

Manobras Evasivas: Técnicas de Evasão para Varreduras com o Nmap

Rafael Ferreira
Sócio Diretor Técnico
rafael@clavis.com.br



rafael@clavis.com.br



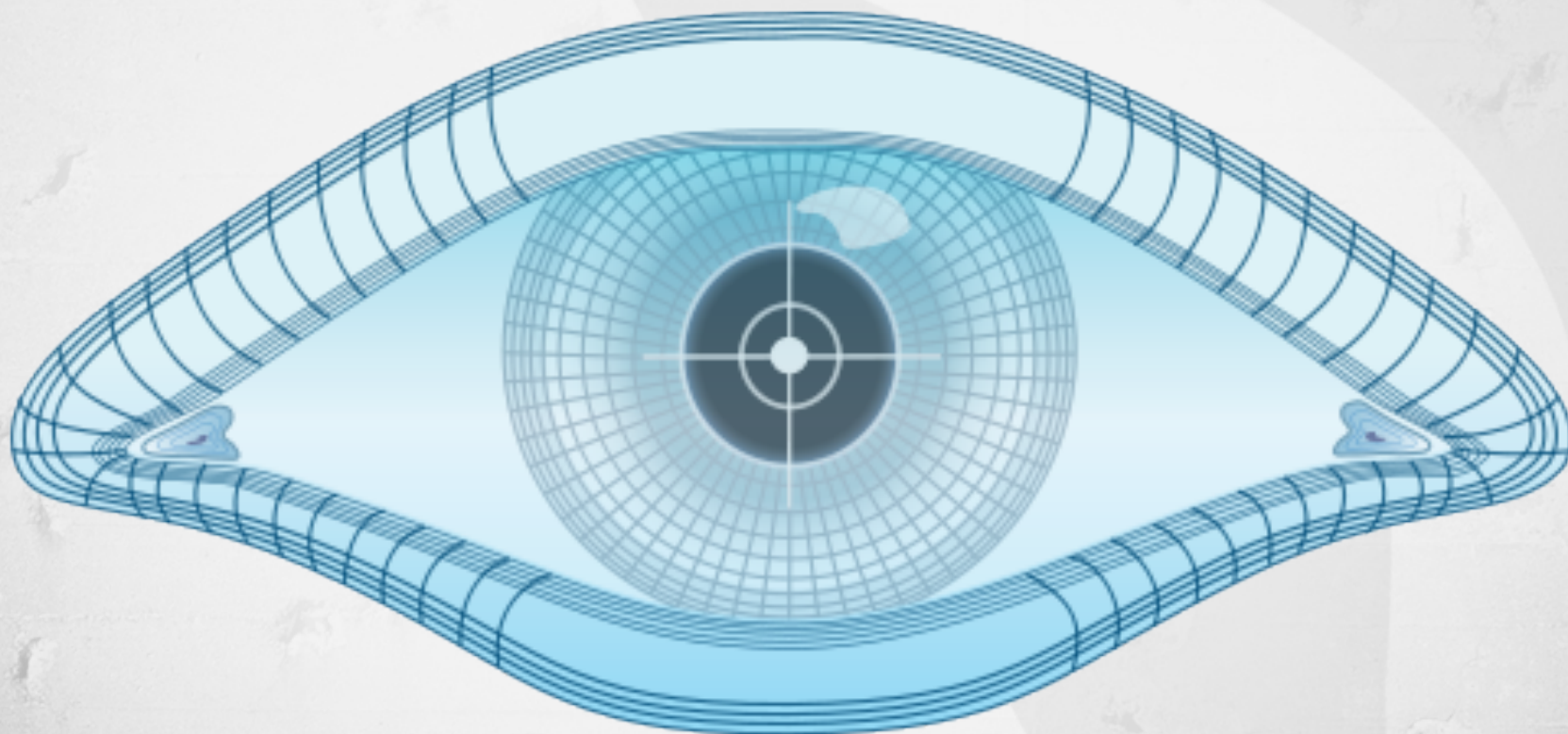
@rafaelsferreira



rafaelsoaresferreira

- Grupo Clavis
- Sócio Diretor Técnico
- Teste de invasão em redes, sistemas e aplicações

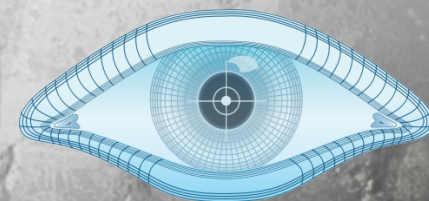
- Introdução
- Varreduras indiretas
- Contornando técnicas de detecção
- Dificultando a detecção da origem
- Conclusão

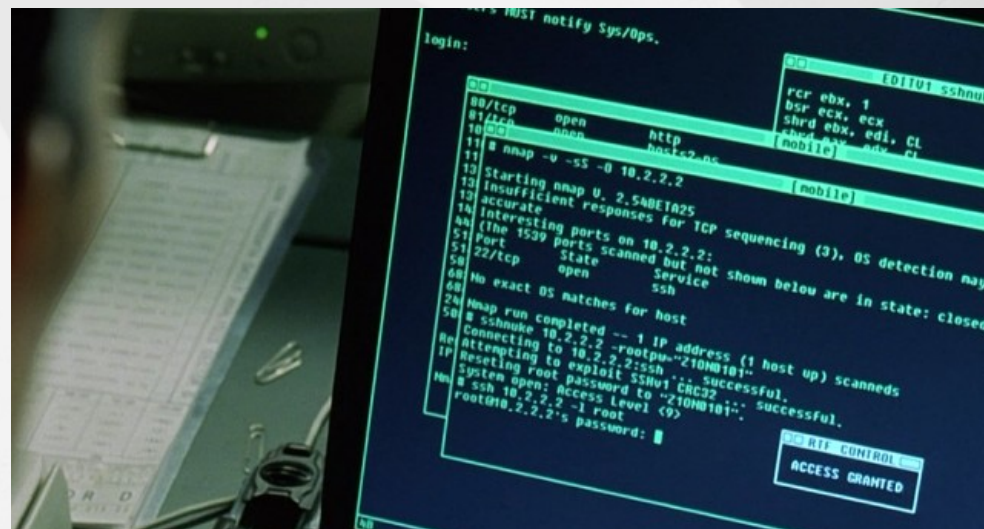


<http://nmap.org/>

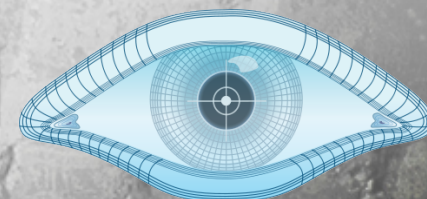
Nmap Security Scanner

- Funcionalidades principais
 - Varreduras de portas
 - Detecção de serviços, versões e SOs
 - Mapeamento e inventário de redes
 - Entre outras...
- Criado por Gordon “Fyodor” Lyon
- Ferramenta livre e código aberto
- Projeto ativo e mantido pela comunidade





