Auditor Security Collection

Maryam Arouzi

Auditor Security Collection

The Auditor security collection is a GPL-licensed live CD based on Knoppix, with more than 300 security software tools. Auditor gives you easy access to a broad range of tools for security audits and penetration testing in almost no time. The Auditor Security Collection's primary focus is on computer security and forensics, and incident response.

Auditor Security Collection – Cont'd

Auditor's menu is divided into several "tool groups" for easy recognition:

- Footprinting -- Applications to gain initial knowledge about a server, such as Whois and Dig.
- Analysis -- Tools to analyze a network, such as Ethereal, Etherape.
- Scanning -- Tools to scan the network, such as Nmap.
- Wireless -- Applications to test the wireless network.
- Brute-forcing -- The brute-force password cracking word list holds more than 64 million word entries, according to the Auditor Web site.
- Cracking -- Cracking tools to be used with the brute-force word lists.

Security Controls

According to the National Institute of Standards and Technology, by enforcing technical, managerial, and operational security controls one can prevent, detect, and recover IT systems from security threats.

Technical Security Controls

- Support - allow implementation of other crontrols
- Prevent - avoid security breaches from occurring
- Detect and Recover - allow for the system to recover from a security breach by utilizing audits, intrusion detection and containment, proof of wholeness, restoration to a secure state, and virus detection.

Technical Security Controls - Cont'd

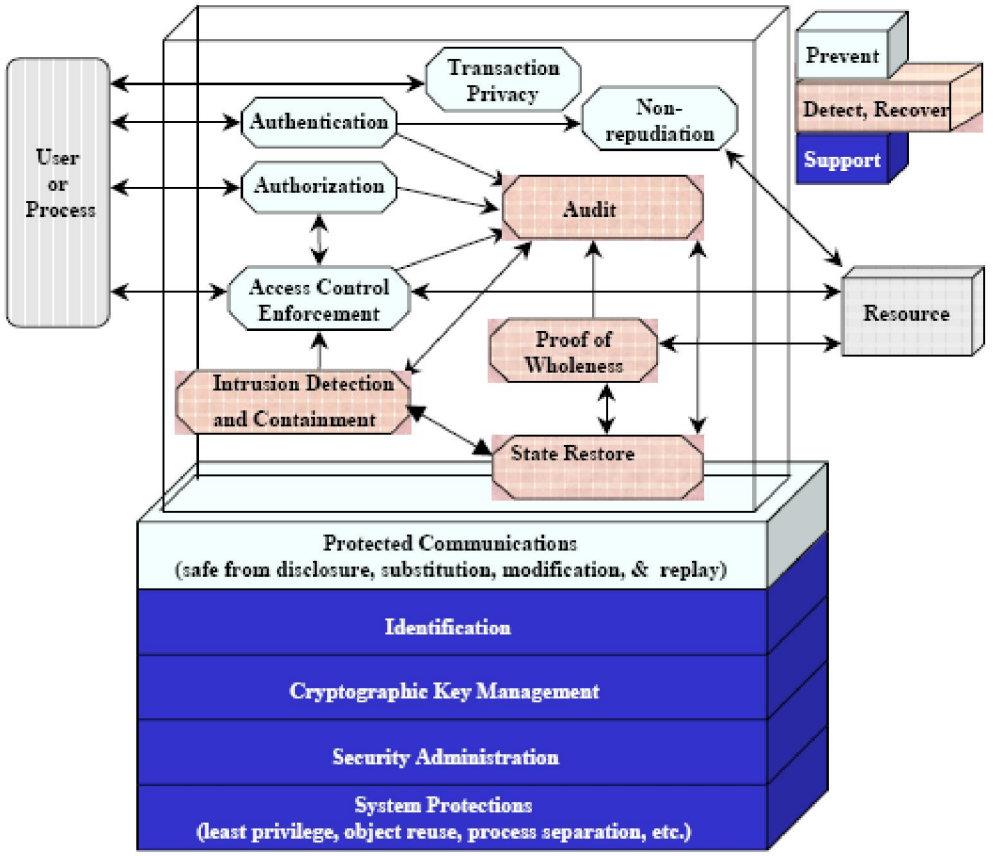


Figure 4-3. Technical Security Controls

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Technical Security Controls - Cont'd

