface as 'ether2-UPSTREAM' and an entry timeout of '00:00:03'. The 'Collect' section has checkboxes for 'Src. Address', 'Dst. Address', 'MAC Protocol', 'Port', 'Protocol', 'VLAN Id', and 'DSCP'. The 'Filters' section has input fields for 'Src. Address', 'Dst. Address', 'Src. Address6', 'Dst. Address6', 'MAC Protocol', 'Protocol', 'Port', 'VLAN Id', and 'DSCP'. The 'Start', 'Stop', 'Close', and 'New Window' buttons are on the right. The main table displays traffic data with columns: Et..., Protocol, Src., Dst., Tx Rate, Rx Rate, Tx Pack..., and Rx Pack... The table shows multiple entries for UDP traffic from various source IP addresses to the destination 192.168.1.1:53. The bottom status bar shows '6200 items', 'Total Tx: 0 bps', 'Total Rx: 9.1 Mbps', 'Total Tx Packet: 0', and 'Total Rx Packet: 19 119'.

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (p)	17 (udp)	64.247.124.230:16074	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	74.246.215.130:16101	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	66.6.136.152:16125	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	68.223.155.223:17278	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	72.124.173.35:17304	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	66.185.185.215:17322	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	74.187.215.252:17323	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	73.61.251.35:17333	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	65.59.239.81:17370	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	64.166.36.152:17405	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	72.129.35.53:17425	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	68.121.62.13:17437	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	64.239.142.236:17441	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	68.134.201.114:17457	192.168.1.1:53 (dns)	0 bps	480 bps	0	1
800 (p)	17 (udp)	68.94.142.199:17517	192.168.1.1:53 (dns)	0 bps	480 bps	0	1

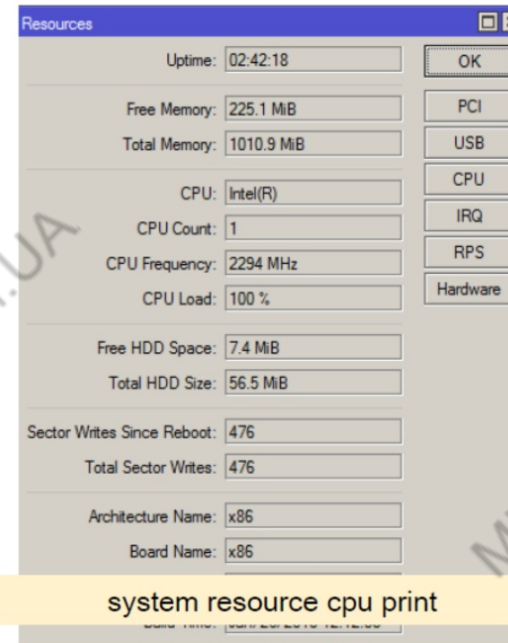
6200 items Total Tx: 0 bps Total Rx: 9.1 Mbps Total Tx Packet: 0 Total Rx Packet: 19 119

UDP flood attack

The attack is exhausting the resources of the router and impacting the performance



tool profile freeze-frame-interval=1



system resource cpu print

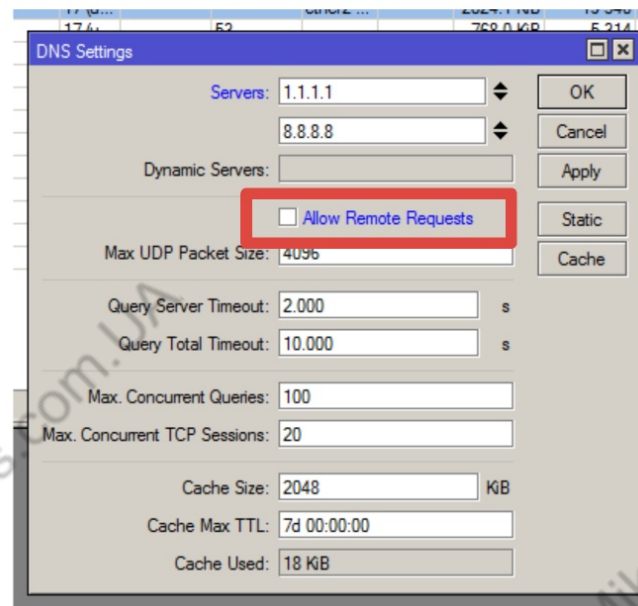
Preventing UDP flood Attack

- Disable DNS forwarder on MikroTik if not required.
- If "IP -> DNS" – Allow remote request is enabled, make sure appropriate filter rule is set to prevent incoming DNS attacks.
- Rate-limiting for each new udp connection