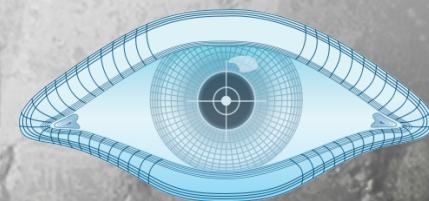
<http://nmap.org/movies/>

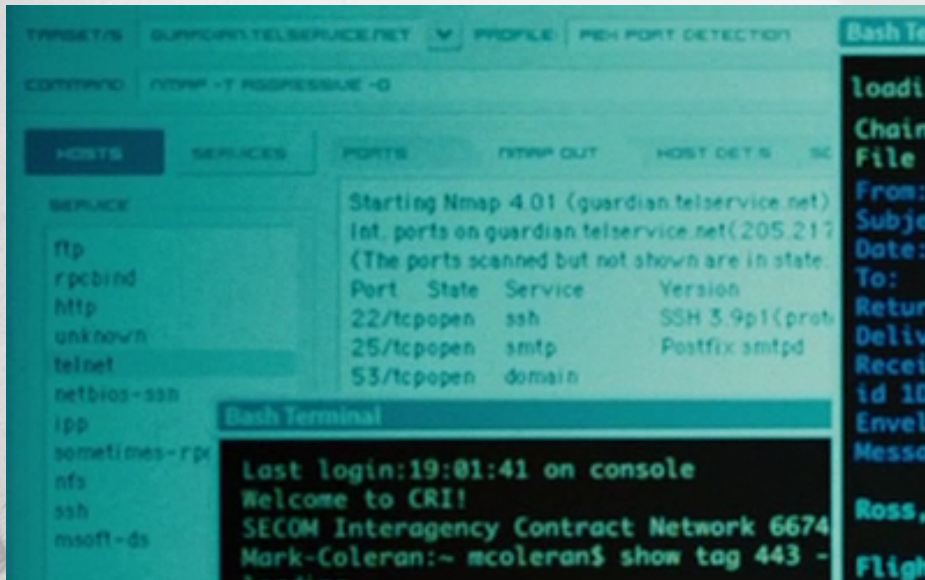




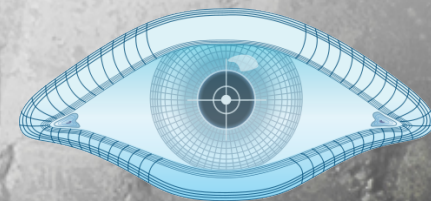
```
clan_techie@sys9:/jobs/pt/level_190_cctv_activity_monitor  
[root@mybox ~]# nmap -p 22 --open -sV 197.213.63.32/29  
Nmap scan report for alex.peachtrees.com (197.213.63.34)  
Host is up (0.014s latency).  
PORT STATE SERVICE VERSION  
22/tcp open  ssh OpenSSH 2.1.1 (protocol 1.99)  
MAC Address: 45:AE:45:6F:0A:5A (Unknown)  
  
Nmap scan report for swilley.peachtrees.com (197.213.63.35)  
Host is up (0.017s latency).  
PORT STATE SERVICE VERSION  
22/tcp open  ssh OpenSSH 5.4 (protocol 2.0)  
MAC Address: 13:A1:43:66:40:6A (Unknown)
```

