



Seguridad Informática hacia equipos RouterOS

- *«El único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces, yo no apostaría mi vida por ello».*
- Gene Spafford, experto en seguridad informática.



Presentación Personal Personal



Andrés Ocampo Dávila

- Supervisor General de Telecomunicaciones, iPlanet
- MSC en Administración de TI e ING en Electrónica y Telecomunicaciones
- Consultor Certificado Mikrotik
- Certificaciones Mikrotik
 - MTCTCE; MTCNA
- Certificaciones Cisco
 - CCNA Routing and Switching; CCNA Security; CCNP Routing and Switching
- Experiencia en Mikrotik desde 2013

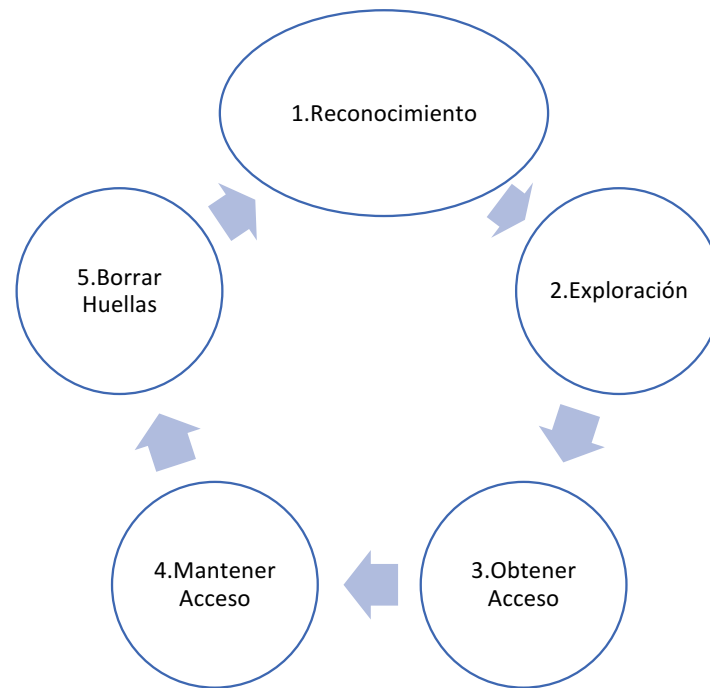
Vulnerabilidad

- De acuerdo con la Real Academia de la Lengua:
 - Vulnerabilidad:
Que puede ser herido o recibir lesión, física o moralmente
- En seguridad informática
 - Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar daño u obtener información importante. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- En equipos de red
 - Vulnerabilidad es una falencia en la configuración de seguridad del equipo, bugs de software o permitir el acceso por hardware el cuál permite tomar el control del equipo para realizar ataques hacia dispositivos finales

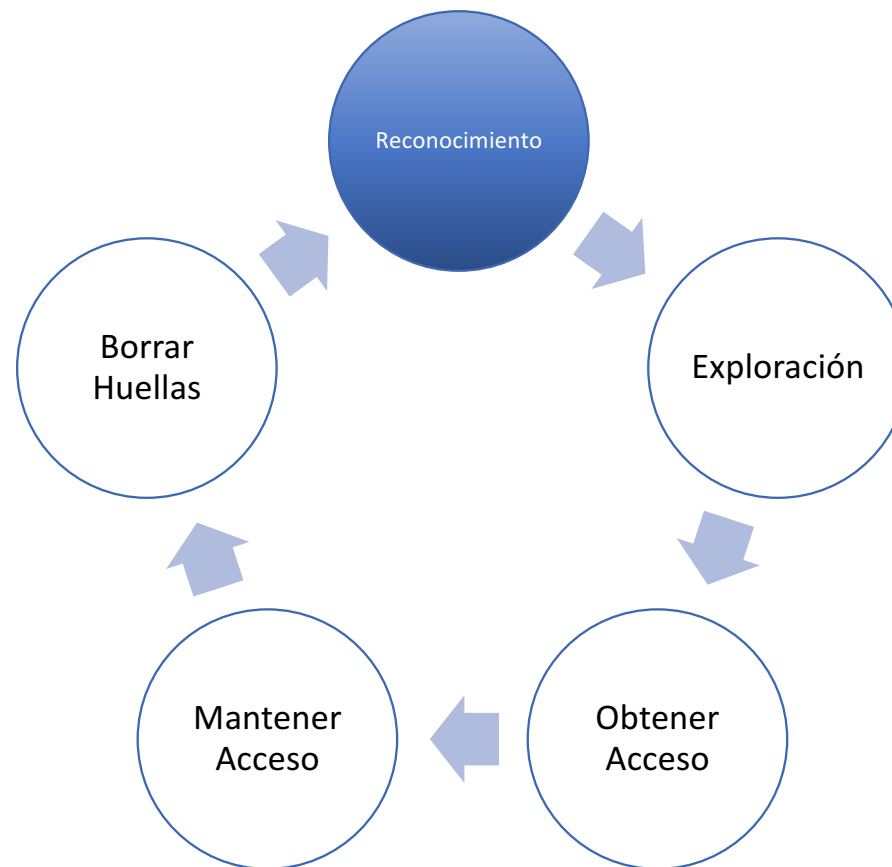


Anatomía de un ataque informático

- La idea es pensar como un atacante!
 - Aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un embate hacia los equipos de red



1. Reconocimiento



Reconocimiento

OBJETIVO:

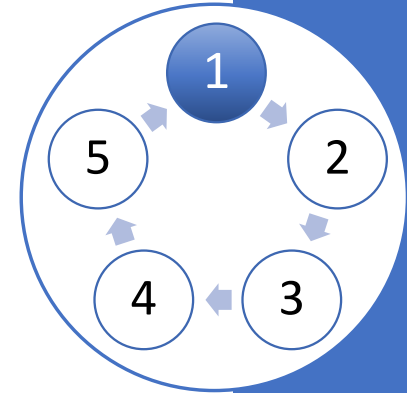
- Obtener información de la víctima

MÉTODOS:

