Sniffing

I Workshop GRIS

Guilherme Iria

Definição

"Farejar"

Registro de informações que alcançam uma interface de rede.

Aplicações

- ➔ Detectar ataques de flood e/ou negação de serviço
- ➔ Detectar tráfego anômalo ou não permitido

  e também...

- ➔ Capturar dados sigilosos

Modo Promíscuo

Recepção de todos os pacotes que trafegam pelo mesmo segmento de rede do receptor, não importando o destino do pacote.

Hub

Replica os dados recebidos em uma porta para TODAS as demais.

Ambiente altamente suscetível ao sniffing

Switch

- Encaminha os dados para a porta com a máquina de destino
- Máquinas mapeadas em uma tabela. [*Endereço físico X Porta do switch*]
- Ambiente que dificulta o sniffing, porém não o impossibilita

Roteadores

- Trabalha na camada 3 do modelo OSI.
- Tabelas de roteamento
- Conecta pelo menos 2 redes
- Transfere os pacotes baseando-se em endereços IP's

O Protocolo ARP

- Traduz IP's em MAC address
- Requisição feita por *broadcast*
- *Cache* ARP

Port Mirroring

- Espelhamento do tráfego

MAC *flooding*

Memória limitada
+ Muitas respostas ARP forjadas

Problemas

ARP spoofing

Técnica “Man in the middle”

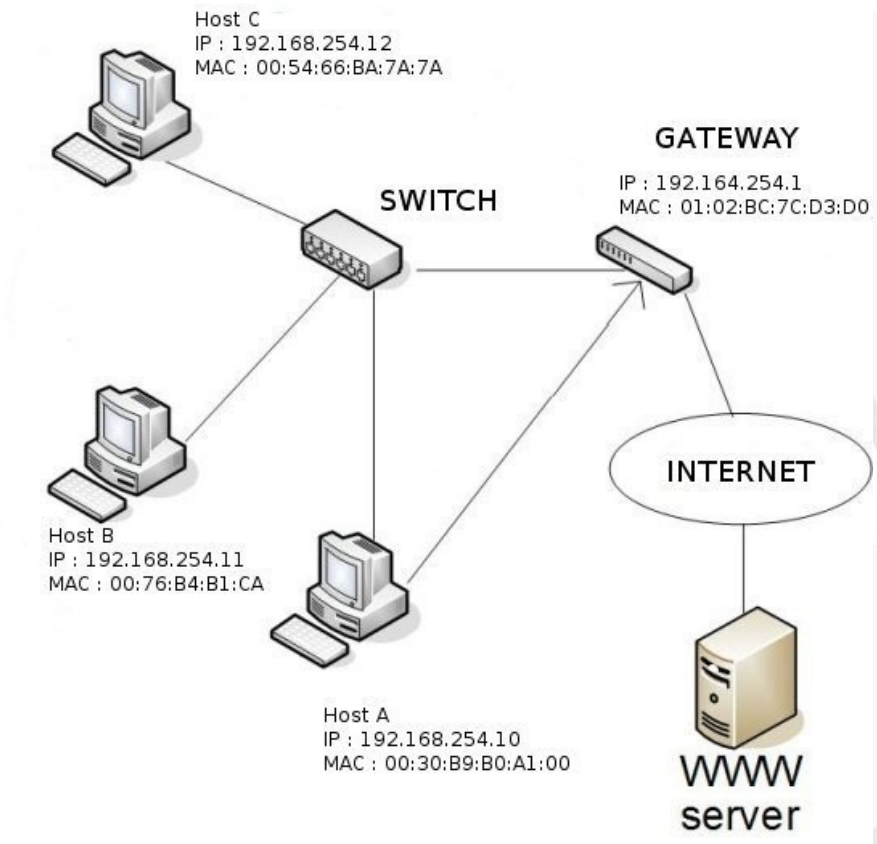
Máquina do atacante:

I. Forja pacotes de resposta ARP

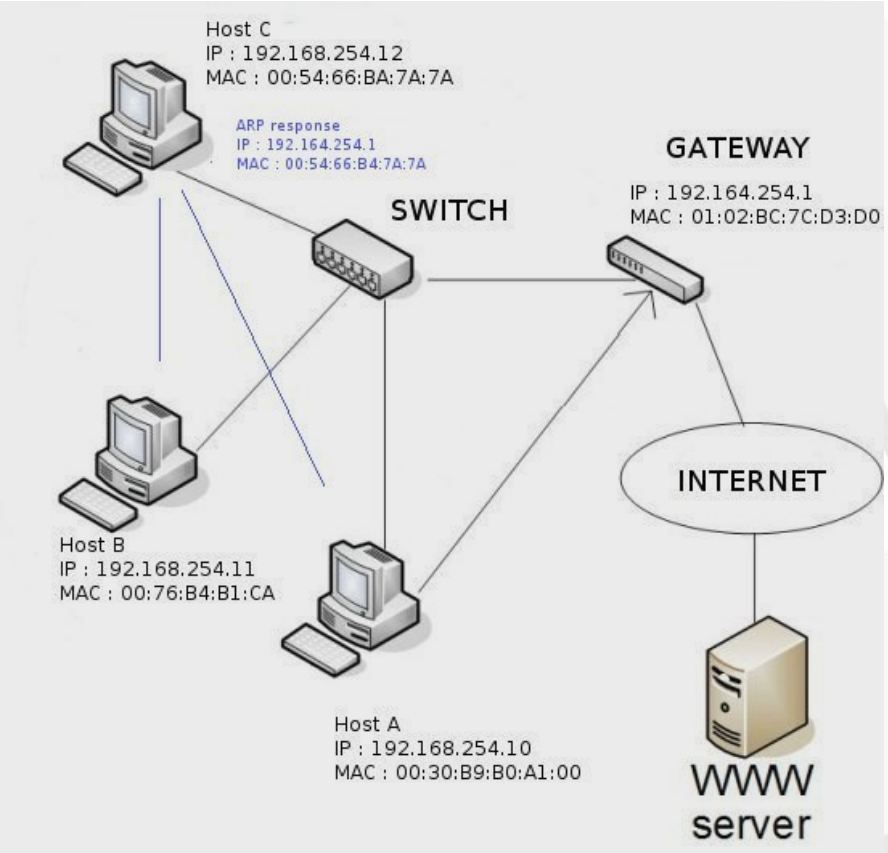
II. Analisa tráfego

III. Repassa os dados para destinatário real

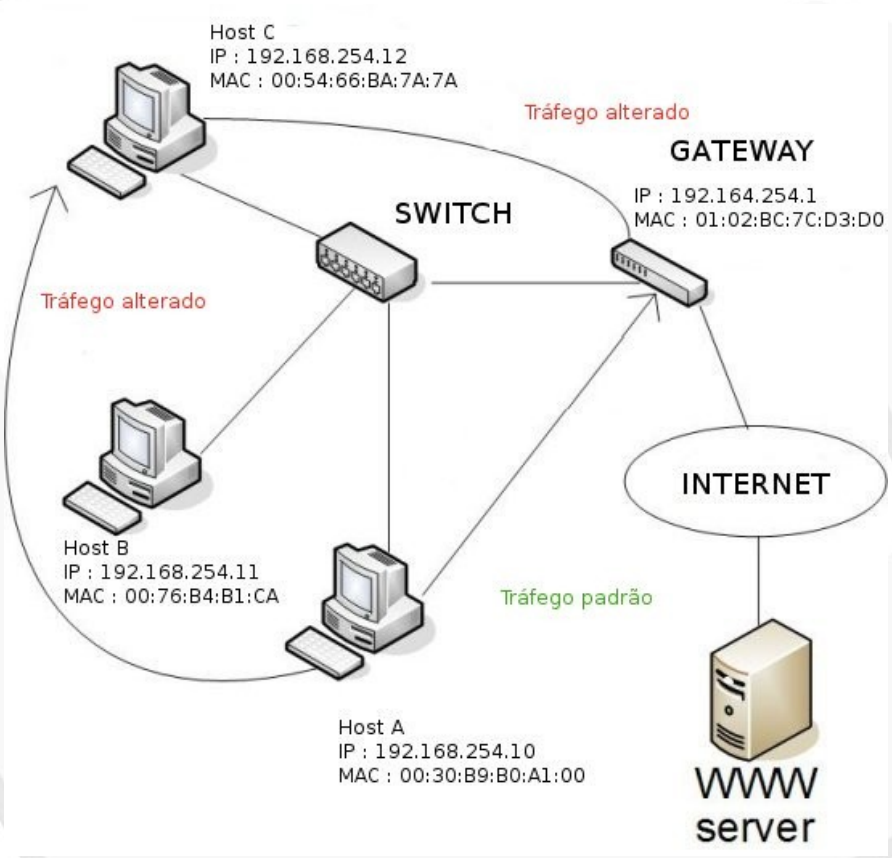
ARP spoofing



ARP spoofing



ARP spoofing



Ferramentas

- TCPDump
- Wireshark
- Suíte Dsniff
  - dsniff - senhas
  - arpspoof – arpspoofing
  - macof – mac flooding
  - urlsnarf – pedidos http
  - tcpkill – fecha conexão tcp
  - sshmitm – logins e senhas por ssh
  - webmitm – logins e senhas http/https
  - webspy – exibe navegação da vítima em tempo real

Ferramentas

- Ettercap
  - Coleta automaticamente senhas de variados protocolos
  - Captura logins e senhas de SSHv1
  - Intercepta sessões de https (certificado falso)
  - Procura por outros sniffers na rede

Filtros

- *[Expressão]*
  - *seleciona que pacotes serão aceitos na captura*
  - *aceita pacotes onde [expressão] for verdadeira*
  - *palavras reservadas e seus tipos :*
    - *Tipo: host, net, port, ...*
    - *Protocolo: ether, ip, tcp, udp, arp, rarp, ...*
    - *Direção: src, dst, src and dst, src or dst, ...*
    - *Operadores lógicos: and, or, not.*