- Auditor Security Collection facilitates audit and detection controls because it is not only very useful for conducting security audits, but it is also very useful for retrieving files from a damaged hard drive in a non-booting system.
- Ethereal, Etherape, and Nmap can all be used to demonstrate these technical audit, monitoring, and detection controls

Etherape

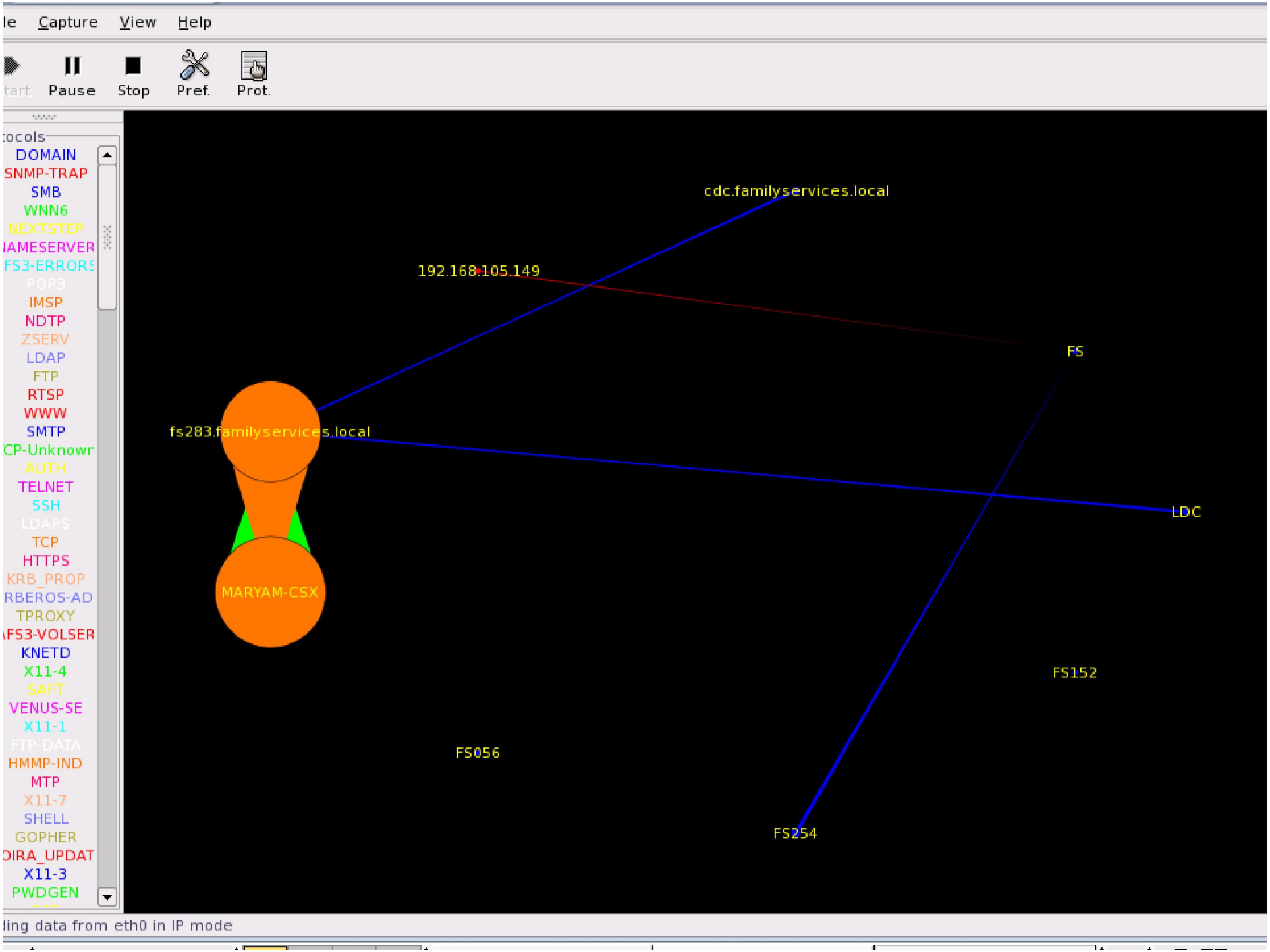
Etherape is used to monitor network traffic. Featuring link layer, IP and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. It supports Ethernet, FDDI, Token Ring, ISDN, PPP and SLIP devices. It can filter traffic to be shown, and can read traffic from a file as well as live from the network.