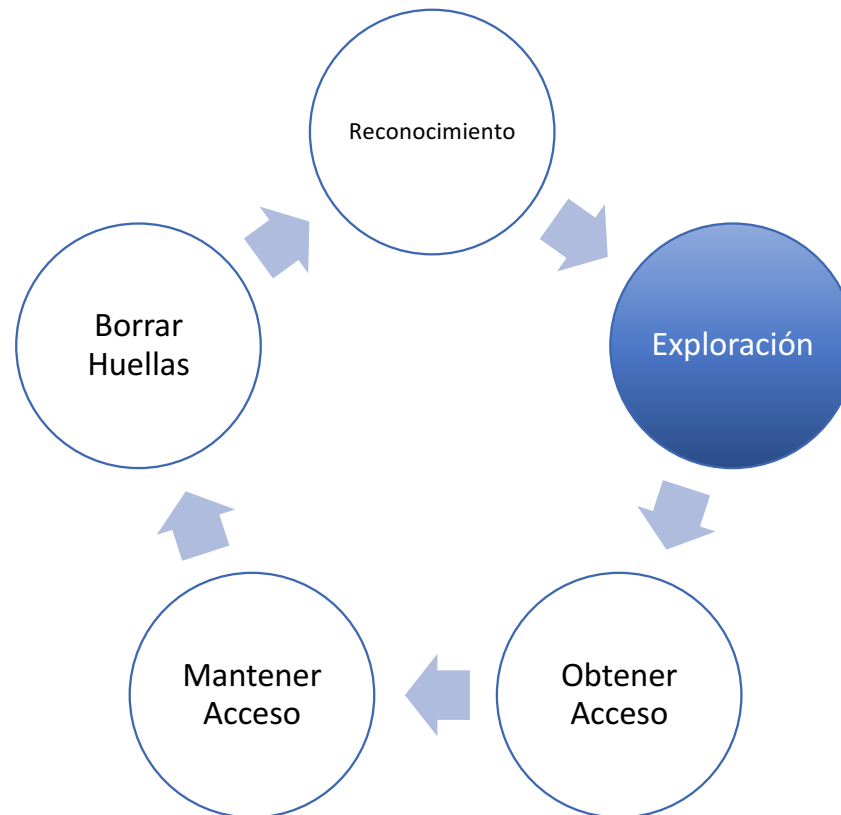
- Ingeniería Social
- Dumpster Diving
- Sistemas operativos que utiliza
- Ubicación de enrutadores / switches
- Hosts accesibles
- Consultas Whois
- (IPs,DNS, contactos,servers)

DEFENSAS:

- No revelar datos confidenciales!!!
- Ser cuidadoso en almacenar documentos importantes



2. Exploración



Exploración

OBJETIVO:

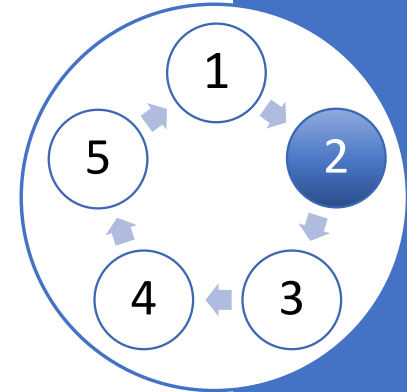
- Buscar vulnerabilidades en base a la información recolectada

MÉTODOS:

- Revisión de puertos (NMAP test)
- <https://www.shodan.io/>
- Revisión de vulnerabilidades del Sistema Operativo
- <https://www.vuldb.com/>

DEFENSAS:

- Realizar bloqueo de escaneo de puertos (RouterOS)
- Mantener actualizados los sistemas operativos.

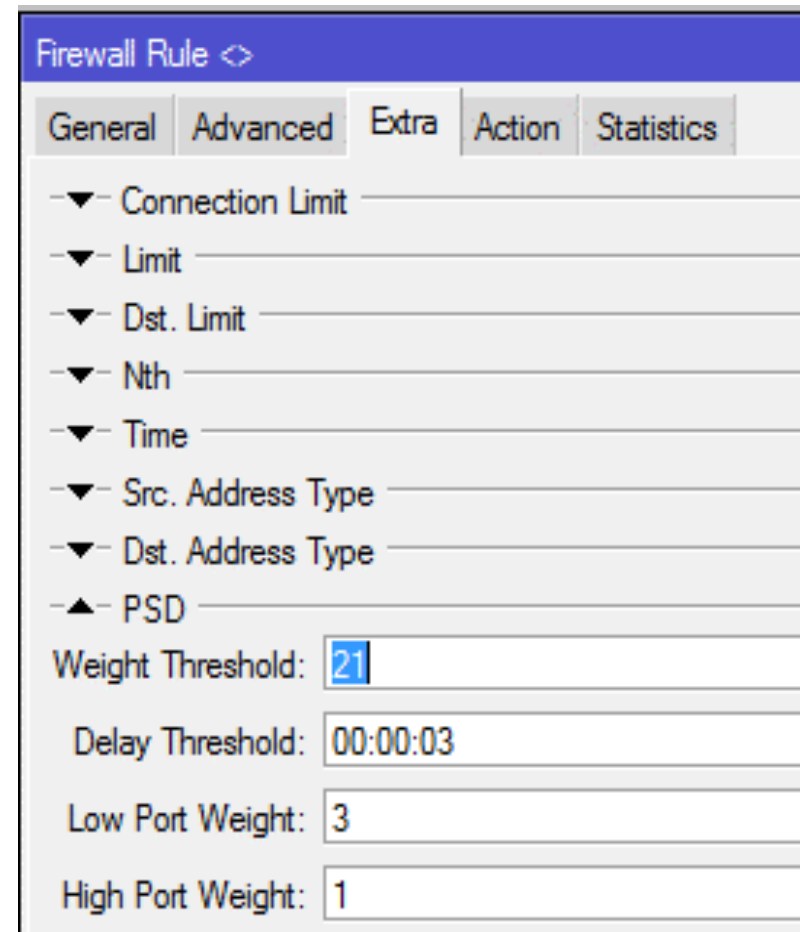


Protección para Mecanismos de Exploración

Dentro de RouterOS, se puede generar un script el cual analiza automáticamente si una IP en particular está tratando de hacer un mapeo de puertos.