<http://nmap.org/movies/>





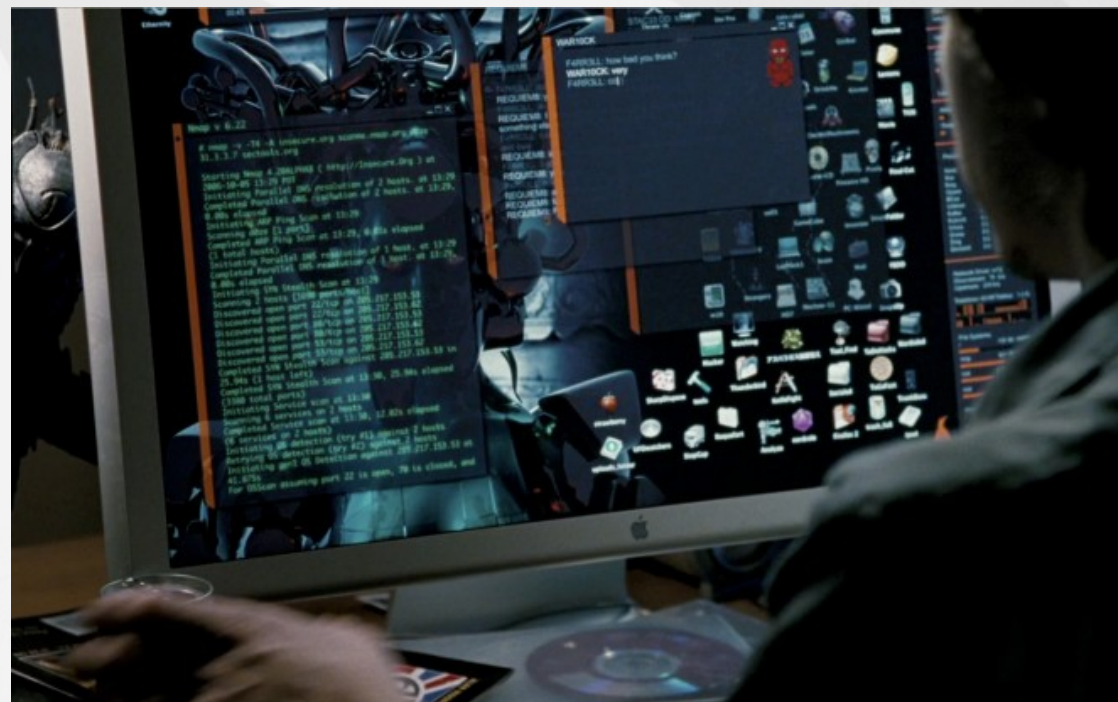
<http://nmap.org/movies/>



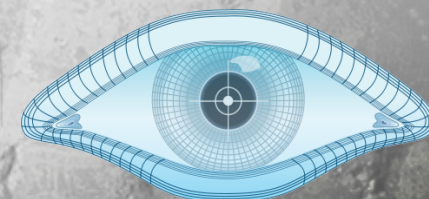
```
Nmap v 6.22

# nmap -v -T4 -A insecure.org scanme.nmap.org -oNze
31.3.3.7 sectools.org

Starting Nmap 4.20ALPHA ( http://Insecure.Org ) at
2006-10-05 13:29 PDT
Initiating Parallel DNS resolution of 2 hosts. at 13:29
Completed Parallel DNS resolution of 2 hosts. at 13:29,
0.00s elapsed
Initiating ARP Ping Scan at 13:29
Scanning dbze [1 port]
Completed ARP Ping Scan at 13:29, 0.01s elapsed
(1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:29
Completed Parallel DNS resolution of 1 host. at 13:29,
0.00s elapsed
Initiating SYN Stealth Scan at 13:29
Scanning 2 hosts [1690 ports/host]
Discovered open port 22/tcp on 205.217.153.53
Discovered open port 22/tcp on 205.217.153.62
Discovered open port 80/tcp on 205.217.153.53
Discovered open port 80/tcp on 205.217.153.62
Discovered open port 53/tcp on 205.217.153.53
Discovered open port 53/tcp on 205.217.153.62
Completed SYN Stealth Scan against 205.217.153.53 in
25.94s (1 host left)
Completed SYN Stealth Scan at 13:30, 25.94s elapsed
(3340 total ports)
Initiating Service scan at 13:30
Scanning 6 services on 2 hosts
Completed Service scan at 13:30, 12.02s elapsed
(6 services on 2 hosts)
Initiating OS detection (try #1) against 2 hosts
Retrying OS detection (try #2) against 2 hosts
Initiating genl OS Detection against 205.217.153.53 at
41.875s
For OSScan assuming port 22 is open, 70 is closed, and
```

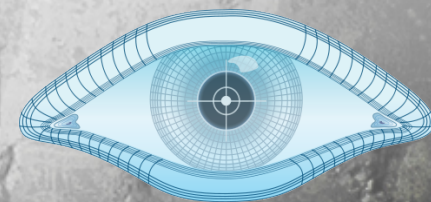


<http://nmap.org/movies/>



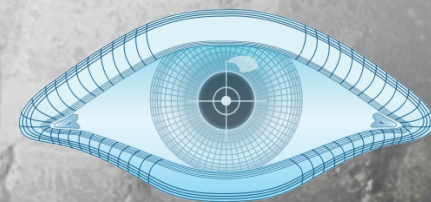
Introdução à Evasão com o Nmap

- Objetivo: evitar detecção/bloqueio por firewalls/IDSs/IPSs
- Técnicas de evasão presentes no Nmap
 - Varredura indireta
 - Abuso da confiança e/ou transferência da culpa
 - Contornar técnicas de detecção
 - Muitos pacotes em portas diferentes chamam a atenção
 - Dificultar a identificação da origem
 - Muito ruído pode dificultar a determinação da origem



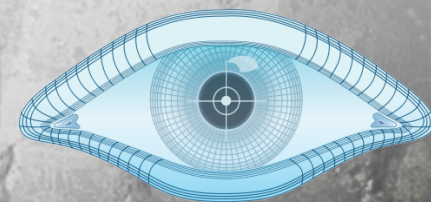
Introdução à Evasão com o Nmap

- Adendos importantes
 - Evasão → Maior consumo de recursos
 - As técnicas são adequadas para qualquer cenário
 - Cuidado com o comportamento padrão



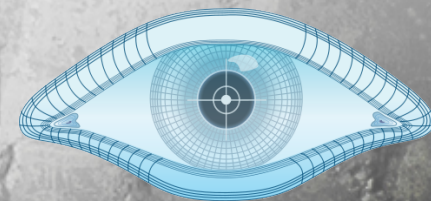
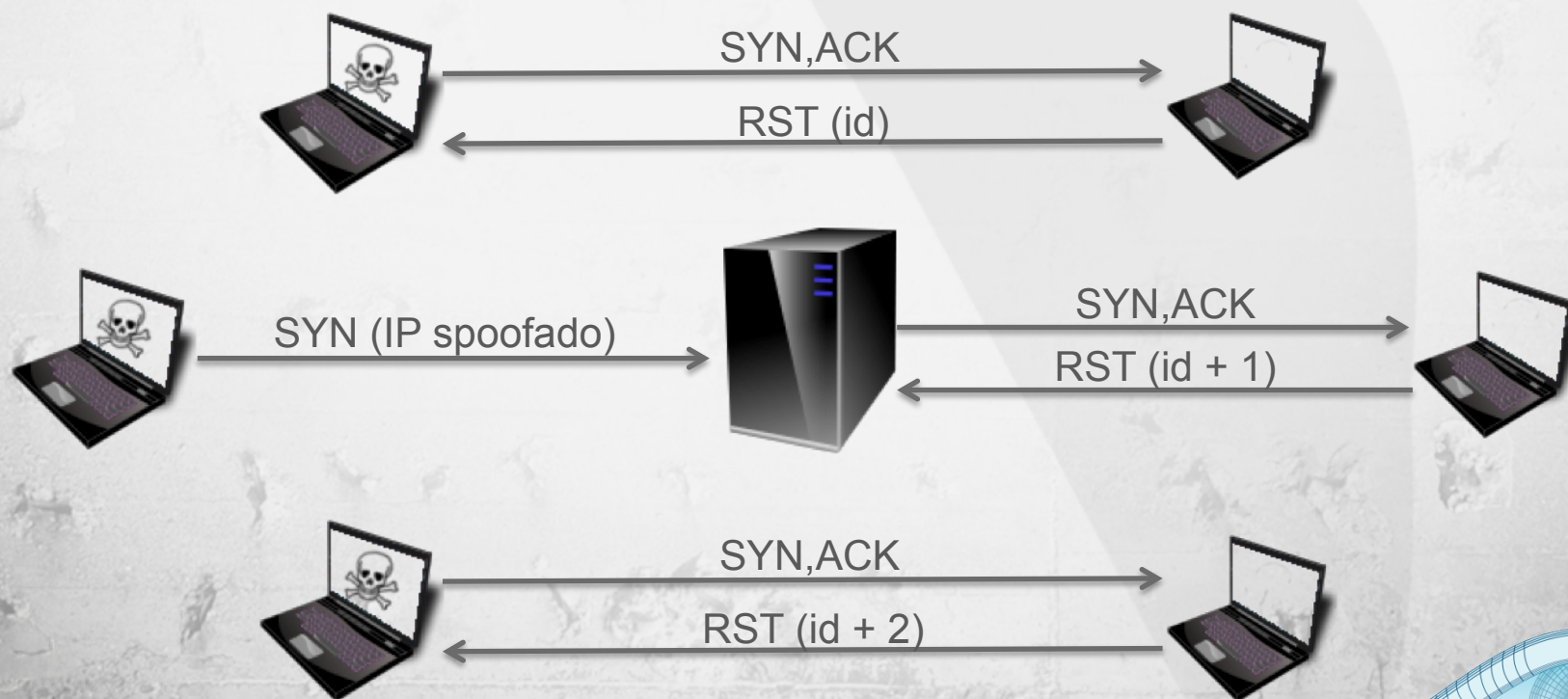
Questões relacionadas ao intermediário