Filtros

- exemplos:
  - `tcpdump -ni eth0 'arp net 192.164'`

    aceita pacotes arp somente da rede 192.164.0.0

  - `tcpdump -ni eth0 'src net 10.10.10.0/24 and dst host 192.168.0.1 and dst port 80'`

    só aceita pacotes da rede 10.10.10.0/24 que vão para 192.168.0.1 na porta 80

Ettercap

Shell - Konsole <3>

```
bt ~ # ettercap -Tzq //21,22,80,443

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on eth0... (Ethernet)

  eth0 ->       YY:YY:YY:YY:YY:YY     XXX.XXX.XXX.XXX       255.255.224.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

Ettercap

Shell - Konsole

```
bt ~ # ftp ftp.openbsd.org
Connected to openbsd.sunsite.ualberta.ca.
220-
220-                    Welcome to SunSITE Alberta
220-
220-     at the University of Alberta, in Edmonton, Alberta, Canada
220-
220-All connections to and transfers from this server are logged. If
220-you do not like this policy, please disconnect now.
220-
220-You may want to grab the index file called "ls-lR.gz" in /pub.  It is
220-updated nightly with the contents of the ftp tree.
220-
220-    If you have any questions, hints, or requests, please email
220-
220-            sunsite@sunsite.ualberta.ca
220-
220
Name (ftp.openbsd.org:root): anonymous
331 Who are you impersonating today?
Password:
230-
230-    Welcome to Sunsite Alberta
230- Login Successful.
230 Your data rate unrestricted
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Ettercap

```
ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on eth0... (Ethernet)

  eth0 ->                                                  255.255.224.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

FTP : 129.128.5.191:21 -> USER: anonymous  PASS: z3_ru3l4@yahoo.com.br
```

Login http


ARSENAL.COM
CONTACT US
ARSENAL TV ONLINE
SHOPPING
MEMBERSHIP
MOBILE
EMIRATES STADIUM
Arsenal.com
BET £20 GET FREE!
paddypower.com
poker · casino · betting · games
Login | Help | Sign up | RSS
Live Search
Go
Home A - Z News Fixtures Tickets Match First Team Reserves/Youth Ladies The Club Fanzone Hospitality Betting
LOG IN TO ARSENAL.COM
Username Jason_Voorhees
Password **********
Go
Login Help | Forgotten password
Please note: The above login is for registered users of the Arsenal.com site or Arsenal TV Online subscribers only. If you are a Red, Silver or Gold Member and you are trying to log-in using your seven digit number you will need to click here to access the Membership login.
Unfortunately, being a Red, Silver or Gold Member does not grant access to the Arsenal.com/TV Online services and being a registered user of the website does not relate to any ticket membership.
Can't remember your username? It is likely to be your e-mail address.
News
News Headlines
News Archive
Injury News
Reserves News
Ladies News
Junior Gunners News
O2 Podcast
O2 Vodcast
Arsenal Gadget
Manager's Email
Newsletter
TWO WAYS TO WATCH Arsenal TV
FREE ARSENAL TV ONLINE!
Arsenal TV ONLINE
ARSENAL TV ONLINE IS FREE WHEN YOU JOIN BT TOTAL BROADBAND

Login http

```
bt / # tcpdump -n -s0 -w /dump.cap not port 53 and not arp
```

opções: -n : não traduz IP por consulta dns
-s[num]: captura pacotes com [num] bytes. Padrão é 68
-w [arquivo] : salva em arquivo binário

Login http

dump.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: http | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
4	0.306011		87.86.92.85	HTTP	POST /asp/verifyuser.asp?log=true HTTP/1.1
6	0.781181		87.86.92.85	HTTP	Continuation or non-HTTP traffic (application/x-www-form-urlencoded
7	1.111968	87.86.92.85		HTTP	HTTP/1.0 302 Object moved (text/html)
9	1.116059		87.86.92.85	HTTP	GET /article.asp?article=badlogin&title=Incorrect+Logon HTTP/1.1
50	2.567617		64.154.81.197	HTTP	GET /HG?hc=&hb=DM540205DGDW&cd=1&hv=6&n=/article%20%28title%20%3D%2
51	2.567657		64.154.81.197	HTTP	Continuation or non-HTTP traffic
73	2.719546		87.86.92.85	HTTP	GET /CommonScripts/common.js HTTP/1.1
77	2.726056	87.86.92.85		HTTP	HTTP/1.0 200 OK (text/html)
81	2.840321	64.154.81.197		HTTP	HTTP/1.1 200 OK (GIF89a)
95	3.609535	87.86.92.85		HTTP	HTTP/1.1 200 OK (application/x-javascript)
97	3.636666		87.86.92.85	HTTP	GET /includes/js/GreatMoments.js HTTP/1.1
128	3.953681	87.86.92.85		HTTP	HTTP/1.0 200 OK (application/x-javascript)
130	4.085590		87.86.92.85	HTTP	GET /includes/css/article.css?v=1 HTTP/1.1
221	5.017688	87.86.92.85		HTTP	HTTP/1.1 200 OK (text/css)

```
▷ Frame 6 (218 bytes on wire, 218 bytes captured)
▷ Ethernet II, Src:
▷ Internet Protocol, Src:
▷ Transmission Control Protocol, Src Port: 36640 (36640), Dst Port: http (80), Seq: 500, Ack: 1, Len: 152
▽ Hypertext Transfer Protocol
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 81
    \r\n
▽ Line-based text data: application/x-www-form-urlencoded
    ReturnURL=%2Findex.asp&UserName=Jason_Voorhees&Password=OndeTahMinhaFaca&x=16&y=6
```

```
0000                                              .0..z..0 O7l...E.
0010                                              ....@.@. ...%..WV
0020                                              \U. .P.g .w......
0030  00 b7 8a 54 00 00 01 01  08 0a 00 05 e2 47 02 bc   ...T.... .....G..
```