Código:

```
/ip firewall filter
add chain=input protocol=tcp
psd=21,3s,3,1 action=add-src-to-
address-list address-list="port
scanners" address-list-timeout=2w
comment="Port scanners to list "
disabled=no
add chain=input src-address-
list=port-scanners action=drop
```



The screenshot shows the 'Firewall Rule' configuration window with the 'Extra' tab selected. The 'PSD' (Port Scanning Detection) section is expanded, showing the following settings:

- Weight Threshold: 21
- Delay Threshold: 00:00:03
- Low Port Weight: 3
- High Port Weight: 1

Protección para Mecanismos de Exploración

Firewall				
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols				
+ - ✓ ✕ [icon] [icon]				
Name	Address	Timeout	Creation Time	
D port scanners	5.149.250.172	10d 05:04:54	Jun/26/2017 20:34:50	
D port scanners	45.76.130.164	10d 12:12:02	Jun/27/2017 02:59:33	
D port scanners	46.17.46.239	13d 01:53:26	Jun/26/2017 19:14:25	
D port scanners	46.218.83.202	13d 00:08:06	Jun/29/2017 15:38:26	
D port scanners	51.254.201.125	11d 18:52:22	Jun/28/2017 03:13:44	
D port scanners	77.234.42.209	10d 02:45:05	Jun/26/2017 18:15:25	
D port scanners	77.234.45.48	10d 04:04:50	Jun/26/2017 19:35:10	
D port scanners	77.234.45.51	10d 15:26:22	Jun/27/2017 06:56:42	
D port scanners	104.238.189.159	10d 12:45:10	Jun/27/2017 03:05:38	
D port scanners	115.231.222.136	13d 22:51:40	Jun/30/2017 14:21:59	
D port scanners	120.132.3.151	13d 16:09:36	Jun/27/2017 10:59:03	
D port scanners	163.182.175.181	13d 12:01:14	Jun/28/2017 00:54:06	
D port scanners	165.227.158.117	12d 21:00:42	Jun/29/2017 12:30:26	
D port scanners	178.238.234.2	13d 01:09:13	Jun/29/2017 16:38:48	
D port scanners	185.73.220.11	10d 17:03:41	Jun/27/2017 08:34:01	
D port scanners	195.154.200.88	13d 08:53:12	Jun/29/2017 05:18:11	
D port scanners	204.93.154.198	10d 09:51:30	Jun/26/2017 20:41:46	
D port scanners	204.93.154.199	13d 14:06:11	Jun/26/2017 17:27:41	
D port scanners	204.93.154.203	13d 03:37:59	Jun/29/2017 16:03:20	
D port scanners	204.93.154.210	12d 22:51:38	Jun/29/2017 13:19:12	
D port scanners	204.93.154.211	10d 18:07:32	Jun/27/2017 07:40:14	
D port scanners	204.93.154.212	13d 23:54:45	Jun/27/2017 22:08:03	
D port scanners	204.93.154.215	13d 15:47:19	Jun/26/2017 18:39:05	
D port scanners	204.93.154.216	13d 07:45:07	Jun/29/2017 15:40:19	
D port scanners	204.93.154.220	13d 23:28:03	Jun/26/2017 19:50:07	
D port scanners	204.93.180.2	13d 21:49:39	Jun/26/2017 17:20:32	
D port scanners	204.93.180.6	13d 08:43:54	Jun/26/2017 22:44:31	
D port scanners	204.93.180.13	13d 07:52:31	Jun/26/2017 23:25:20	
D port scanners	213.202.242.55	11d 22:40:12	Jun/28/2017 14:10:32	

Raw output

Save as pdf

```
Starting Nmap ( http://nmap.org ) at 2017-06-30 23:40 EEST
NSE: Loaded 29 scripts for scanning.
Initiating Ping Scan at 23:40
Scanning 204.93.154.212 [4 ports]
Completed Ping Scan at 23:40, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 23:40
Scanning host9.204.93.154.212 ec (204.93.154.212) [100 ports]
Completed SYN Stealth Scan at 23:40, 9.05s elapsed (100 total ports)
Initiating Service scan at 23:40
Initiating OS detection (try #1) against host9.204.93.154.212 ec (204.93.154.212)
Retrying OS detection (try #2) against host9.204.93.154.212 ec (204.93.154.212)
NSE: Script scanning 204.93.154.212.

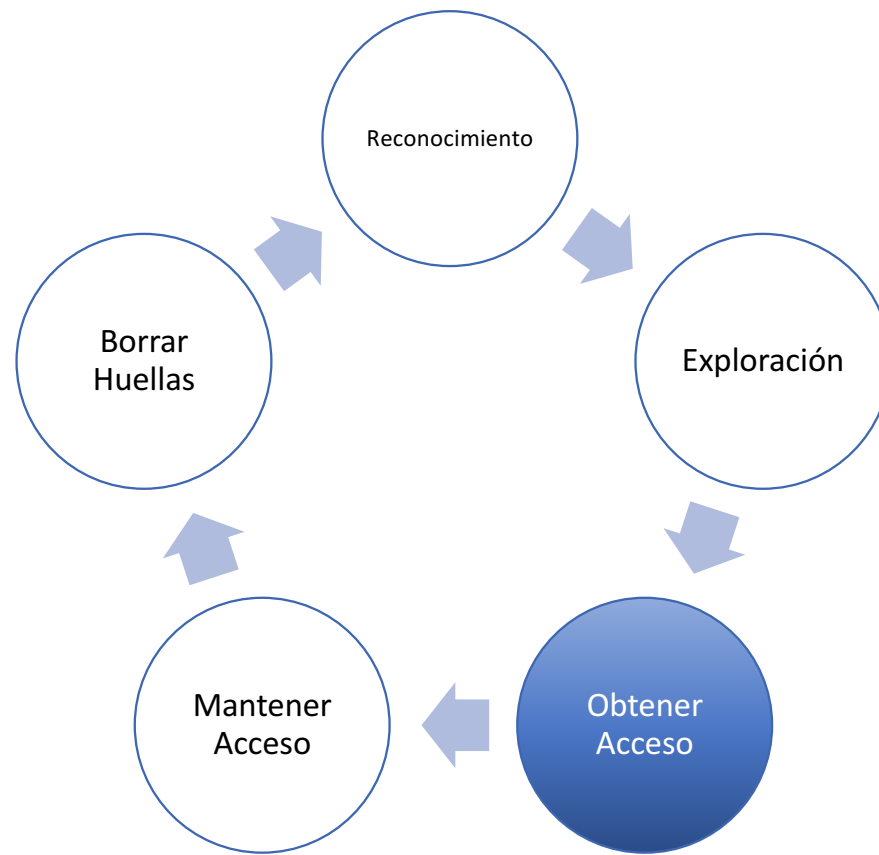
[*] Nmap scan report for host9.204.93.154.212 ec (204.93.154.212)
Host is up (0.18s latency).
All 100 scanned ports on host9.204.93.154.212 ec (204.93.154.212) are filtered

Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 15.37 seconds
Raw packets sent: 252 (15.624KB) | Rcvd: 2 (68B)
```