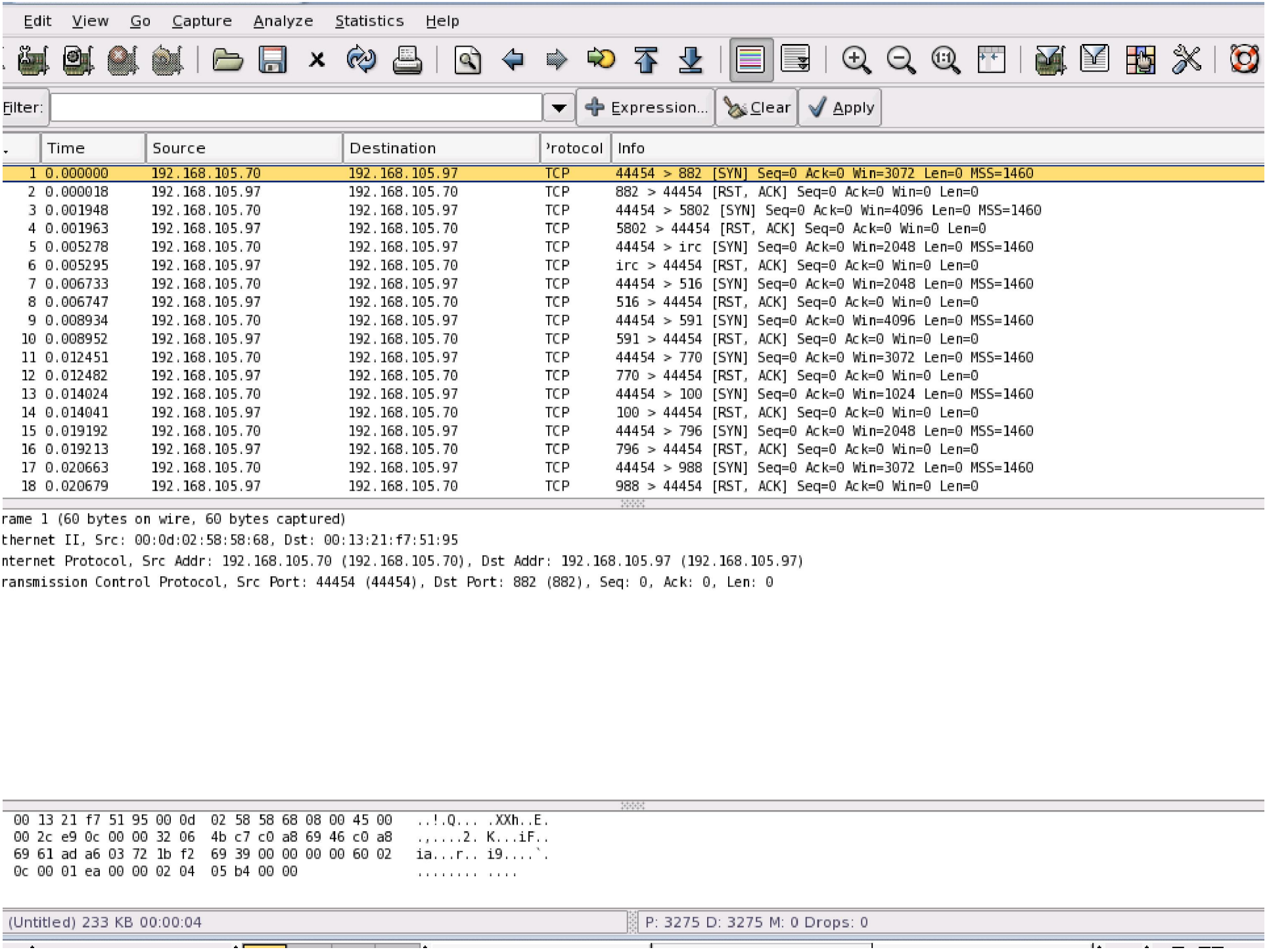
Ethereal

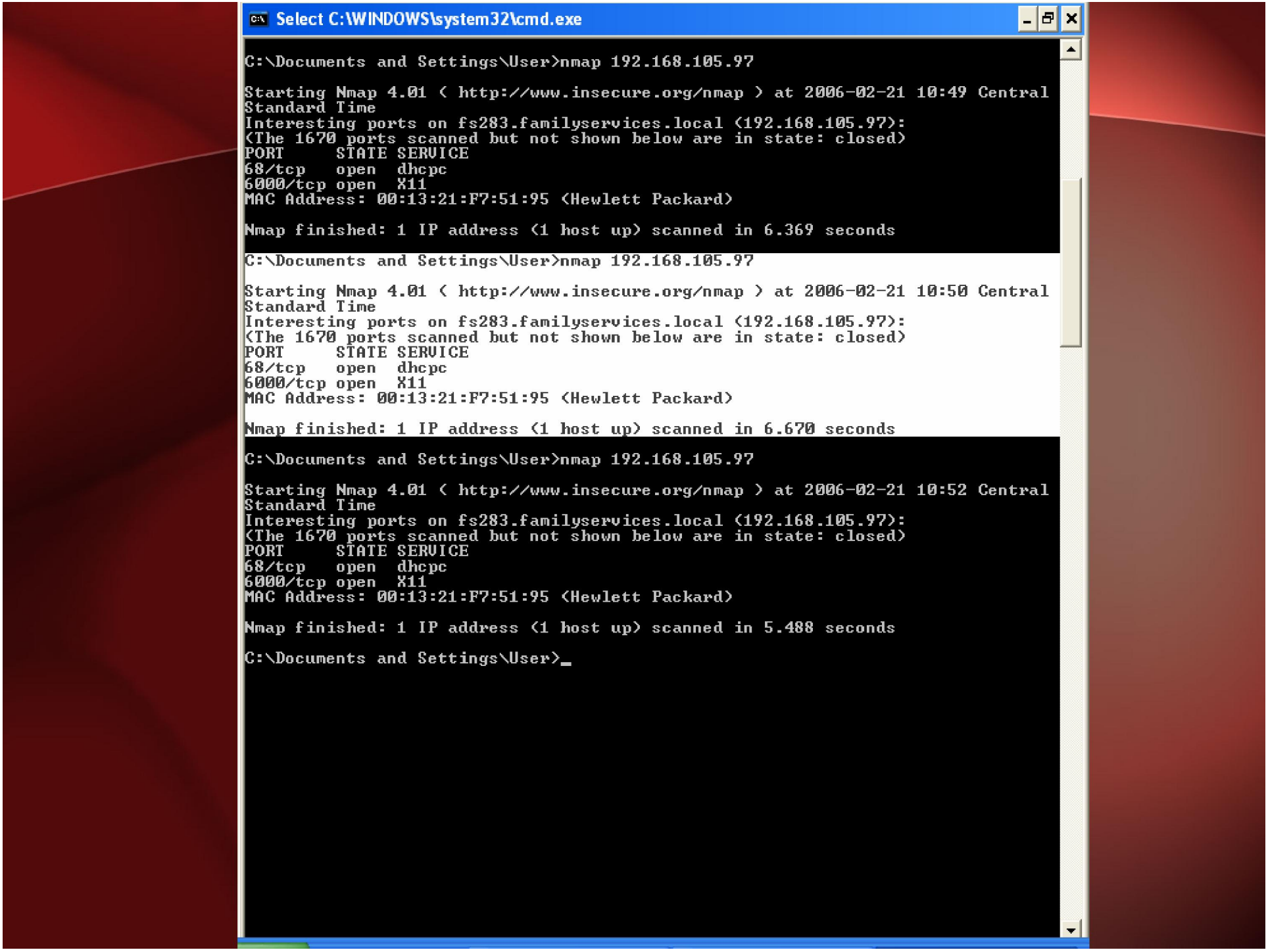
Ethereal can be run to analyze the traffic. Basically Ethereal is a network protocol analyzer, or "sniffer" for Unix and Windows, that lets you capture and interactively browse the contents of network frames.