File: "/mnt/sda1/dump.cap" 334 KB 00:00:12 | P: 458 D: 60 M: 0

Shell - Konsole | dump.cap - Wiresh | 2 | 22:42

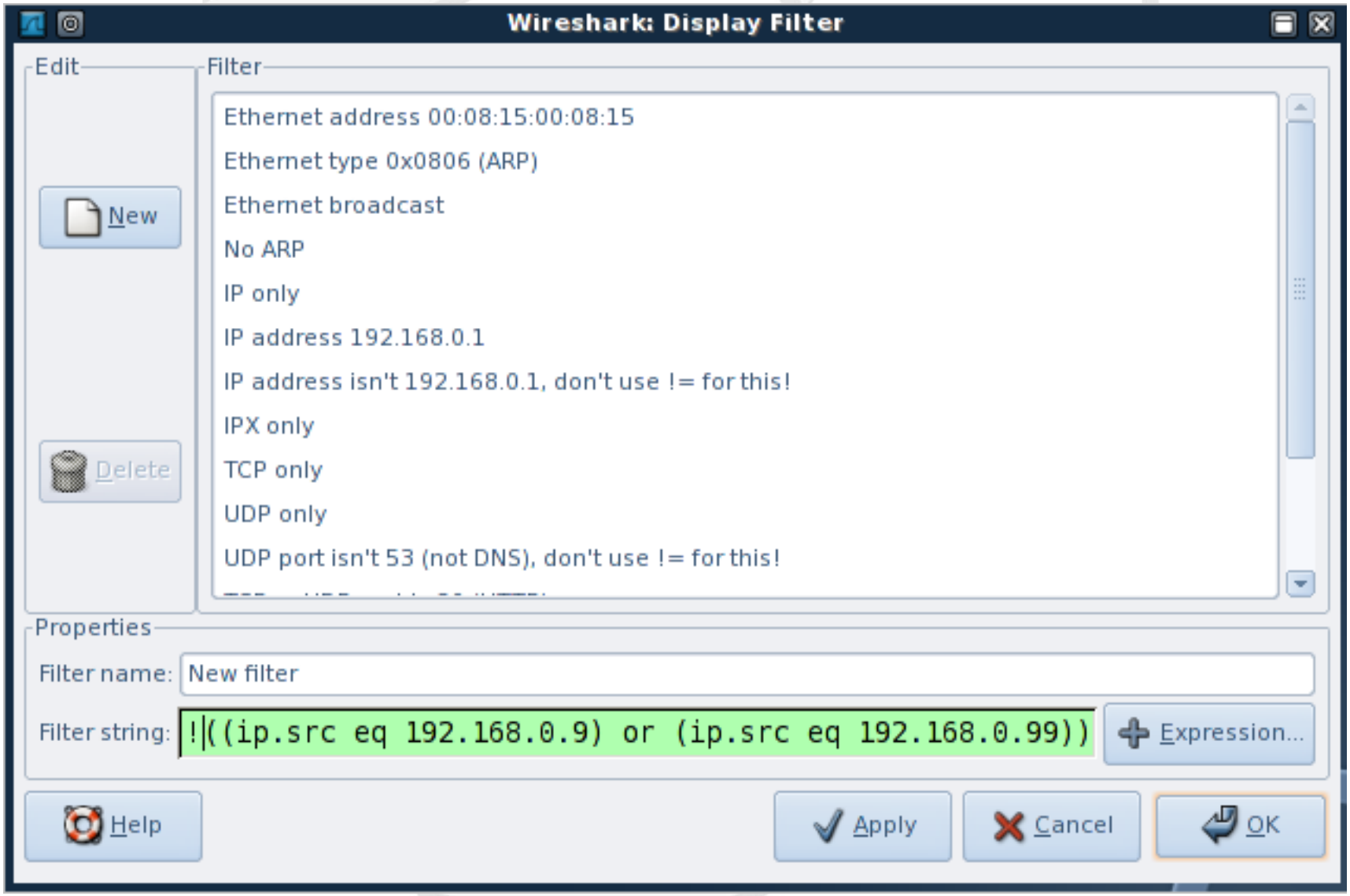
Scan

- Analise alguns dados de log de um IDS e responda:
  - O que está acontecendo na rede ?
  - Quem está envolvido ?
  - O que conseguiu ?