Preventing UDP flood Attack

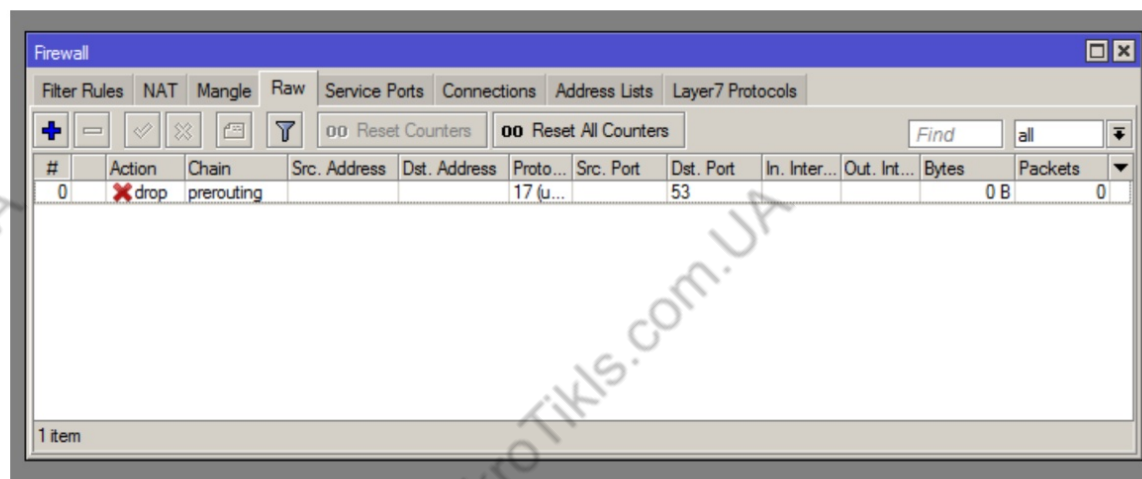
Отключите Allow Remote Requests
если вам не нужно использовать MikroTik в
качестве кэширующего DNS cacher

Если нужно использовать MikroTik как DNS
cacher - то в firewall ограничьте запросы с
нужного интерфейса*



Preventing UDP flood Attack

Блокируйте DNS запросы “udp/53” с
публичных(недоверительных) интерфейсов



```
/ip firewall raw add action=drop chain=prerouting dst-port=53 in-interface-list=OUTSIDE protocol=udp
```

Preventing UDP flood Attack

Rate-limiting every udp/53 packet requests

#	Action	Chain	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Interface List	Bytes	Packets
0	✗ drop	prerouting		17 (udp)		53			OUTSIDE	0 B	0
1	✓ acc...	prerouting		17 (udp)		53			!OUTSIDE	0 B	0
2	✗ drop	prerouting		17 (udp)		53			!OUTSIDE	0 B	0

3 items (2 selected)

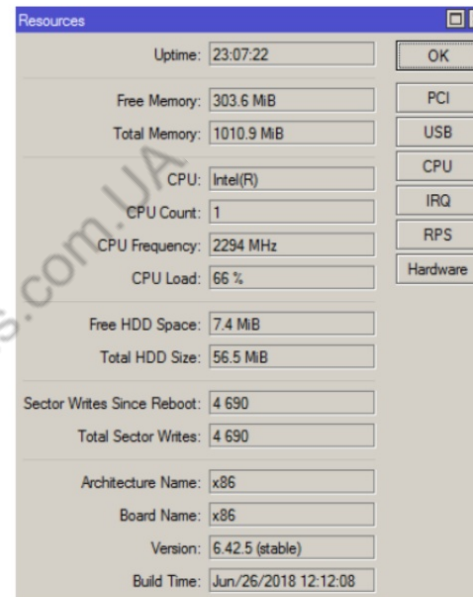
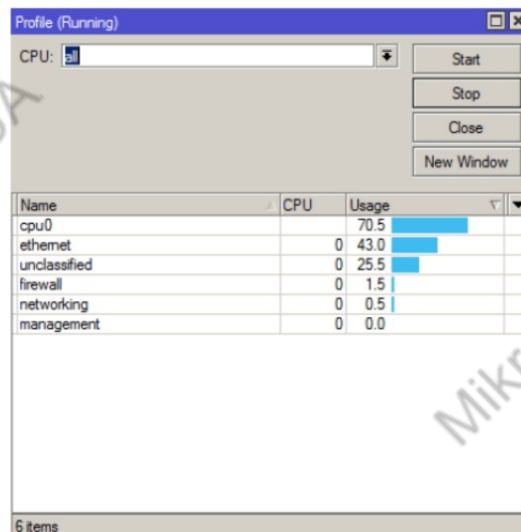
/ip firewall raw