- Se utilizar um intermediário qualquer
 - Simplesmente transferindo a culpa
 - Resultado iguais aos de uma varredura direta
 - A culpa é minha e eu a coloco em quem eu quiser!!!
- Se utilizar um intermediário na infraestrutura alvo
 - Abusa da confiança do host que esta na mesma infraestrutura
 - Buscando contornar controles de acesso externo
 - Pode detectar serviços que não são acessíveis externamente
 - Utiliza proxy chains



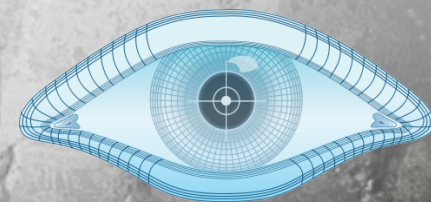
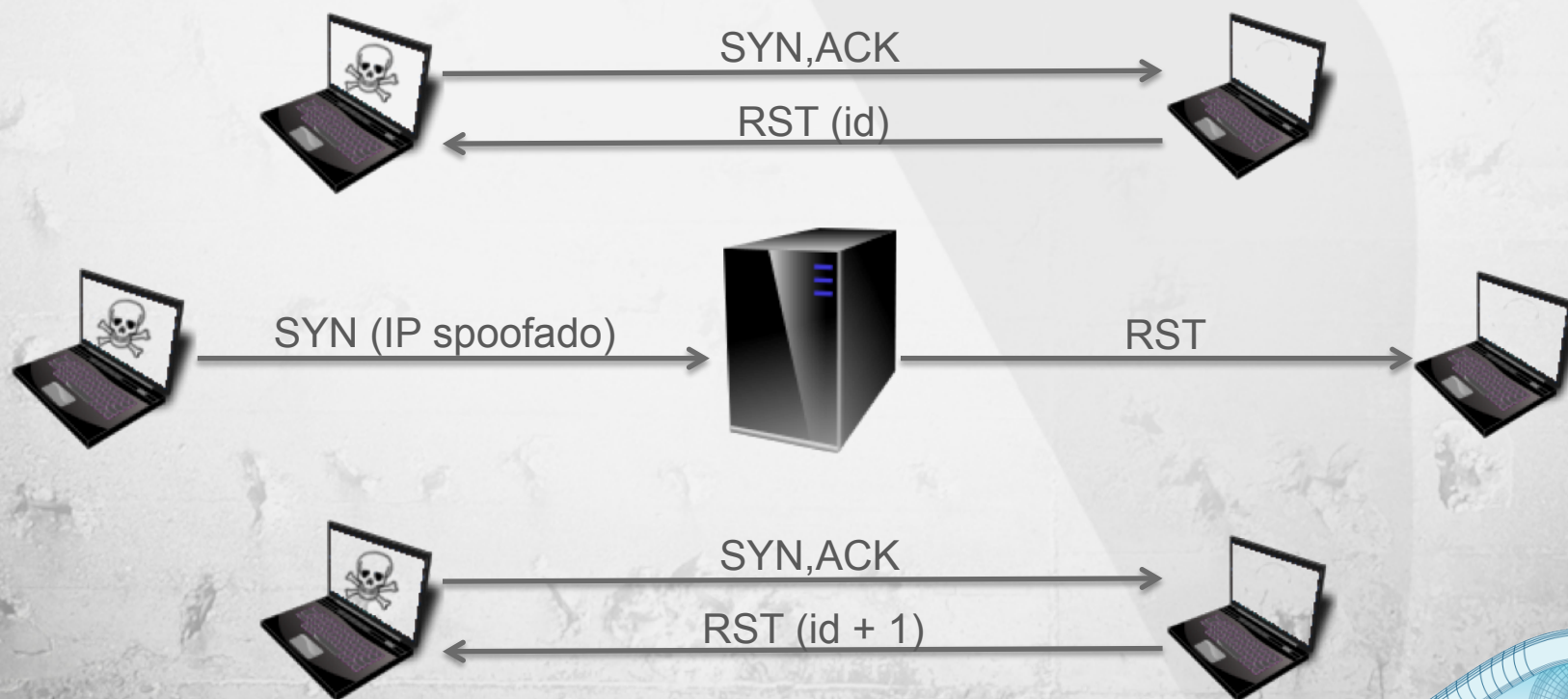
Varredura TCP Idle (-sI)

- Classificações possíveis: open e closed|filtered
- Dificuldade: encontrar intermediário vulnerável