Scan

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.9	192.168.0.99	ICMP	Echo (ping) request
2	0.000078	192.168.0.99	192.168.0.9	ICMP	Echo (ping) reply
3	0.000044	192.168.0.9	192.168.0.99	TCP	52218 > http [ACK] Seq=0 Ack=0 Win=2048 Len=0
4	0.000119	192.168.0.99	192.168.0.9	TCP	http > 52218 [RST] Seq=0 Len=0
5	10.346091	192.168.0.9	192.168.0.99	TCP	52198 > 52156 [SYN] Seq=0 Len=0
6	10.346199	192.168.0.99	192.168.0.9	TCP	52156 > 52198 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
7	10.346137	192.168.0.9	192.168.0.99	TCP	52198 > 28494 [SYN] Seq=0 Len=0
8	10.346235	192.168.0.99	192.168.0.9	TCP	28494 > 52198 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
9	10.346167	192.168.0.9	192.168.0.99	TCP	52198 > 11179 [SYN] Seq=0 Len=0
10	10.346246	192.168.0.99	192.168.0.9	TCP	11179 > 52198 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
11	10.346193	192.168.0.9	192.168.0.99	TCP	52198 > 11796 [SYN] Seq=0 Len=0
12	10.346274	192.168.0.99	192.168.0.9	TCP	11796 > 52198 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
13	10.346228	192.168.0.9	192.168.0.99	TCP	52198 > 44101 [SYN] Seq=0 Len=0
14	10.346297	192.168.0.99	192.168.0.9	TCP	44101 > 52198 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0

Scan


Wireshark: Display Filter
Edit
Filter
New
Delete
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
Properties
Filter name:
New filter
Filter string:
!((ip.src eq 192.168.0.9) or (ip.src eq 192.168.0.99))
Expression...
Help
Apply
Cancel
OK