add action=accept chain=prerouting dst-port=53 in-interface-list=!OUTSIDE limit=100.5/packet
protocol=udp

add action=drop chain=prerouting dst-port=53 in-interface-list=!OUTSIDE protocol=udp

Preventing TCP SYN Attack

- These rules are stopping the tcp SYN attack, but still affecting the CPU resources. (*need more powerful router for preventing*)



MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



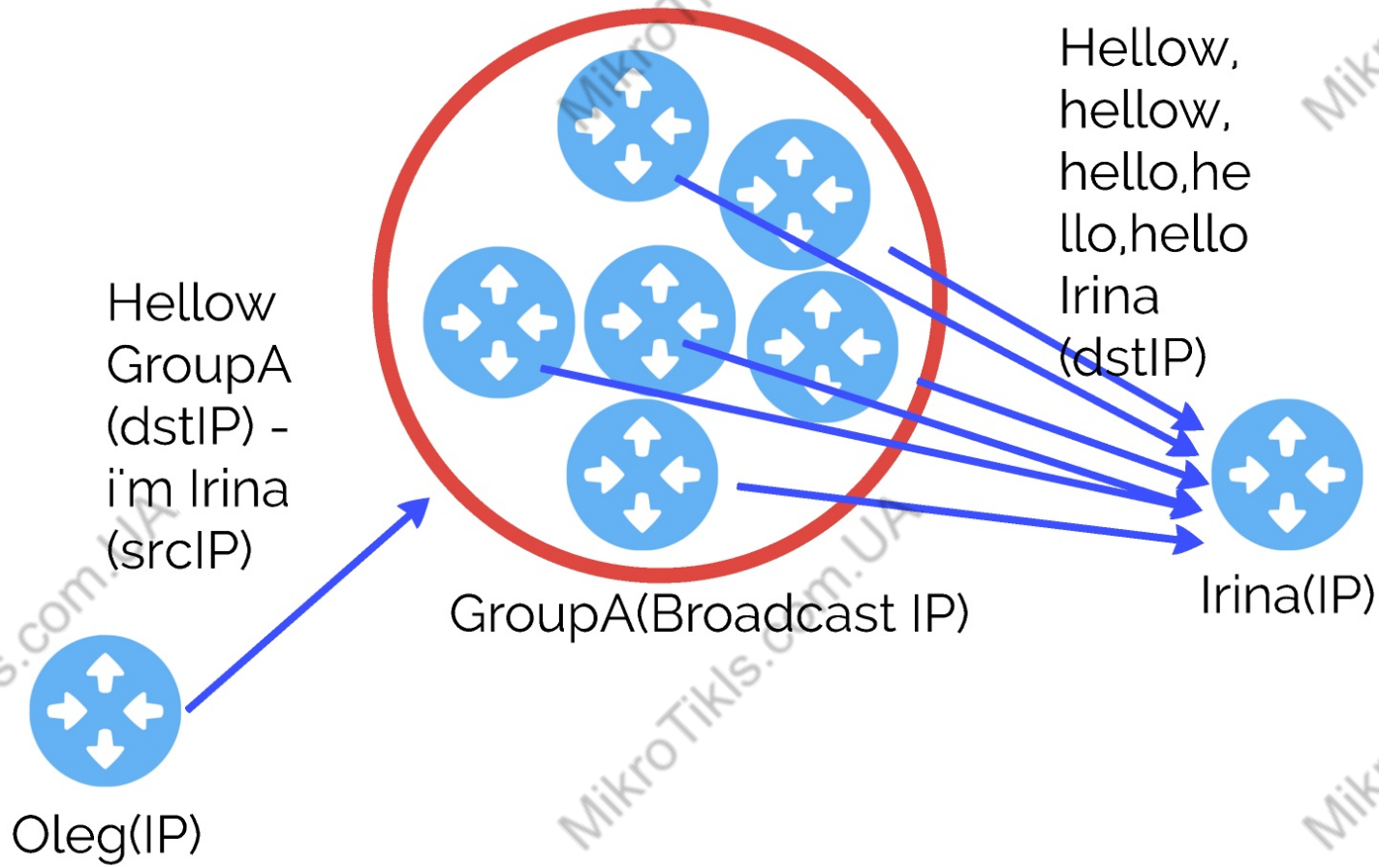
qualitytraining
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