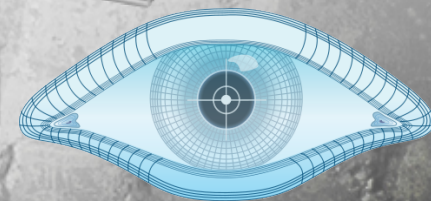
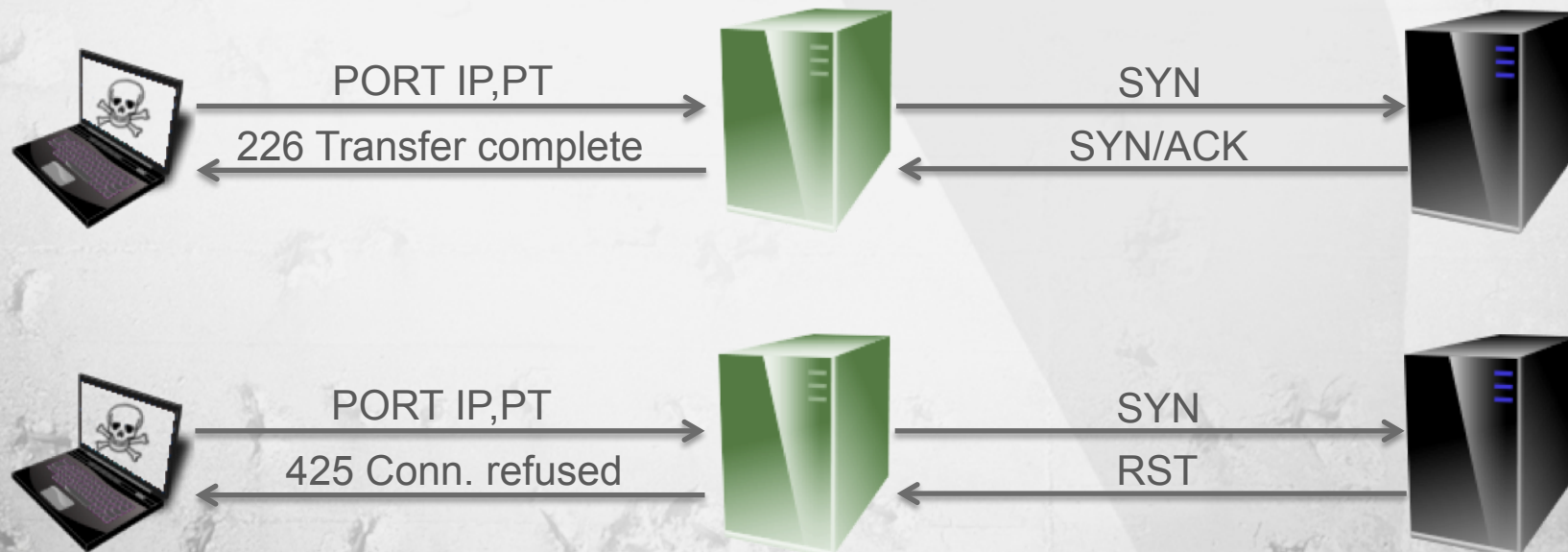
Varredura TCP Idle (-sI)

- Classificações possíveis: open e closed|filtered
- Dificuldade: encontrar intermediário vulnerável



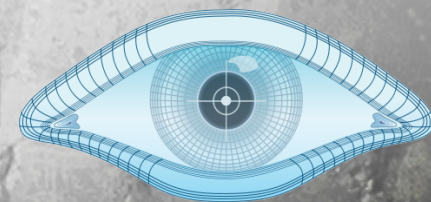
Varredura FTP Bounce (-b)

- Classificações possíveis: open, closed e filtered
- Dificuldade: encontrar servidor FTP vulnerável



Outras Abordagens Possíveis

- Varredura com spoofing IP (-S)
 - Dificuldade: interceptar o tráfego de resposta
 - Se a ideia é só transferir a culpa, dá pra fazer de tudo!
- Varredura com spoofing MAC (--spoof-mac)
 - Dificuldade: interceptar o tráfego de resposta
 - Pode simular MACs de diferentes fabricantes ou aleatório
 - Cuidado com o endereço IP!!!



IP Spoofing

```
root@kali:~# nmap -e eth0 -Pn -S 10.10.10.10 192.168.56.102

Starting Nmap 6.40 ( http://nmap.org ) at 2013-12-05 15:41 EST
NSOCK ERROR [0.0480s] mksock_bind_addr(): Bind to 10.10.10.10:0 failed
(99)
Nmap scan report for 192.168.56.102
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.56.102 are filtered
MAC Address: 08:00:27:62:5C:2C (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 34.23 seconds
```

13	13.007633	10.10.10.10	192.168.56.102	TCP	60 54667 > ddi-tcp-1 [SYN] Seq=0
14	13.007774	10.10.10.10	192.168.56.102	TCP	60 54667 > smux [SYN] Seq=0 Win=
15	13.007794	10.10.10.10	192.168.56.102	TCP	60 54667 > http [SYN] Seq=0 Win=
16	13.007813	10.10.10.10	192.168.56.102	TCP	60 54667 > imap [SYN] Seq=0 Win=
17	13.007939	10.10.10.10	192.168.56.102	TCP	60 54667 > http-alt [SYN] Seq=0 W
18	13.008075	10.10.10.10	192.168.56.102	TCP	60 54667 > rfb [SYN] Seq=0 Win=10
19	13.008094	10.10.10.10	192.168.56.102	TCP	60 54667 > rap [SYN] Seq=0 Win=10
20	13.008193	10.10.10.10	192.168.56.102	TCP	60 54667 > ms-wbt-server [SYN] Se
21	13.008288	10.10.10.10	192.168.56.102	TCP	60 54667 > pptp [SYN] Seq=0 Win=
22	13.008307	10.10.10.10	192.168.56.102	TCP	60 54667 > ssh [SYN] Seq=0 Win=10
23	14.109204	10.10.10.10	192.168.56.102	TCP	60 54668 > ssh [SYN] Seq=0 Win=10

MAC Spoofing

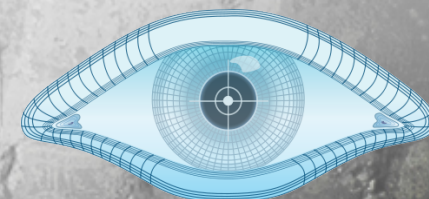
```
root@kali:~# nmap -Pn --spoof-mac Cisco 192.168.56.102

Starting Nmap 6.40 ( http://nmap.org ) at 2013-12-05 16:03 EST
Spoofing MAC address 00:00:0C:9A:2C:2E (Cisco Systems)
Nmap done: 1 IP address (0 hosts up) scanned in 0.47 seconds
```