3. Obtener Acceso



Obtener Acceso

OBJETIVO:

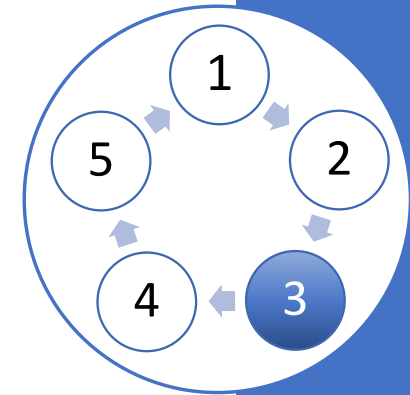
- Explotar las vulnerabilidades encontradas
- <https://www.exploit-db.com/>

MÉTODOS (Kali Linux)

- Buffer Overflows
- <https://forum.mikrotik.com/viewtopic.php?t=119255>
- Denial of Service & Distributed DoS
- Session Hijacking
- Password Cracking (Brute Force Attacks)

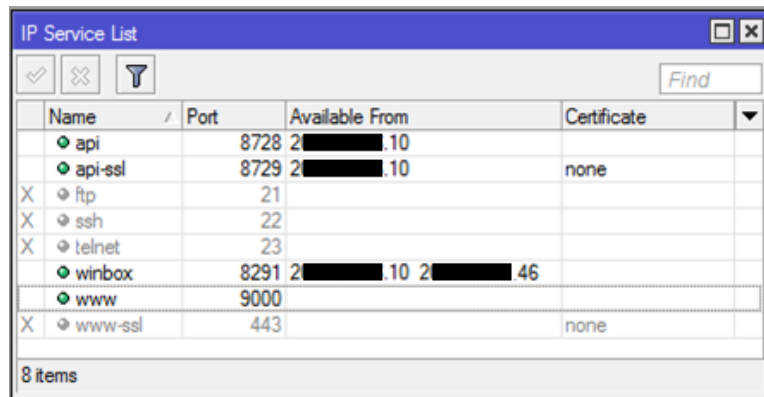
DEFENSAS:

- Establecer políticas de control y filtrado (RouterOS)



Protección para Mecanismos de Exploits

Restringir al máximo el acceso al equipo:



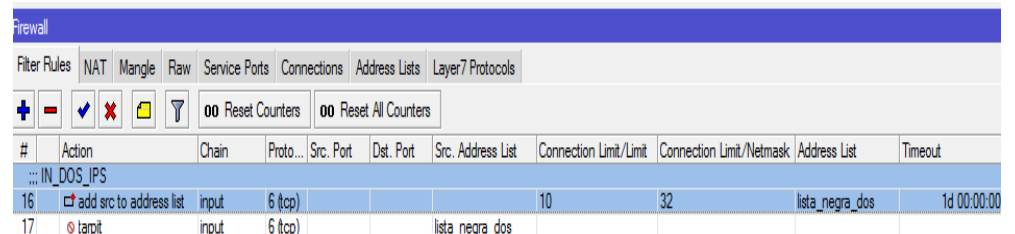
	Name	Port	Available From	Certificate
	api	8728	2[REDACTED].10	
	api-ssl	8729	2[REDACTED].10	none
X	ftp	21		
X	ssh	22		
X	telnet	23		
	winbox	8291	2[REDACTED].10 2[REDACTED].46	
	www	9000		
X	www-ssl	443		none

8 items

Utilizar para evitar ataques de DoS

```
/ip firewall filter add chain=input  
protocol=tcp connection-limit=10,32 \  
action=add-src-to-address-list address-  
list=blocked-addr address-list-timeout=1d
```

```
/ip firewall filter add chain=input  
protocol=tcp src-address-list=blocked-addr \  
connection-limit=3,32 action=tarpit
```



#	Action	Chain	Proto...	Src. Port	Dst. Port	Src. Address List	Connection Limit/Limit	Connection Limit/Netmask	Address List	Timeout
16	add src to address list	input	6 (tcp)				10	32	lista_negra_dos	1d 00:00:00
17	tarpit	input	6 (tcp)			lista_negra_dos				

Protección para Mecanismos de Exploits

- Evitar un ataque mediante SYN Flood, ocurre cuando la comunicación TCP es interrumpida, y el server se acumula de paquetes incompletos.

```
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new \ action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=no
```

```
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new \ action=accept comment="" disabled=no
```

```
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new \ action=drop comment="" disabled=no
```

Finalmente habilitar SYN Cookies

- `/ip settings set tcp-syncookies=yes` (RouterOS > V6,0)
- `/ip firewall connection tracking set tcp-syncookie=yes` (RouterOS < v6.0)

Protección para Mecanismos de Exploits

- Amplification Attacks
 - Existen ataques los cuales no solo se enfoca en degradar la calidad del servicio que provee un equipo Mikrotik, sino que también busca atacar a otros servidores.
 - Generalmente son causados por paquetes UDP (DNS, NTP, SNMP)
- Métodos de Solución
 - Permitir la comunicación en el Firewall de direcciones IPs autorizadas que puedan comunicarse en los puertos UDP/53 (DNS); UDP/123 (NTP) y UDP/161 (SNMP).