Ping(ICMP) flood and ICMP SMURF attack

- Ping flood -тип атаки на сетевое оборудование, ставящий своей целью отказ в обслуживании. Ключевой особенностью (по сравнению с остальными видами флуд-атак) является возможность осуществления атаки «бытовыми средствами» (программами и утилитами, входящими в состав домашних/офисных версий операционных систем).
- Атака SMURF относится экспертами к наиболее опасной разновидности атаки DDoS, поскольку имеет эффект усиления, являющийся результатом отправки прямых широковещательных запросов ping к системам, которые обязаны послать ответ.
- Атака smurf пользуется особенностями прямой широковещательной рассылки и требует как минимум трех участников: атакующий, усиливающая сеть и жертва.
- Атакующий посылает мистифицированный пакет ICMP ECHO по адресу широковещательной рассылки усиливающей сети. Адрес источника этого пакета заменяется адресом жертвы, чтобы представить дело так, будто именно целевая система инициировала запрос. Поскольку пакет ECHO послан по широковещательному адресу, все системы усиливающей сети возвращают жертве свои ответы.
- Послав один пакет ICMP в сеть из 100 систем, атакующий инициирует усиление атаки DDoS в сто раз! Коэффициент усиления зависит от размера сети, поэтому атакующий ищет большую сеть, способную полностью подавить работу системы-жертвы



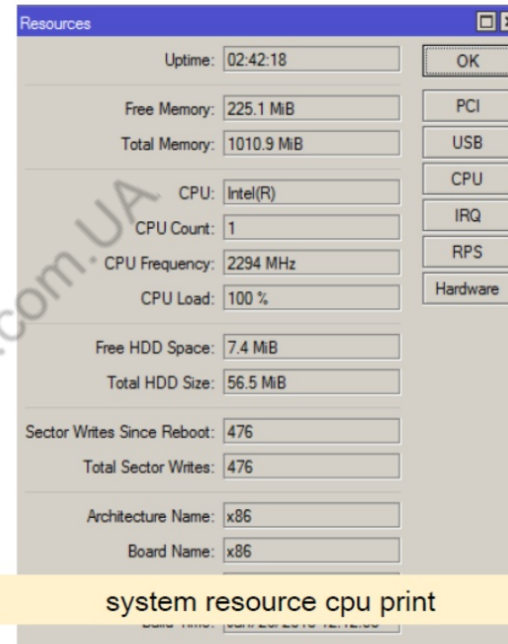
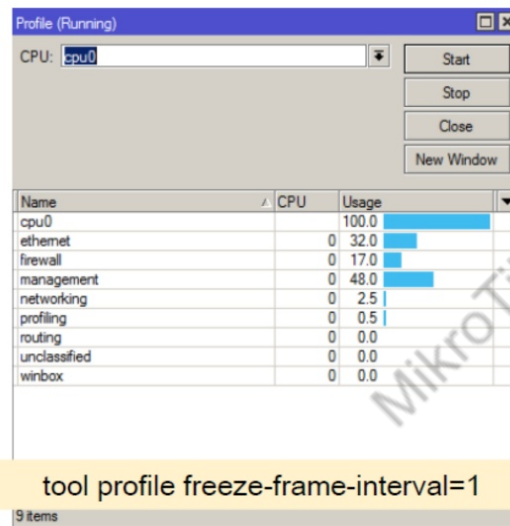
ICMP smurf attack

Start attacking ICMP smurf with random source

```
root@kali:~# hping3 --icmp --flood --rand-source -c 20000 --spoof 192.168.1.1 192.168.1.255  
HPING 192.168.1.255 (eth0 192.168.1.255): icmp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown
```

ICMP smurf attack

аналогичная наблюдаемая картина в ip firewall connection и torch
так же ресурсы и каналы будут загружены