Scan

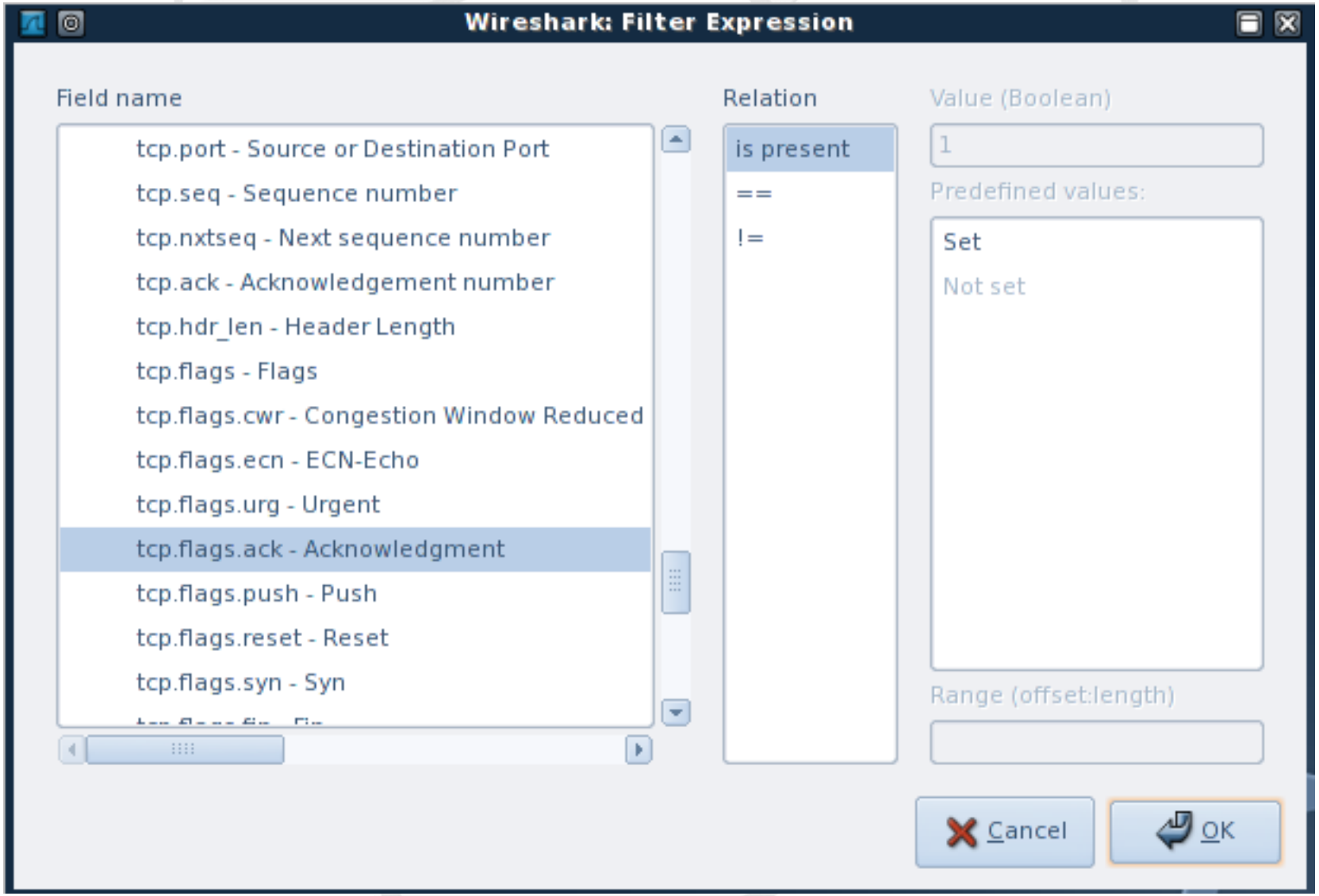
155987	1602.084879	192.168.0.1	192.168.0.99	ICMP	Echo (ping) request
155988	1602.084912	192.168.0.254	192.168.0.99	ICMP	Echo (ping) request
155989	1602.084941	192.168.0.199	192.168.0.99	ICMP	Echo (ping) request
155990	1602.084976	192.168.0.199	192.168.0.99	ICMP	Echo (ping) request
155991	1602.085026	192.168.0.1	192.168.0.99	TCP	35984 > http [ACK] Seq=1 Ack=1 Win=3072 Len=0
155992	1602.085031	192.168.0.254	192.168.0.99	TCP	35984 > http [ACK] Seq=1 Ack=1 Win=3072 Len=0
155995	1602.085111	192.168.0.199	192.168.0.99	TCP	35984 > http [ACK] Seq=1 Ack=1 Win=3072 Len=0
156008	1612.404870	192.168.0.1	192.168.0.99	TCP	35964 > qbikgdp [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156009	1612.404914	192.168.0.254	192.168.0.99	TCP	35964 > qbikgdp [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156012	1612.404992	192.168.0.199	192.168.0.99	TCP	35964 > qbikgdp [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156013	1612.405153	192.168.0.1	192.168.0.99	TCP	35964 > gridgen-elmd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156014	1612.405159	192.168.0.254	192.168.0.99	TCP	35964 > gridgen-elmd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156017	1612.405236	192.168.0.199	192.168.0.99	TCP	35964 > gridgen-elmd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156018	1612.405269	192.168.0.1	192.168.0.99	TCP	35964 > dca [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156019	1612.405291	192.168.0.254	192.168.0.99	TCP	35964 > dca [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156022	1612.405363	192.168.0.199	192.168.0.99	TCP	35964 > dca [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156023	1612.405415	192.168.0.1	192.168.0.99	TCP	35964 > 6008 [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156024	1612.405431	192.168.0.254	192.168.0.99	TCP	35964 > 6008 [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156027	1612.405514	192.168.0.199	192.168.0.99	TCP	35964 > 6008 [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156028	1612.405567	192.168.0.1	192.168.0.99	TCP	35964 > ncube-lm [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156029	1612.405597	192.168.0.254	192.168.0.99	TCP	35964 > ncube-lm [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156032	1612.405662	192.168.0.199	192.168.0.99	TCP	35964 > ncube-lm [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156033	1612.405715	192.168.0.1	192.168.0.99	TCP	35964 > urd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156034	1612.405729	192.168.0.254	192.168.0.99	TCP	35964 > urd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156037	1612.405812	192.168.0.199	192.168.0.99	TCP	35964 > urd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156038	1612.405856	192.168.0.1	192.168.0.99	TCP	35964 > nest-protocol [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156039	1612.405871	192.168.0.254	192.168.0.99	TCP	35964 > nest-protocol [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156042	1612.405925	192.168.0.199	192.168.0.99	TCP	35964 > nest-protocol [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156043	1612.405979	192.168.0.1	192.168.0.99	TCP	35964 > qotd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156044	1612.406007	192.168.0.254	192.168.0.99	TCP	35964 > qotd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
156047	1612.406067	192.168.0.199	192.168.0.99	TCP	35964 > qotd [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0

Scan

Wireshark: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	4732	283920	0.038	0	0	0.000
Ethernet	100.00%	4732	283920	0.038	0	0	0.000
Internet Protocol	100.00%	4732	283920	0.038	0	0	0.000
Internet Control Message Protocol	0.08%	4	240	0.000	4	240	0.000
Transmission Control Protocol	99.92%	4728	283680	0.038	4728	283680	0.038