Protección para Mecanismos de Exploits

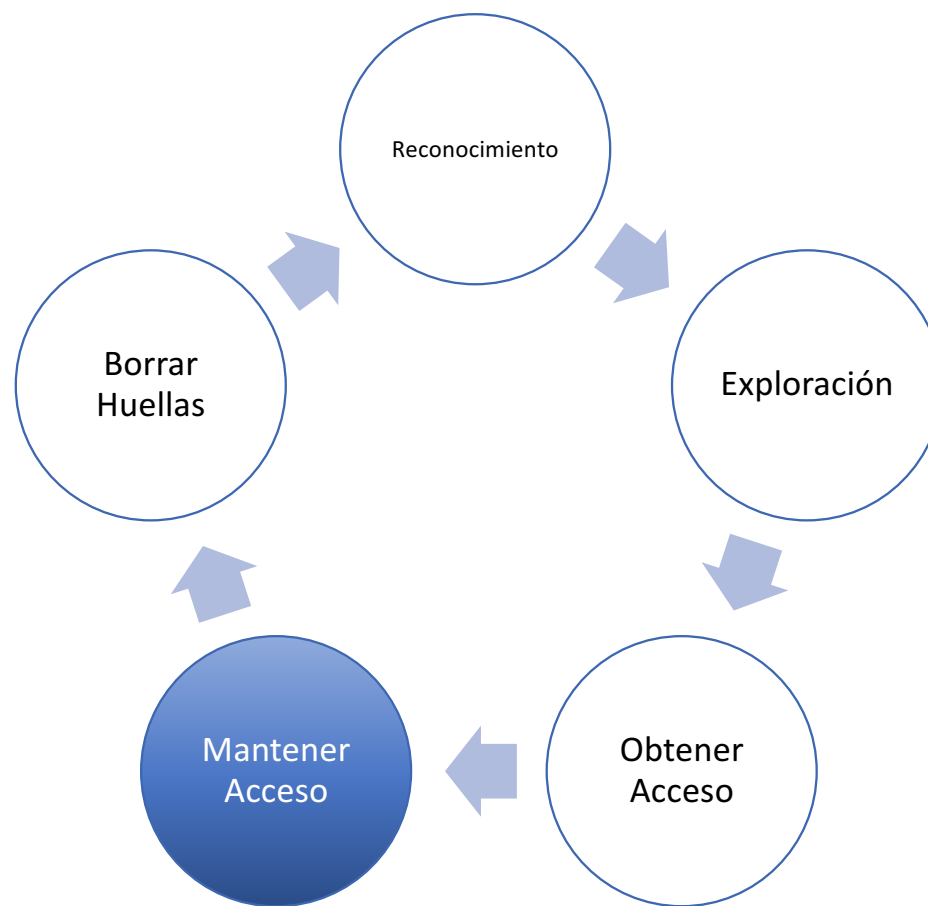
- Amplification Attacks

Firewall			
Filter Rules	NAT	Mangle	Raw
Service Ports	Connections	Address Lists	Layer7 Protocols
+	-	✓	✗
+	-	✓	✗
Name	Address	Timeout	Creation Time
ntp	0.south-america.pool....		May/12/2017 20:40:19
...	0.south-america.pool.ntp.org		
D ntp	200.89.75.198		Jun/30/2017 16:29:36
...	0.south-america.pool.ntp.org		
D ntp	201.49.148.135		Jun/30/2017 16:40:13
...	0.south-america.pool.ntp.org		
D ntp	201.217.3.85		Jun/30/2017 16:40:13
D ntp	1.south-america.pool....		May/12/2017 20:40:25
...	1.south-america.pool.ntp.org		
D ntp	190.3.107.187		Jun/30/2017 16:38:37
...	1.south-america.pool.ntp.org		
D ntp	190.15.128.196		Jun/30/2017 16:35:47
...	1.south-america.pool.ntp.org		
D ntp	200.1.19.4		Jun/30/2017 16:35:57
...	1.south-america.pool.ntp.org		
D ntp	200.160.7.193		Jun/30/2017 16:33:17
ntp	10.150.150.1		Mar/14/2017 15:04:41
ntp	2.south-america.pool....		May/12/2017 20:40:34
...	2.south-america.pool.ntp.org		
D ntp	200.189.40.8		Jun/30/2017 16:35:42
ntp	200.20.186.76		Mar/14/2017 15:04:56
ntp	3.south-america.pool....		May/12/2017 20:40:40
...	3.south-america.pool.ntp.org		
D ntp	131.0.232.2		Jun/30/2017 16:40:05
...	3.south-america.pool.ntp.org		
D ntp	200.1.19.16		Jun/30/2017 16:40:05
...	3.south-america.pool.ntp.org		
D ntp	200.89.75.197		Jun/30/2017 16:34:47
ntp	time.windows.com		May/12/2017 20:38:28
...	time.windows.com		
D ntp	52.179.17.38		Jun/25/2017 23:32:17