Prevent ICMP smurf attack

- Configure routers not to forward or accept packets directed to broadcast addresses.
- Configure individual hosts or routers to not respond to ping requests from outside

```
/ip firewall filter  
add action=drop chain=input dst-address-type=broadcast  
icmp-options=0:0-255 protocol=icmp  
add action=drop chain=input in-interface-list=OUTSIDE  
protocol=icmp
```

Rate Limit and ICMP flood prevention

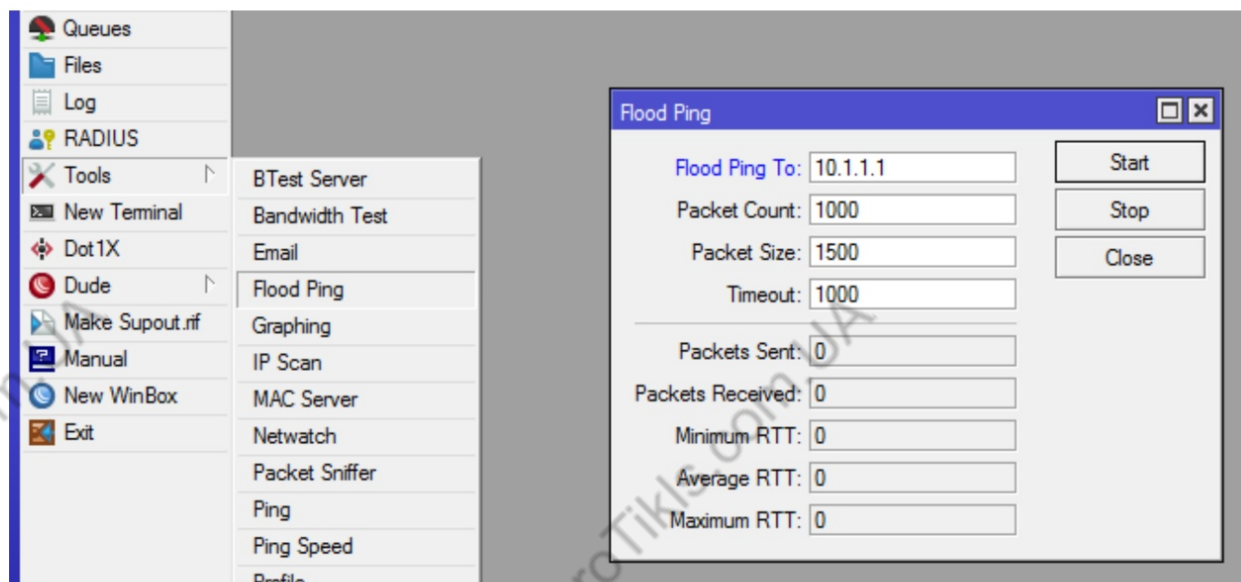
- Открывайте только нужные типы и коды ICMP, остальные блокируйте.
- Открывайте только нужное кол-во за период времени используйте параметр Rate-limit
- Не принимайте ICMP 0 на broadcast
- Используйте встроенную утилиту Ping Flood для тестирования (только для тестирования)

The screenshot displays the Mikrotik WinBox Firewall configuration interface. The main window shows a list of firewall rules with the following data:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✓ acc...	input			1 (icmp)					22.0 KB	15
1	✗ drop	input			1 (icmp)					10.3 KB	7

The right-hand pane shows the 'Firewall Rule' configuration for rule 0, with the 'Limit' tab selected. The 'Limit' section is expanded, showing the following settings:

- Connection Limit: (collapsed)
- Limit: (expanded)
 - Rate: 1 / sec
 - Burst: 5
- Dst. Limit: (collapsed)
- Nth: (collapsed)



MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



qualitytraining
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

Password Brute Force Attack

- Брутфорсом называется метод взлома различных учетных записей*, путем подбора логина и пароля*.
- Термин образован от сочетания английских слов brute force, означающих в переводе "грубой силы"
- Его суть заключается в автоматизированном переборе всех допустимых комбинаций пароля к учетной записи с целью выявления правильного.
- Решение задачи находится при переборе большого количества символов, чисел, их комбинаций. Каждый вариант проверяется на верность.
- С точки зрения математики решить задачу таким способом можно всегда, но временные затраты на поиски не во всех случаях оправдывают цель, так как поле поиска решений огромно.