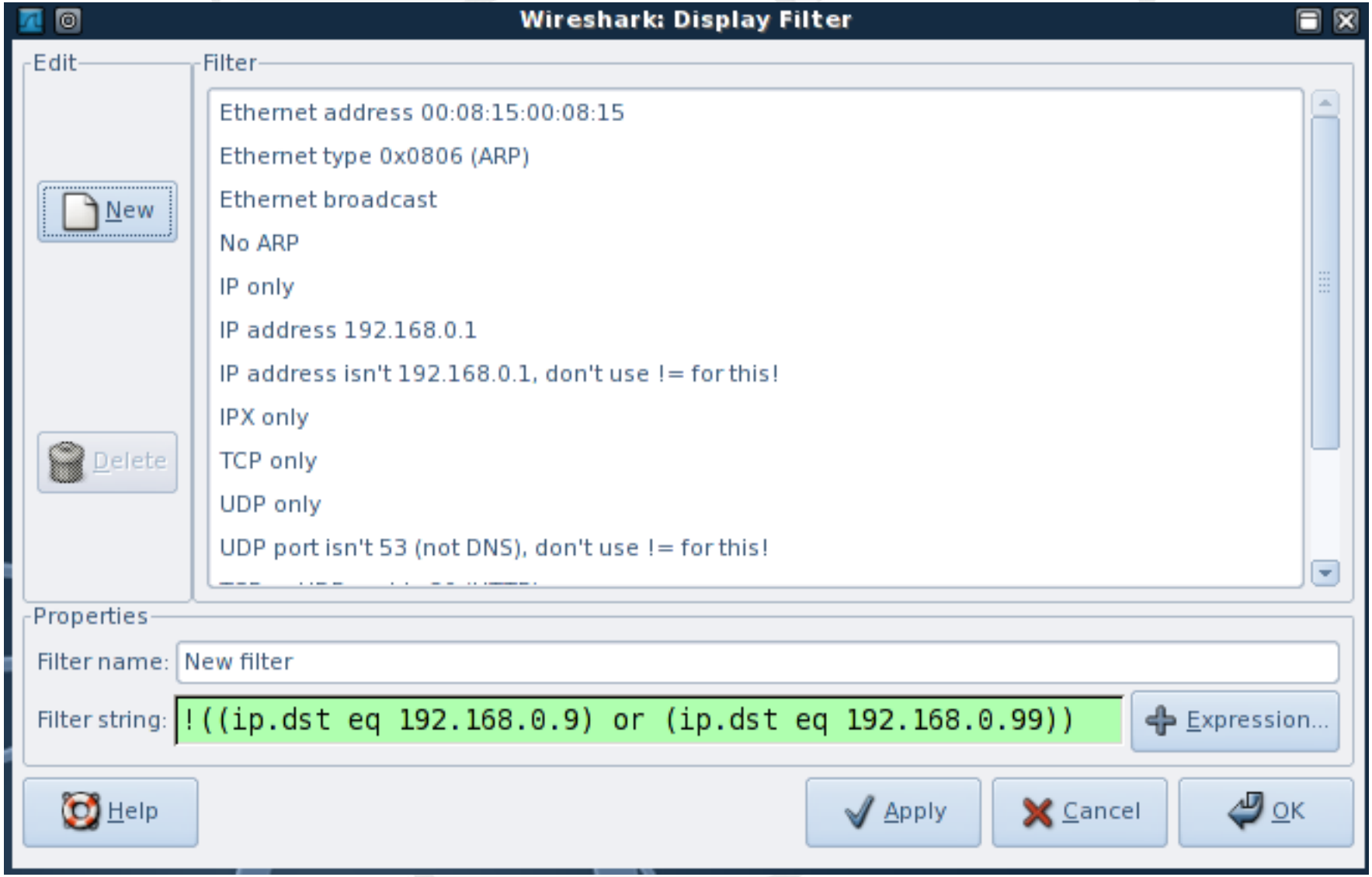
Scan


Wireshark: Filter Expression
Field name
tcp.port - Source or Destination Port
tcp.seq - Sequence number
tcp.nxtseq - Next sequence number
tcp.ack - Acknowledgement number
tcp.hdr_len - Header Length
tcp.flags - Flags
tcp.flags.cwr - Congestion Window Reduced
tcp.flags.ecn - ECN-Echo
tcp.flags.urg - Urgent
tcp.flags.ack - Acknowledgment
tcp.flags.push - Push
tcp.flags.reset - Reset
tcp.flags.syn - Syn
Relation
is present
==
!=
Value (Boolean)
1
Predefined values:
Set
Not set
Range (offset:length)
Cancel
OK