Firewall			
Filter Rules	NAT	Mangle	Raw
Service Ports	Connections	Address Lists	Layer7 Protocols
+	-	✓	✗
+	-	✓	✗
Name	Address	Timeout	Creation Time
snmp	1 [REDACTED] 15		May/04/2017 16:47:01
snmp	5 [REDACTED] 50		Mar/14/2017 16:20:41
snmp	2 [REDACTED] 54		May/18/2017 20:36:08
snmp	2 [REDACTED] 10		Mar/14/2017 16:20:13

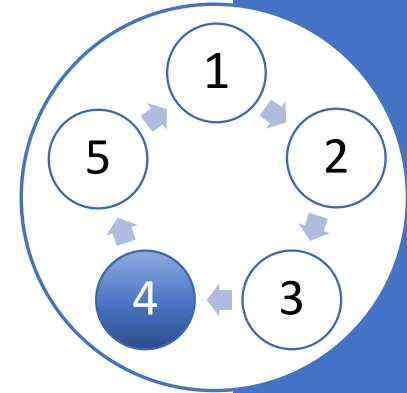
Firewall			
Filter Rules	NAT	Mangle	Raw
Service Ports	Connections	Address Lists	Layer7 Protocols
+	-	✓	✗
+	-	✓	✗
Name	Address	Timeout	Creation Time
dns	8.8.4.4		Mar/14/2017 15:04:09
dns	8.8.8.8		Mar/14/2017 15:04:06
dns	20 [REDACTED] 94		Mar/14/2017 15:03:54
dns	20 [REDACTED] 95		Mar/14/2017 15:04:00
dns	20 [REDACTED] 20		Mar/31/2017 17:20:13
dns	20 [REDACTED] 22		Mar/31/2017 17:20:02

4.Mantener Acceso

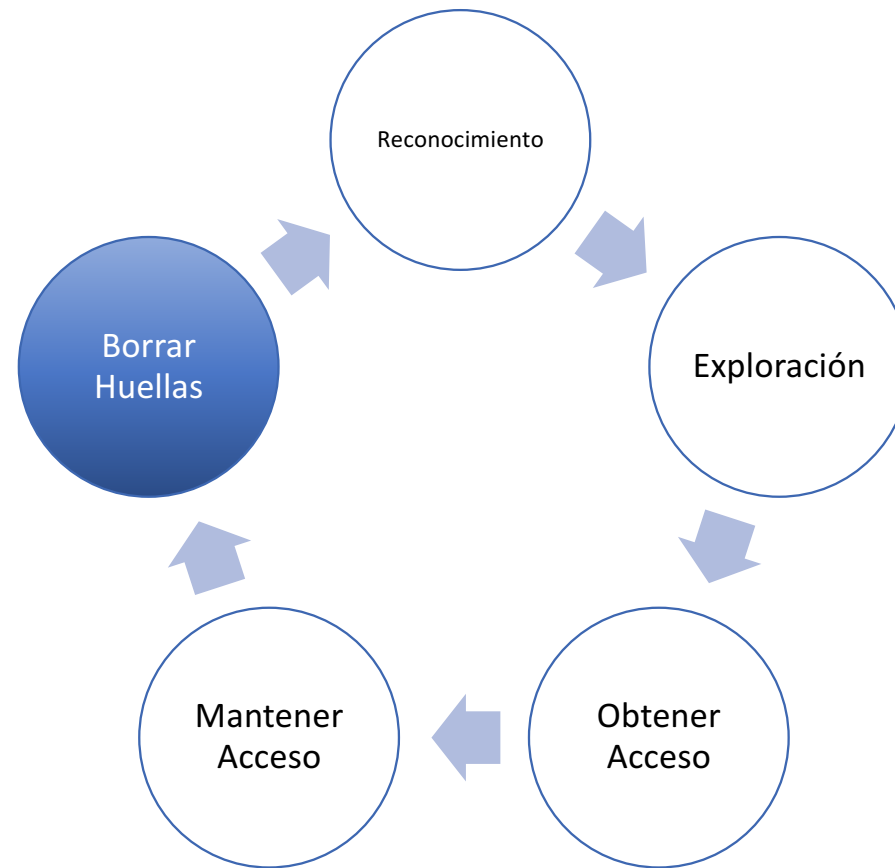


Mantener Acceso

- OBJETIVO:
 - Generar una puerta de acceso oculta
- MÉTODOS
 - Backdoors
 - Trojans
- DEFENSAS:
 - Para RouterOS hasta el momento no se han detectado backdoors o trojans que afecten o comprometan al sistema.