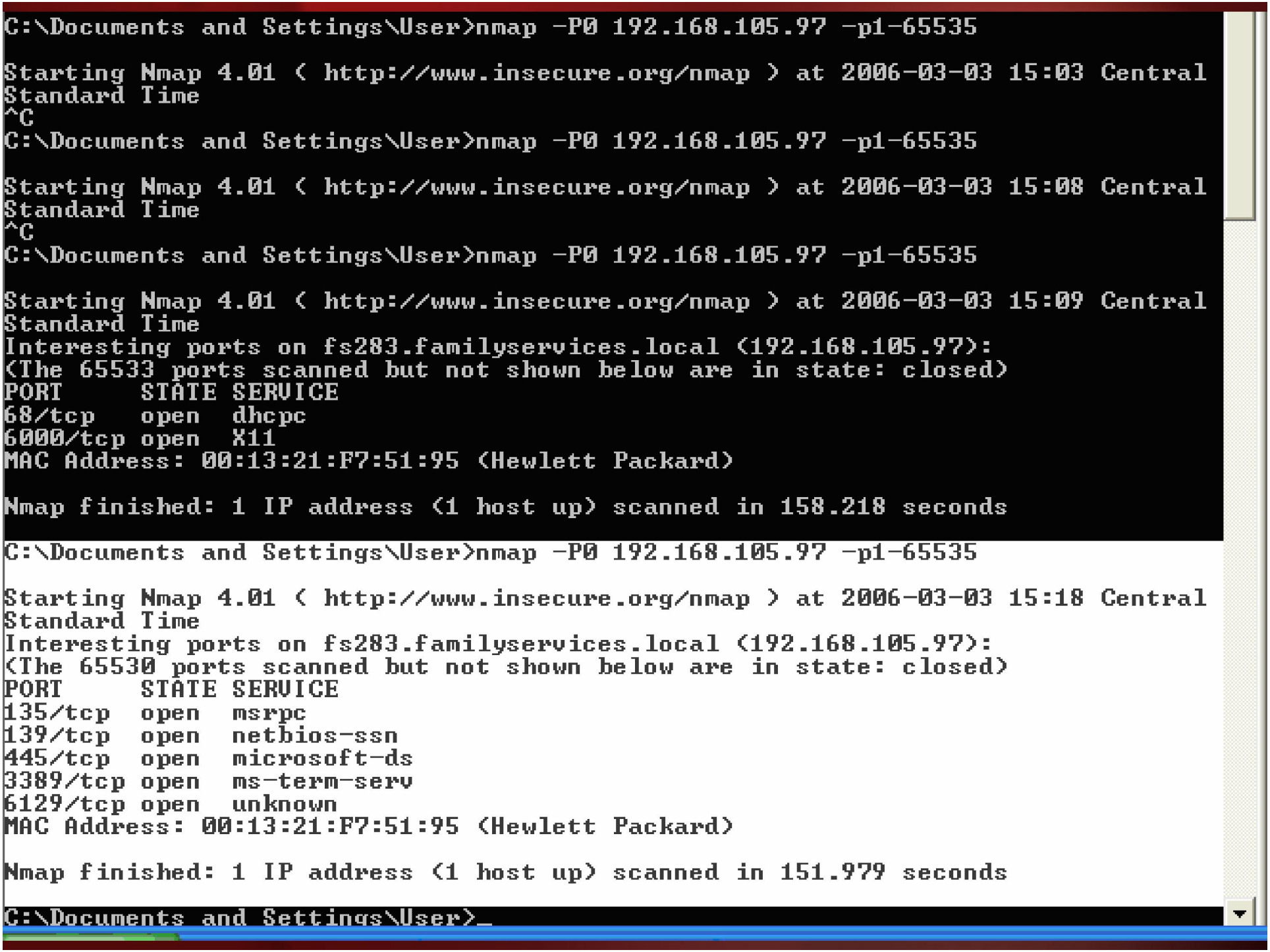
Nmap

- Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing.
- It was designed to rapidly scan large networks, although it works fine against single hosts.
- Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.
- Nmap runs on most types of computers and both console and graphical versions are available.


le Capture View Help
Pause
Stop
Pref.
Prot.
cocols
DOMAIN
SNMP-TRAP
SMB
WNN6
NEXTSTEP
AMESERVER
FS3-ERRORS
POP3
IMSP
NDTP
ZSERV
LDAP
FTP
RTSP
WWW
SMTP
CP-Unknowr
AUTH
TELNET
SSH
LDAPS
TCP
HTTPS
KRB_PROP
RBEROS-AD
TPROXY
AFS3-VOLSER
KNETD
X11-4
SAFT
VENUS-SE
X11-1
FTP-DATA
HMMP-IND
MTP
X11-7
SHELL
GOPHER
OIRA_UPDAT
X11-3
PWDGEN
cdc.familyservices.local
192.168.105.149
FS
fs283.familyservices.local
LDC
MARYAM-CSX
FS152
FS056
FS254
ling data from eth0 in IP mode


Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.105.70 192.168.105.97 TCP 44454 > 882 [SYN] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
2 0.000018 192.168.105.97 192.168.105.70 TCP 882 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
3 0.001948 192.168.105.70 192.168.105.97 TCP 44454 > 5802 [SYN] Seq=0 Ack=0 Win=4096 Len=0 MSS=1460
4 0.001963 192.168.105.97 192.168.105.70 TCP 5802 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
5 0.005278 192.168.105.70 192.168.105.97 TCP 44454 > irc [SYN] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
6 0.005295 192.168.105.97 192.168.105.70 TCP irc > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
7 0.006733 192.168.105.70 192.168.105.97 TCP 44454 > 516 [SYN] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
8 0.006747 192.168.105.97 192.168.105.70 TCP 516 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