Password Brute Force Attack

наблюдаемая ситуация...

Torch (Running)

Interface: ether2-LAN

Entry Timeout: 00:00:03

Collect:

- ☒ Src. Address
- ☒ Dst. Address
- ☐ MAC Protocol
- ☒ Protocol
- ☐ DSCP
- ☒ Src. Address6
- ☒ Dst. Address6
- ☒ Port
- ☐ VLAN Id

Filters:

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (p)	6 (tcp)	192.168.1.254:39202	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:45605	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:38707	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:40363	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:57012	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:51584	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:40917	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:59630	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:42983	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:56839	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:42752	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:58035	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:34975	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:52383	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:57142	192.168.1.1:22 (ssh)	0 bps	0 bps	0	0

70 items | Total Tx: 0 bps | Total Rx: 0 bps | Total Tx Packet: 0 | Total Rx Packet: 0

варианты защиты?

Torch (Running)

Interface: ether2-LAN

Entry Timeout: 00:00:03

Collect:

- ☒ Src. Address
- ☒ Dst. Address
- ☐ MAC Protocol
- ☒ Protocol
- ☐ DSCP
- ☒ Src. Address6
- ☒ Dst. Address6
- ☒ Port
- ☐ VLAN Id

Filters:

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

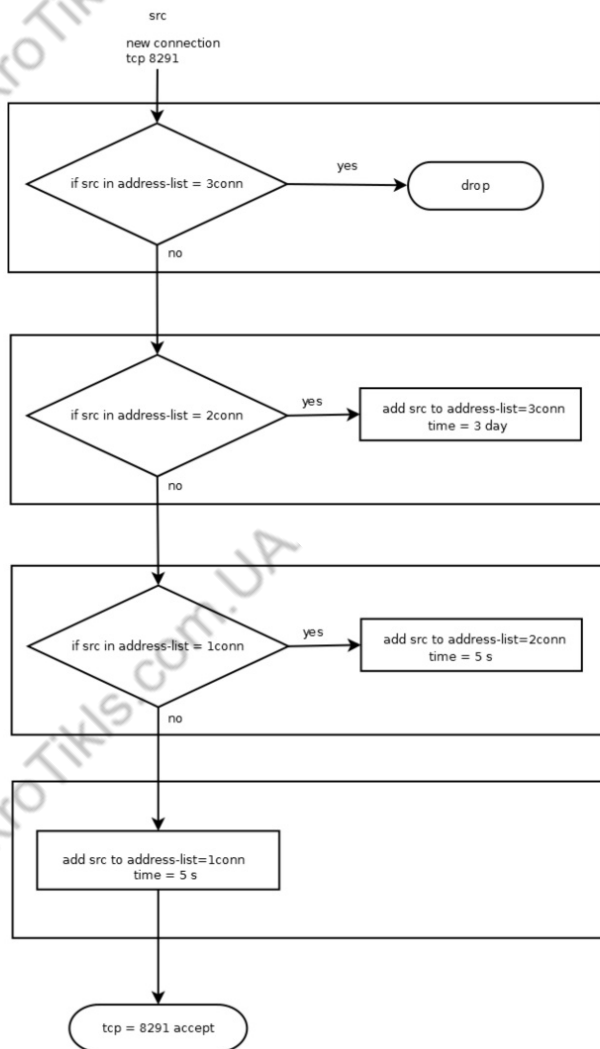
Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (p)	6 (tcp)	192.168.1.254:40876	192.168.1.1:23 (telnet)	592 bps	1120 bps	1	2
800 (p)	6 (tcp)	192.168.1.254:57657	192.168.1.1:23 (telnet)	968 bps	1056 bps	1	2
800 (p)	6 (tcp)	192.168.1.254:44580	192.168.1.1:23 (telnet)	2.2 kbps	528 bps	1	1
800 (p)	6 (tcp)	192.168.1.254:53595	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:45764	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0
800 (p)	6 (tcp)	192.168.1.254:51001	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0

6 items | Total Tx: 3.8 kbps | Total Rx: 2.7 kbps | Total Tx Packet: 3 | Total Rx Packet: 5

8.1.1.23 | 6 (tcp) | 23:59:40 established | 0 bps/0 bps | 683 B/765 B

Prevention Password Brute Force Attack

- Ограничение количества попыток доступных пользователям для безуспешно входа
- Временная блокировка пользователей, которые превышают указанный лимит неудачных попыток входа
- Требование к пользователям создавать сложные пароли
- Периодическая смена пароля