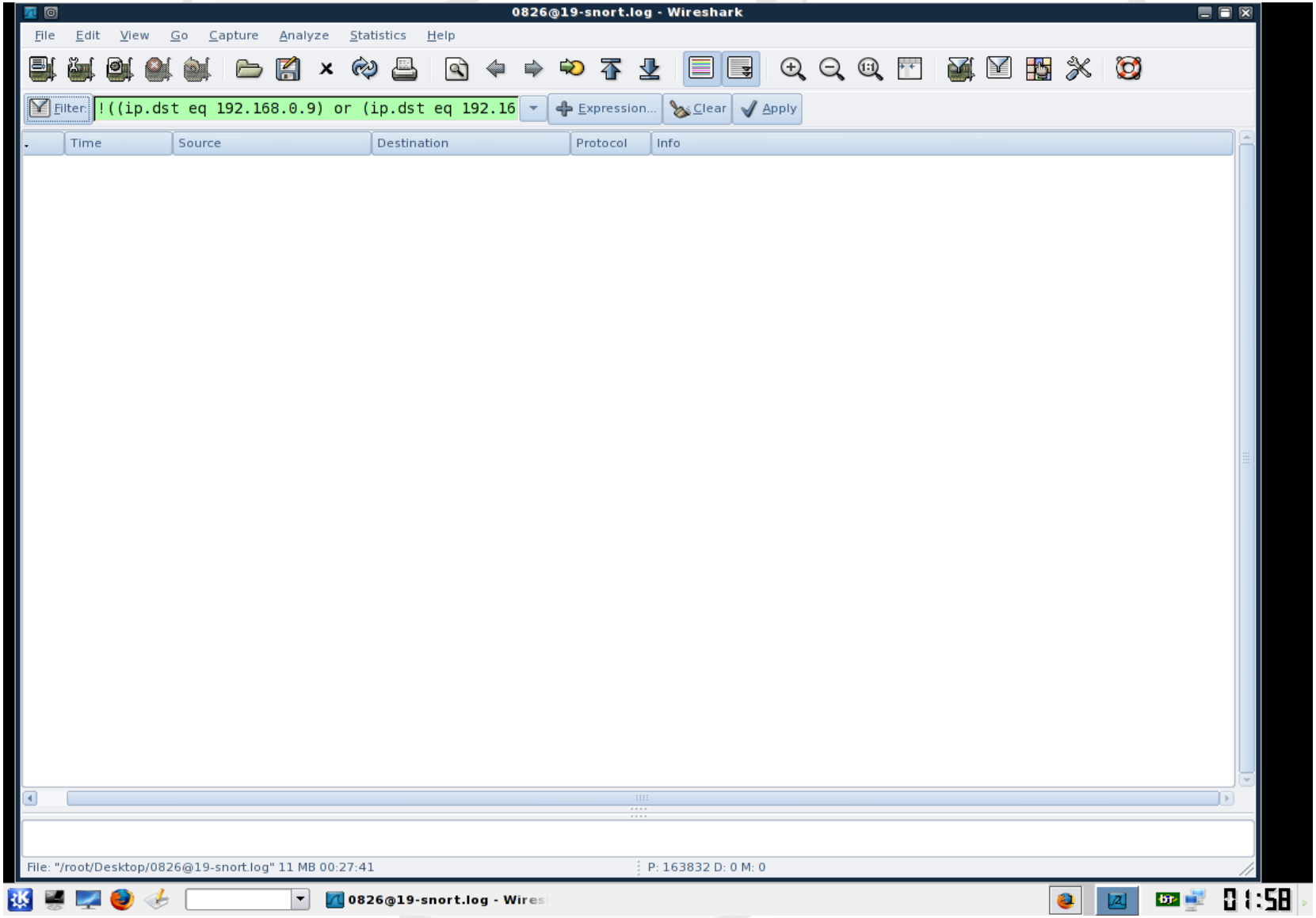
Scan

8332	158.126037	192.168.0.99	192.168.0.9	TCP	22 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8686	162.118460	192.168.0.99	192.168.0.9	TCP	22 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
9610	168.118458	192.168.0.99	192.168.0.9	TCP	22 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
0890	180.118458	192.168.0.99	192.168.0.9	TCP	22 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3772	204.318458	192.168.0.99	192.168.0.9	TCP	22 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8876	252.518458	192.168.0.99	192.168.0.9	TCP	22 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
1061	680.600481	192.168.0.99	192.168.0.9	TCP	111 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
1643	684.598460	192.168.0.99	192.168.0.9	TCP	111 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2313	690.598459	192.168.0.99	192.168.0.9	TCP	111 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3653	702.598458	192.168.0.99	192.168.0.9	TCP	111 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
5062	716.351779	192.168.0.99	192.168.0.9	TCP	32768 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
5086	716.669146	192.168.0.99	192.168.0.9	TCP	32768 > 52199 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
5494	720.348460	192.168.0.99	192.168.0.9	TCP	32768 > 52198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

Scan


Wireshark: Display Filter
Edit
Filter
New
Delete
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
Properties
Filter name:
New filter
Filter string:
!((ip.dst eq 192.168.0.9) or (ip.dst eq 192.168.0.99))
Expression...
Help
Apply
Cancel
OK

Scan


0826@19-snort.log - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: !((ip.dst eq 192.168.0.9) or (ip.dst eq 192.16
Expression... Clear Apply
Time Source Destination Protocol Info
File: "/root/Desktop/0826@19-snort.log" 11 MB 00:27:41
P: 163832 D: 0 M: 0
0826@19-snort.log - Wires
01:58

Scan

- Repostas:
  - O que está acontecendo?

    r: PortScan, status de portas.

  - Quem está envolvido?

    r: máquina 192.168.0.9, as outras máquinas foram usadas como chamarizes para esconder o endereço real do atacante

  - O que conseguiu?

    r: Portas abertas : 22, 53, 80, 443, 32768

Proteção

Substituir Hubs por switchs

Uso de protocolos/soluçoes que usam criptografia
- SSH
- Secure Sockets Layer (SSL)
- OpenPGP
- S/MIME

Arpwatch

MAC Binding

Referências

- http://www.honeynet.org/
- http://www.guiadohardware.net/
- http://www.tcpdump.org
- http://www.wikipedia.org/

e para não perder o costume:

- http://www.google.com
- Man pages

Obrigado !!!

Já chegou ao fim????
sniff... sniff... sniff

Até a próxima....