9 0.008934 192.168.105.70 192.168.105.97 TCP 44454 > 591 [SYN] Seq=0 Ack=0 Win=4096 Len=0 MSS=1460
10 0.008952 192.168.105.97 192.168.105.70 TCP 591 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
11 0.012451 192.168.105.70 192.168.105.97 TCP 44454 > 770 [SYN] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
12 0.012482 192.168.105.97 192.168.105.70 TCP 770 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
13 0.014024 192.168.105.70 192.168.105.97 TCP 44454 > 100 [SYN] Seq=0 Ack=0 Win=1024 Len=0 MSS=1460
14 0.014041 192.168.105.97 192.168.105.70 TCP 100 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
15 0.019192 192.168.105.70 192.168.105.97 TCP 44454 > 796 [SYN] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
16 0.019213 192.168.105.97 192.168.105.70 TCP 796 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
17 0.020663 192.168.105.70 192.168.105.97 TCP 44454 > 988 [SYN] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
18 0.020679 192.168.105.97 192.168.105.70 TCP 988 > 44454 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
rame 1 (60 bytes on wire, 60 bytes captured)
thernet II, Src: 00:0d:02:58:58:68, Dst: 00:13:21:f7:51:95
nternet Protocol, Src Addr: 192.168.105.70 (192.168.105.70), Dst Addr: 192.168.105.97 (192.168.105.97)
ransmission Control Protocol, Src Port: 44454 (44454), Dst Port: 882 (882), Seq: 0, Ack: 0, Len: 0
00 13 21 f7 51 95 00 0d 02 58 58 68 08 00 45 00 ..!.Q... .XXh..E.
00 2c e9 0c 00 00 32 06 4b c7 c0 a8 69 46 c0 a8 .,....2. K...iF..
69 61 ad a6 03 72 1b f2 69 39 00 00 00 00 60 02 ia...r.. i9....`.
0c 00 01 ea 00 00 02 04 05 b4 00 00 ....
(Untitled) 233 KB 00:00:04
P: 3275 D: 3275 M: 0 Drops: 0