Prevention Password Brute Force Attack

ip firewall filter
action=add-src-to-address-list
time=

LAB

настройте защиту от BruteForce в отдельной цепочке
для портов 8291,22 (или других, если вы изменили порты)

MikroTikls.com

MikroTikls.com

MikroTikls.com

MikroTikls.com.UA

MikroTikls.com.UA

MikroTikls.com.UA

Tikls.com.UA

Tikls.com.UA

Tikls.com.UA

MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



qualitytraining
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

Port Scan Detection

- A port scan is a method for determining which ports on a network are open or available.
- Running a port scan on a network or server reveals which ports are open and listening (receiving information)
- Port Scan tools (like NMAP) can detect what version of an application is running on a port
- Port scanning is the “gate” for starting an attack or penetration to your networks

Port Scan Detection

- Scanning available ports on the target

```
root@kali:~# nmap 192.168.1.1

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-09-26 04:33 WIB
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
179/tcp   open  bgp
443/tcp   open  https
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: 00:50:56:3B:5B:C6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```


Preventing Port Scanner

ip firewall filter - extra

Port Scan Detect(PSD). Опция, позволяющая настроить определенные события сканирования портов.

Поля:

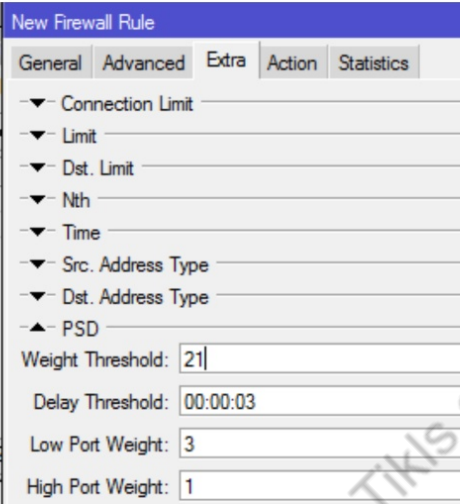
Weight Threshold = При каком значении сработает.

Delay Threshold = Максимальная задержка между пакетами с разными портами назначения, пришедшими с одного адреса.

Low Port Weight = сколько при подсчете стоит каждый порт в диапазоне 0-1023.

High Port Weight = сколько при подсчете стоит каждый порт в диапазоне 1024-65535.

Например, на скриншоте правило сработает, если будет просканировано 7 и более портов в привилегированном диапазоне; Или 21 и более портов в непривилегированном диапазоне. При этом пауза между поступающими пакетами с одного источника, направленного на разные порты будет не более 3 секунд.



New Firewall Rule				
General	Advanced	Extra	Action	Statistics
▼ Connection Limit				
▼ Limit				
▼ Dst. Limit				
▼ Nth				
▼ Time				
▼ Src. Address Type				
▼ Dst. Address Type				
▲ PSD				
Weight Threshold:		21		
Delay Threshold:		00:00:03		
Low Port Weight:		3		
High Port Weight:		1		

action=add-src-to-address-list
address-list="port scanners"

Preventing Port Scanner

```
/ip firewall filter
add action=drop chain=input src-address-list="port scanners"
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=input
comment="Port scanners to list " protocol=tcp psd=21,3s,3,1
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=input
comment="NMAP FIN Stealth scan" protocol=tcp tcp-flags=\
fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=input
comment="SYN/FIN scan" protocol=tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=input
comment="SYN/RST scan" protocol=tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=input
comment="FIN/PSH/URG scan" protocol=tcp tcp-flags=\
fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=input
comment="ALL/ALL scan" protocol=tcp tcp-flags=\
fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w
chain=input
comment="NMAP NULL scan" protocol=tcp tcp-flags=\
!fin,!syn,!rst,!psh,!ack,!urg
```

Preventing Port Scanner

LAB

Добавьте защиту к вашему Firewall от сканирования портов

MikroTik Certified Security Engineer

MTCSE

Chapter 3: OSI Layer Attacks

MNDP
(CDP) Attack

DHCP
Starvation /
Rogue
Attack

TCP SYN
Attack

UDP flood
Attack

Port Scan
Detection

Password Brute
Force Attack

Ping flood and
SMURF Attack



qualitytraining
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01