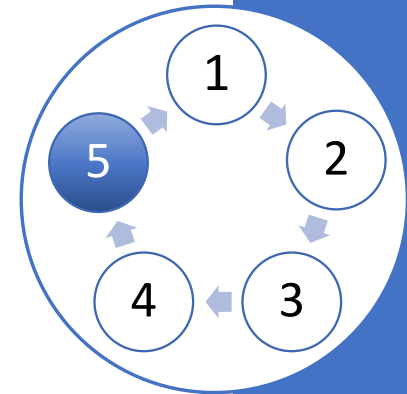


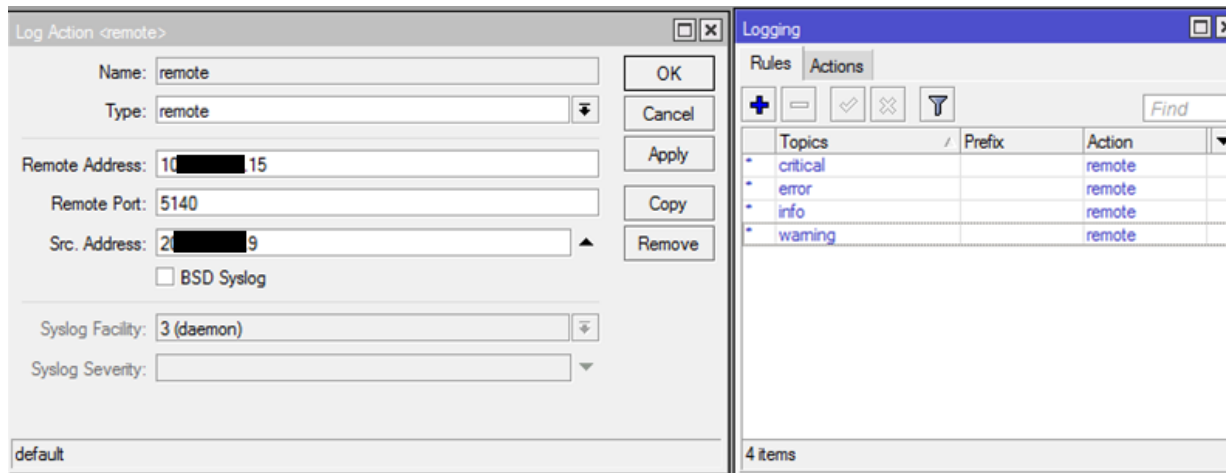
5.Borrar Huellas



Borrar Huellas

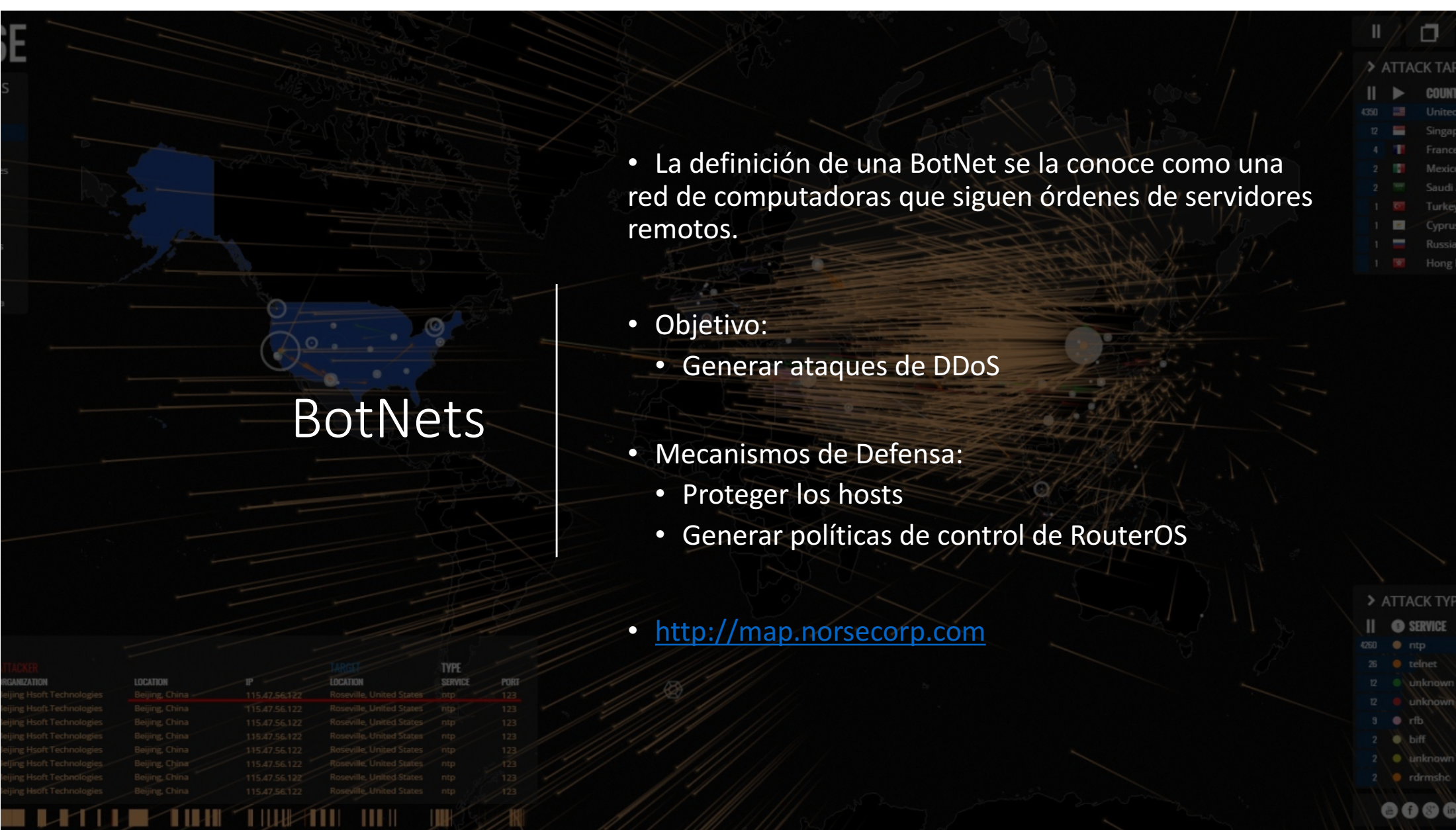
- OBJETIVO:
 - Eliminar rastros de acceso al equipo
- MÉTODOS
 - Eliminar registros de acceso (Logs)
- DEFENSAS:
 -
 - Habilitar registros de logs y procesos hacia un servidor centralizado, y proteger su acceso.





- Los archivos de LOGs, inicialmente se guardan en la memoria del equipo, por lo que un simple reinicio los borra permanentemente.
- Configurar la opción “remote” en el logging de RouterOS, apuntando hacia un servidor de Syslog externo.