1	0.000000	Cisco_9a:2c:2e	Broadcast	ARP	60 Who has 192.168.56.102? Tell 192.168.56.101
2	0.000070	CadmusCo_62:5c:2c	Cisco_9a:2c:2e	ARP	42 192.168.56.102 is at 08:00:27:62:5c:2c
3	0.201336	Cisco_9a:2c:2e	Broadcast	ARP	60 Who has 192.168.56.102? Tell 192.168.56.101
4	0.201392	CadmusCo_62:5c:2c	Cisco_9a:2c:2e	ARP	42 192.168.56.102 is at 08:00:27:62:5c:2c

Varredura TCP Null (-sN), FIN (-sF) e Xmas (-sX)

- Classificações possíveis: closed e open|filtered
- Varreduras para evadir de firewalls stateless mal-configurados

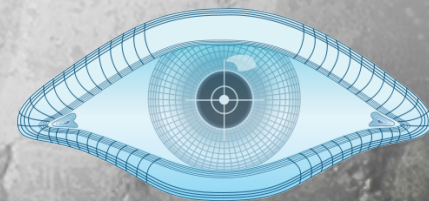


TCP Null, FIN e Xmas

13	13.005026	192.168.56.101	192.168.56.102	TCP	60 58742 > mysql [<None>] Seq=1 Win=1024 Len=0
14	13.005045	192.168.56.101	192.168.56.102	TCP	60 58742 > http [<None>] Seq=1 Win=1024 Len=0
15	13.005061	192.168.56.101	192.168.56.102	TCP	60 58742 > domain [<None>] Seq=1 Win=1024 Len=0
16	13.005075	192.168.56.101	192.168.56.102	TCP	60 58742 > smtp [<None>] Seq=1 Win=1024 Len=0
17	13.005089	192.168.56.101	192.168.56.102	TCP	60 58742 > epmap [<None>] Seq=1 Win=1024 Len=0
18	13.005299	192.168.56.102	192.168.56.101	TCP	54 epmap > 58742 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	13.005104	192.168.56.101	192.168.56.102	TCP	60 58742 > rtsp [<None>] Seq=1 Win=1024 Len=0
20	13.005389	192.168.56.102	192.168.56.101	TCP	54 rtsp > 58742 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	13.006854	192.168.56.101	192.168.56.102	TCP	60 63873 > domain [FIN] Seq=1 Win=1024 Len=0
12	13.006873	192.168.56.101	192.168.56.102	TCP	60 63873 > netbios-ssn [FIN] Seq=1 Win=1024 Len=0
13	13.006892	192.168.56.101	192.168.56.102	TCP	60 63873 > ms-wbt-server [FIN] Seq=1 Win=1024 Len=0
14	13.007056	192.168.56.102	192.168.56.101	TCP	54 ms-wbt-server > 63873 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
15	13.006910	192.168.56.101	192.168.56.102	TCP	60 63873 > pop3 [FIN] Seq=1 Win=1024 Len=0
16	13.007120	192.168.56.102	192.168.56.101	TCP	54 pop3 > 63873 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
8	13.005774	192.168.56.101	192.168.56.102	TCP	60 64709 > https [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
9	13.006078	192.168.56.102	192.168.56.101	TCP	54 https > 64709 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
10	13.005806	192.168.56.101	192.168.56.102	TCP	60 64709 > ddi-tcp-1 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
11	13.006233	192.168.56.102	192.168.56.101	TCP	54 ddi-tcp-1 > 64709 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
12	13.005830	192.168.56.101	192.168.56.102	TCP	60 64709 > h323hostcall [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
13	13.006379	192.168.56.102	192.168.56.101	TCP	54 h323hostcall > 64709 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
14	13.005851	192.168.56.101	192.168.56.102	TCP	60 64709 > auth [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Varredura TCP ACK (-sA)

- Classificações possíveis: filtered e unfiltered
- Mapeamento de regras de firewall (*firewalking*)

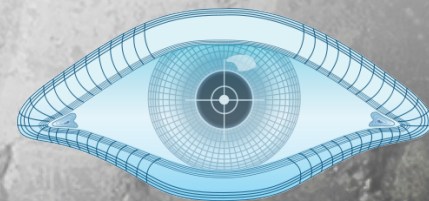


TCP ACK

5	13.007441	192.168.56.101	192.168.56.102	TCP	60 53162 > imap [ACK] Seq=1 Ack=1 Win=1024 Len=0
6	13.007673	192.168.56.102	192.168.56.101	TCP	54 imap > 53162 [RST] Seq=1 Win=0 Len=0
7	13.007461	192.168.56.101	192.168.56.102	TCP	60 53162 > sunrpc [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	13.007772	192.168.56.102	192.168.56.101	TCP	54 sunrpc > 53162 [RST] Seq=1 Win=0 Len=0
9	13.007478	192.168.56.101	192.168.56.102	TCP	60 53162 > http [ACK] Seq=1 Ack=1 Win=1024 Len=0
10	13.007859	192.168.56.102	192.168.56.101	TCP	54 http > 53162 [RST] Seq=1 Win=0 Len=0
11	13.007496	192.168.56.101	192.168.56.102	TCP	60 53162 > domain [ACK] Seq=1 Ack=1 Win=1024 Len=0
12	13.007938	192.168.56.102	192.168.56.101	TCP	54 domain > 53162 [RST] Seq=1 Win=0 Len=0
13	13.007513	192.168.56.101	192.168.56.102	TCP	60 53162 > blackjack [ACK] Seq=1 Ack=1 Win=1024 Len=0
14	13.008016	192.168.56.102	192.168.56.101	TCP	54 blackjack > 53162 [RST] Seq=1 Win=0 Len=0

Controle de Desempenho (-T)

- Perfis existentes
 - Paranóico (-T0 ou paranoid): 5min entre probes e sem paralelismo
 - Furtivo (-T1 ou sneaky): 15s entre probes e sem paralelismo
 - Educado (-T2 ou polite): 0,4s entre probes e sem paralelismo
 - Normal (-T3 ou normal): 0,4s entre probes e com paralelismo
 - Agressivo (-T4 ou aggressive): reduz intervalos de timeout
 - Insano (-T5 ou insane): reduz muito os intervalos de timeout
- Eficaz no contorno de:
 - Filtros baseados em tempo entre pacotes e vazão total



