Auditing Networks and Perimeters

Prepared and Presented By:

Tanya Baccam, CPA, CISA, CISM, GCFW, GCIH, CISSP, CCNA, CCSE, Oracle DBA

Baccam Consulting

tanya@baccam.com

www.baccam.com

Agenda

- Overview of the auditor's role
- Strategy for Network Audits
- Stimulus-Response Testing
- Examples of key tools and techniques used to conduct stimulus-response testing

Auditor's Role

- Aligns the IT strategy with the enterprise strategy
- Assist with managing the risks in the ongoing development and operation of IT systems

Why perform Network Audits?

- Prevention is the best medicine!
- Part of a ‘Defense in Depth’ strategy
- Identify potential intrusion
- Identify extent of a compromise
- Answer the question: How do you know?

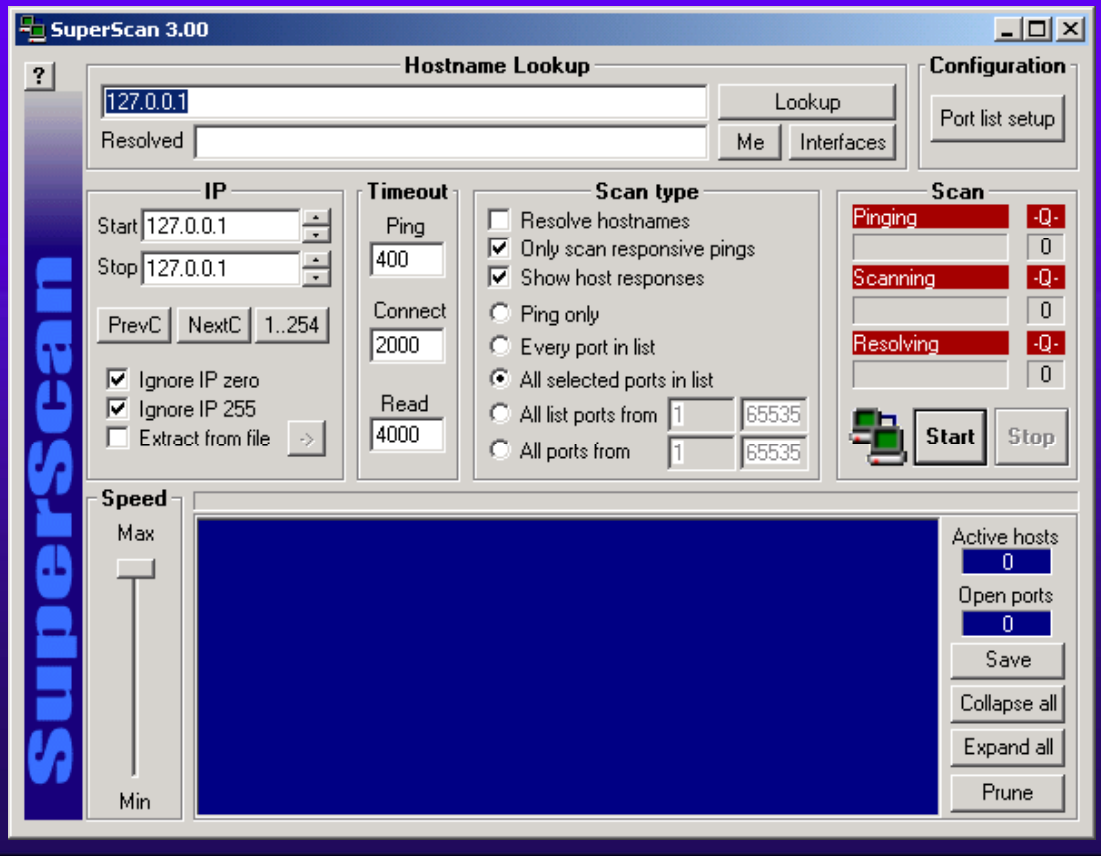
Strategy

- **Identify Devices**
- Understand Vulnerabilities and Risks
- Assess and Secure the Perimeter
- Assess and Secure the DMZ
- Assess and Secure the Internal Environment

Use
Stimulus-Response
Testing

Superscan

- Ping hosts
- Port Scan hosts



Fingerprinting Devices

- Active
  - Queries the machine for information
- Passive
  - Sniffs passing traffic for information