Protección para guardar los LOGs



BotNets

- La definición de una BotNet se la conoce como una red de computadoras que siguen órdenes de servidores remotos.
- Objetivo:
 - Generar ataques de DDoS
- Mecanismos de Defensa:
 - Proteger los hosts
 - Generar políticas de control de RouterOS
- <http://map.norsecorp.com>

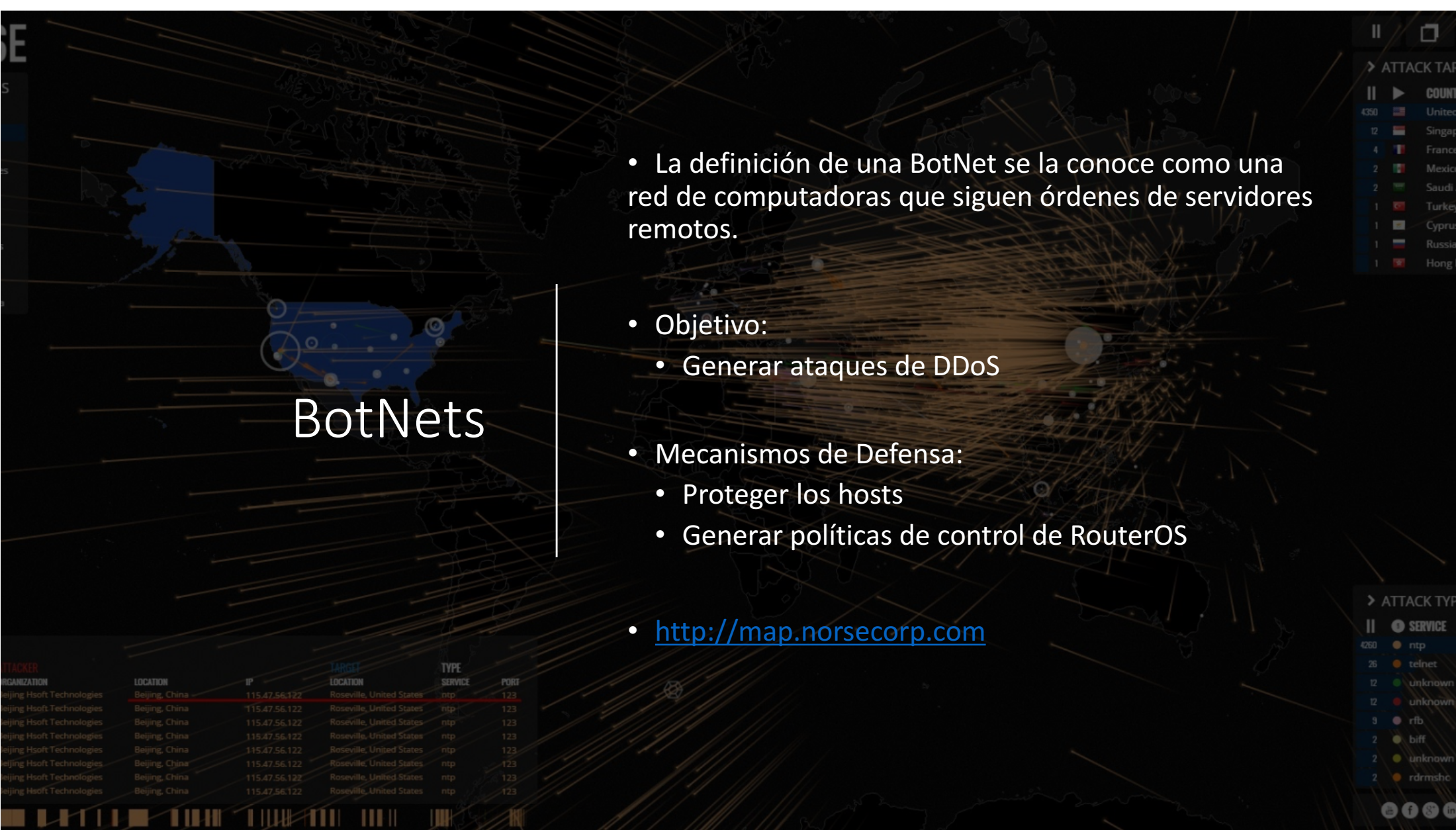
ORGANIZATION	LOCATION	IP	TARGET	TYPE	SERVICE	PORT
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123
Beijing Hssoft Technologies	Beijing, China	115.47.56.122	Roseville, United States	ntp	ntp	123

ATTACK TARGET

COUNT	COUNTRY
4350	United States
12	Singapore
4	France
2	Mexico
2	Saudi Arabia
1	Turkey
1	Cyprus
1	Russia
1	Hong Kong

ATTACK TYPE

SERVICE
ntp
telnet
unknown
unknown
rft
biff
unknown
rdmshe

- 
- # BotNets
- La definición de una BotNet se la conoce como una red de computadoras que siguen órdenes de servidores remotos.
 - Objetivo:
 - Generar ataques de DDoS
 - Mecanismos de Defensa:
 - Proteger los hosts
 - Generar políticas de control de RouterOS
 - <http://map.norsecorp.com>
- | ORGANIZATION | LOCATION | IP | TARGET | TYPE | SERVICE | PORT |
|----------------------------|----------------|---------------|--------------------------|------|---------|------|
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
| Beijing Hsoft Technologies | Beijing, China | 115.47.56.122 | Roseville, United States | ntp | 123 | |
- ATTACK TARGET
- | COUNT | COUNTRY |
|-------|---------------|
| 4350 | United States |
| 12 | Singapore |
| 4 | France |
| 2 | Mexico |
| 2 | Saudi Arabia |
| 1 | Turkey |
| 1 | Cyprus |
| 1 | Russia |
| 1 | Hong Kong |
- ATTACK TYPE
- | SERVICE |
|---------|
| ntp |
| telnet |
| unknown |
| unknown |
| rft |
| biff |
| unknown |
| rdmshe |

Protección hacia BotNets

- Protección hacia BotNets debe ser configurada en los hosts o dispositivos finales (Desktops, Laptops, Smartphones, DVRs).
- Se puede bloquear a nivel de L3 un gran porcentaje de subredes las cuales fueron listadas como fuentes de SPAM, servidores madre de Command & Control (C&C) y de Botnets conocidos a nivel mundial.
- La mejor opción siempre va a ser tener un sistema operativo actualizado en conjunto con una solución de antivirus / anti-spam / anti-phishing / anti-ransomware