Select C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\User>nmap 192.168.105.97
Starting Nmap 4.01 (http://www.insecure.org/nmap) at 2006-02-21 10:49 Central Standard Time
Interesting ports on fs283.familyservices.local (192.168.105.97):
(The 1670 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
68/tcp open dhcpc
6000/tcp open X11
MAC Address: 00:13:21:F7:51:95 (Hewlett Packard)
Nmap finished: 1 IP address (1 host up) scanned in 6.369 seconds
C:\Documents and Settings\User>nmap 192.168.105.97
Starting Nmap 4.01 (http://www.insecure.org/nmap) at 2006-02-21 10:50 Central Standard Time
Interesting ports on fs283.familyservices.local (192.168.105.97):
(The 1670 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
68/tcp open dhcpc
6000/tcp open X11
MAC Address: 00:13:21:F7:51:95 (Hewlett Packard)
Nmap finished: 1 IP address (1 host up) scanned in 6.670 seconds
C:\Documents and Settings\User>nmap 192.168.105.97
Starting Nmap 4.01 (http://www.insecure.org/nmap) at 2006-02-21 10:52 Central Standard Time
Interesting ports on fs283.familyservices.local (192.168.105.97):
(The 1670 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
68/tcp open dhcpc
6000/tcp open X11
MAC Address: 00:13:21:F7:51:95 (Hewlett Packard)
Nmap finished: 1 IP address (1 host up) scanned in 5.488 seconds
C:\Documents and Settings\User>


C:\Documents and Settings\User>nmap -P0 192.168.105.97 -p1-65535
Starting Nmap 4.01 (http://www.insecure.org/nmap) at 2006-03-03 15:03 Central Standard Time
^C
C:\Documents and Settings\User>nmap -P0 192.168.105.97 -p1-65535
Starting Nmap 4.01 (http://www.insecure.org/nmap) at 2006-03-03 15:08 Central Standard Time
^C
C:\Documents and Settings\User>nmap -P0 192.168.105.97 -p1-65535
Starting Nmap 4.01 (http://www.insecure.org/nmap) at 2006-03-03 15:09 Central Standard Time
Interesting ports on fs283.familyservices.local (192.168.105.97):
(The 65533 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
68/tcp open dhcpc
6000/tcp open X11
MAC Address: 00:13:21:F7:51:95 (Hewlett Packard)
Nmap finished: 1 IP address (1 host up) scanned in 158.218 seconds
C:\Documents and Settings\User>nmap -P0 192.168.105.97 -p1-65535
Starting Nmap 4.01 (http://www.insecure.org/nmap) at 2006-03-03 15:18 Central Standard Time
Interesting ports on fs283.familyservices.local (192.168.105.97):
(The 65530 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-term-serv
6129/tcp open unknown
MAC Address: 00:13:21:F7:51:95 (Hewlett Packard)
Nmap finished: 1 IP address (1 host up) scanned in 151.979 seconds
C:\Documents and Settings\User>_

Conclusion

- Using Auditor, are able to quickly start up EtherApe to start monitoring network traffic on our LAN, use Dsniff to scan for passwords sent over the network, and run Nessus to scan for vulnerabilities.
- In addition to scanning and penetration testing, Auditor would come in handy for forensics on compromised computers with tools like Wipe, Sleuthkit, recover and testdisk. Auditor also includes productivity tools, which will come in handy for admins and security consultants to produce full reports on the same machine they use for scanning and penetration testing.
- It is the “Swiss army knife of security tools”

http://www.irongeek.com/i.php?page=security/auditornotes