Paranóico (-T0)

1	16:44:10.880779	CadmusCo_bd:68:45	Broadcast	ARP	60 who has 192.168.56.100? Tell 192.168.56.101
2	16:49:11.581073	CadmusCo_bd:68:45	Broadcast	ARP	60 who has 192.168.56.102? Tell 192.168.56.101
3	16:53:39.538425	CadmusCo_bd:68:45	Broadcast	ARP	60 who has 192.168.56.100? Tell 192.168.56.101
4	16:54:24.646105	CadmusCo_bd:68:45	Broadcast	ARP	60 who has 192.168.56.102? Tell 192.168.56.101
5	16:54:24.646758	192.168.56.101	192.168.56.102	TCP	60 57026 > pop3s [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	16:54:29.645924	CadmusCo_bd:68:45	CadmusCo_62:5c:2c	ARP	60 192.168.56.101 is at 08:00:27:bd:68:45
7	16:59:24.750940	CadmusCo_bd:68:45	Broadcast	ARP	60 who has 192.168.56.102? Tell 192.168.56.101
8	16:59:24.751596	192.168.56.101	192.168.56.102	TCP	60 57026 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	16:59:24.752203	192.168.56.101	192.168.56.102	TCP	60 57026 > ssh [RST] Seq=1 Win=0 Len=0
10	16:59:29.744909	CadmusCo_bd:68:45	CadmusCo_62:5c:2c	ARP	60 192.168.56.101 is at 08:00:27:bd:68:45
11	17:03:08.423017	CadmusCo_bd:68:45	Broadcast	ARP	60 who has 192.168.56.100? Tell 192.168.56.101

Furtivo (-T1)

3	37.390596	192.168.56.101	192.168.56.102	TCP	60 38737 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	37.390904	192.168.56.101	192.168.56.102	TCP	60 38737 > domain [RST] Seq=1 Win=0 Len=0
5	42.382843	CadmusCo_bd:68:45	CadmusCo_62:5c:2c	ARP	60 192.168.56.101 is at 08:00:27:bd:68:45
6	52.403670	192.168.56.101	192.168.56.102	TCP	60 38737 > smux [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	57.409444	CadmusCo_bd:68:45	CadmusCo_62:5c:2c	ARP	60 who has 192.168.56.102? Tell 192.168.56.101
8	67.418961	192.168.56.101	192.168.56.102	TCP	60 38737 > https [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	82.433864	192.168.56.101	192.168.56.102	TCP	60 38737 > http-alt [SYN] Seq=0 Win=1024 Len=0 MSS=14

Educado (-T2)

3	13.406275	192.168.56.101	192.168.56.102	TCP	60 36574 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	13.406534	192.168.56.101	192.168.56.102	TCP	60 36574 > domain [RST] Seq=1 Win=0 Len=0
5	13.806657	192.168.56.101	192.168.56.102	TCP	60 36574 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	13.807006	192.168.56.101	192.168.56.102	TCP	60 36574 > ftp [RST] Seq=1 Win=0 Len=0
7	14.207421	192.168.56.101	192.168.56.102	TCP	60 36574 > imaps [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	14.608415	192.168.56.101	192.168.56.102	TCP	60 36574 > rap [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	15.009800	192.168.56.101	192.168.56.102	TCP	60 36574 > ddi-tcp-1 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	15.410918	192.168.56.101	192.168.56.102	TCP	60 36574 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Normal (-T3)

1	0.000000	CadmusCo_bd:68:45	Broadcast	ARP	60 Who has 192.168.56.102? Tell 192.168.56.101
2	13.007703	192.168.56.101	192.168.56.102	TCP	60 43001 > ms-wbt-server [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	13.007724	192.168.56.101	192.168.56.102	TCP	60 43001 > mysql [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	13.007742	192.168.56.101	192.168.56.102	TCP	60 43001 > imaps [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	13.007827	192.168.56.101	192.168.56.102	TCP	60 43001 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	13.007845	192.168.56.101	192.168.56.102	TCP	60 43001 > smux [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	13.007974	192.168.56.101	192.168.56.102	TCP	60 43001 > netbios-ssn [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	13.008043	192.168.56.101	192.168.56.102	TCP	60 43001 > h323hostcall [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Agressivo (-T4)

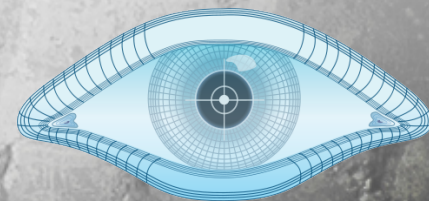
3	13.004088	192.168.56.101	192.168.56.102	TCP	60 50757 > auth [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	13.004114	192.168.56.101	192.168.56.102	TCP	60 50757 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	13.004137	192.168.56.101	192.168.56.102	TCP	60 50757 > sunrpc [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	13.004161	192.168.56.101	192.168.56.102	TCP	60 50757 > ddi-tcp-1 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	13.004186	192.168.56.101	192.168.56.102	TCP	60 50757 > ms-wbt-server [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	13.004211	192.168.56.101	192.168.56.102	TCP	60 50757 > telnet [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	13.004236	192.168.56.101	192.168.56.102	TCP	60 50757 > smtp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	13.004259	192.168.56.101	192.168.56.102	TCP	60 50757 > rfb [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Insano (-T5)

2	13.006468	192.168.56.101	192.168.56.102	TCP	60 43053 > smtp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	13.006489	192.168.56.101	192.168.56.102	TCP	60 43053 > rfb [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	13.006507	192.168.56.101	192.168.56.102	TCP	60 43053 > pop3 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	13.006542	192.168.56.101	192.168.56.102	TCP	60 43053 > submission [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	13.006646	192.168.56.101	192.168.56.102	TCP	60 43053 > smux [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	13.006723	192.168.56.101	192.168.56.102	TCP	60 43053 > imaps [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	13.006758	192.168.56.101	192.168.56.102	TCP	60 43053 > netbios-ssn [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	13.006869	192.168.56.101	192.168.56.102	TCP	60 43053 > imap [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	13.006887	192.168.56.101	192.168.56.102	TCP	60 43053 > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460

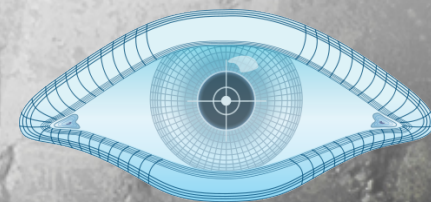
Controle de Desempenho (-T)

- Outras opções interessantes
 - Número de hosts simultâneos (--{min,max}-hostgroup)
 - Número de probes simultâneos (--{min,max}-parallelism)
 - Número de retransmissões (--max-retries)
 - Tempo de espera por respostas (--{min,max,initial}-rtt-timeout)
 - Tempo máximo de espera por host (--host-timeout)
 - Tempo de espera entre probes (--scan-delay e --max-scan-delay)
 - Controle de fluxo (--{min,max}-rate)



Outras técnicas interessantes

- Pacotes fragmentados (-f)
 - Divide o cabeçalho do protocolo de transporte
 - Eficaz no contorno de:
 - Filtros que não armazenam fragmentos para repasse
 - Filtros com severas restrições de performance
- Definição da porta de origem (-g)
 - Contorna filtros que permitem tráfego em determinadas portas
 - Portas de interesse: 20 (FTP), 53 (DNS), 67 (DHCP), 88 (Kerberos)
 - Eficaz no contorno de:
 - Firewalls mal configurados



Pacotes fragmentados (-f)

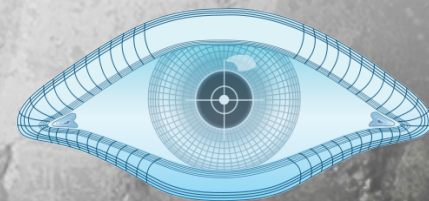
3	13.004065	192.168.56.101	192.168.56.102	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=0, ID=5bl
4	13.004087	192.168.56.101	192.168.56.102	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=8, ID=5bl
5	13.004109	192.168.56.101	192.168.56.102	TCP	60 36461 > submission [SYN] Seq=0 Win=1024 Len=0 MSS=
6	13.004158	192.168.56.101	192.168.56.102	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=0, ID=13
7	13.004179	192.168.56.101	192.168.56.102	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=8, ID=13
8	13.004202	192.168.56.101	192.168.56.102	TCP	60 36461 > imap [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	13.004222	192.168.56.101	192.168.56.102	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=0, ID=6e
10	13.004243	192.168.56.101	192.168.56.102	IPv4	60 Fragmented IP protocol (proto=TCP 6, off=8, ID=6e
11	13.004264	192.168.56.101	192.168.56.102	TCP	60 36461 > pop3 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Porta origem (-g)

2	13.003494	192.168.56.101	192.168.56.102	TCP	60 ftp-data > telnet [SYN] Seq=0 Win=1024 Len=0 MSS=
3	13.003657	192.168.56.101	192.168.56.102	TCP	60 ftp-data > pop3 [SYN] Seq=0 Win=1024 Len=0 MSS=1
4	13.003810	192.168.56.101	192.168.56.102	TCP	60 ftp-data > rtsp [SYN] Seq=0 Win=1024 Len=0 MSS=1
5	13.003935	192.168.56.101	192.168.56.102	TCP	60 ftp-data > rap [SYN] Seq=0 Win=1024 Len=0 MSS=14
6	13.004085	192.168.56.101	192.168.56.102	TCP	60 ftp-data > imap [SYN] Seq=0 Win=1024 Len=0 MSS=1
7	13.004327	192.168.56.101	192.168.56.102	TCP	60 ftp-data > domain [SYN] Seq=0 Win=1024 Len=0 MSS=
8	13.004489	192.168.56.101	192.168.56.102	TCP	60 ftp-data > telnet [RST] Seq=1 Win=0 Len=0
9	13.004684	192.168.56.101	192.168.56.102	TCP	60 ftp-data > blackjack [SYN] Seq=0 Win=1024 Len=0

Varredura com decoys (-D)

- Para cada pacote, envia outro spoofado para cada decoy
- Gera MUITO ruído, mas dificulta a definição da origem
- Eficaz no contorno de:
 - Ferramentas de gerência automatizada de logs

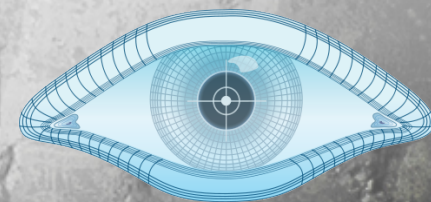


Varredura com decoys (-D)

5	13.003743	1.1.1.1	192.168.56.102	TCP	60 52552 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	13.003764	2.2.2.2	192.168.56.102	TCP	60 52552 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	13.003785	192.168.56.101	192.168.56.102	TCP	60 52552 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	13.004748	192.168.56.102	192.168.56.101	TCP	58 domain > 52552 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
9	13.003804	3.3.3.3	192.168.56.102	TCP	60 52552 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	13.003824	1.1.1.1	192.168.56.102	TCP	60 52552 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	13.003844	2.2.2.2	192.168.56.102	TCP	60 52552 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	13.003865	192.168.56.101	192.168.56.102	TCP	60 52552 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	13.004890	192.168.56.102	192.168.56.101	TCP	58 ftp > 52552 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
14	13.003884	3.3.3.3	192.168.56.102	TCP	60 52552 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	13.003903	1.1.1.1	192.168.56.102	TCP	60 52552 > imaps [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	13.003923	2.2.2.2	192.168.56.102	TCP	60 52552 > imaps [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	13.003942	192.168.56.101	192.168.56.102	TCP	60 52552 > imaps [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Com técnicas evasivas é possível:

- Enumeração de controles e filtros
- Teste da eficácia de tais controles
- Avaliação da capacidade de resposta





[**http://clav.is/slideshare**](http://clav.is/slideshare)



[**http://clav.is/twitter**](http://clav.is/twitter)



[**http://clav.is/facebook**](http://clav.is/facebook)



[**http://clav.is/youtube**](http://clav.is/youtube)

Muito Obrigado!



rafael@clavis.com.br



@rafaelsferreira

Rafael Ferreira
Sócio Diretor Técnico