Active Fingerprinting

- Send a packet and look at the response.
  - Change the flags for the packet
  - ISN numbers
  - Initial windows size
  - Handling of ICMP messages
  - TOS field
  - TCP options
  - How fragmentation is handled
- Paper
  - www.insecure.org/nmap/nmap-fingerprinting-article.html

Passive Fingerprinting

- Passively watch for information during communication
  - TTL
  - Window Size
  - Don’t fragment bit
  - TOS

Critical Devices

- Make sure you know where the critical devices are

Strategy

- Identify Devices
- **Understand Vulnerabilities and Risks**
- Assess and Secure the Perimeter
- Assess and Secure the DMZ
- Assess and Secure the Internal Environment

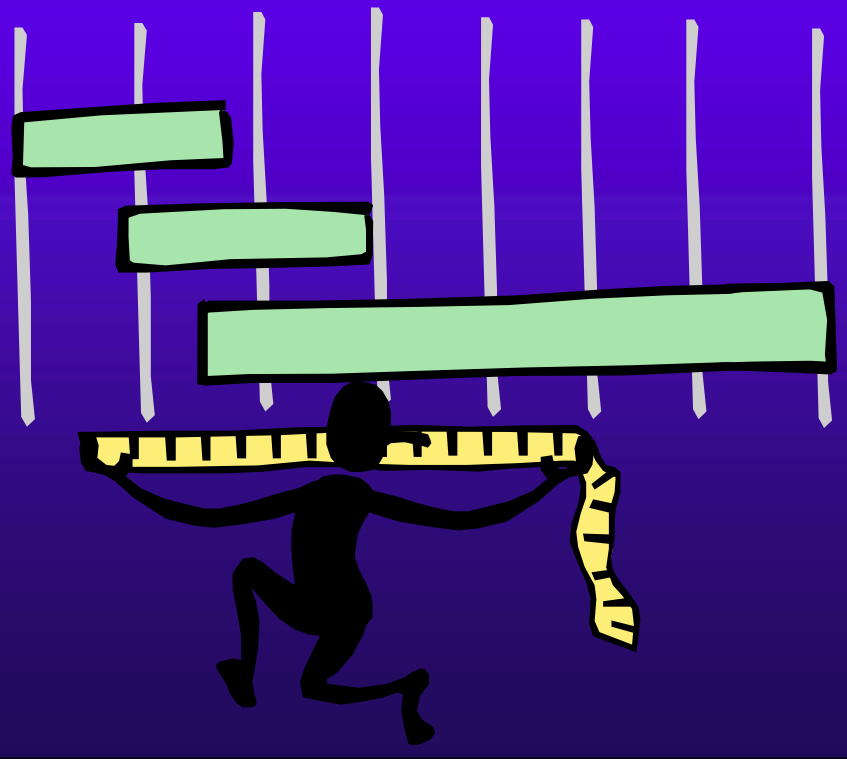
Research is essential!

- www.google.com
- Vendor web sites
- www.securityfocus.com

Think like an attacker…

Prioritize

- Based on your research, what vulnerabilities are the highest risk to your environment?



Strategy

- Identify Devices
- Understand Vulnerabilities and Risks
- **Assess and Secure the Perimeter**
- Assess and Secure the DMZ
- Assess and Secure the Internal Environment

Scanning

- ICMP
- SYN
- TCP Stealth
- Fragment
- UDP

Nmap

- Sample Options
  - -sS: SYN scan
  - -sT: TCP connect scan
  - -sF: FIN scan
  - -sX: Xmas tree scan
  - -sN: Null scan
  - -sP: ping scan
  - -sU: UDP scan
  - -sA: ACK scan
  - -sR: RPC scan

Nmap fragment scan

- nmap –f : tiny-fragment scan

```
17:02:59.418110 10.10.10.10 > 10.10.10.102: icmp: echo request
17:02:59.418110 10.10.10.10.45994 > 10.10.10.102.http: . ack 269371834 win 4096
17:02:59.418110 10.10.10.102 > 10.10.10.10: icmp: echo reply
17:02:59.418110 10.10.10.102.http > 10.10.10.10.45994: R 269371834:269371834(0) win 0
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.2307: [|tcp] (frag 49783:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 49783:4@16)
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.6003: [|tcp] (frag 51187:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 51187:4@16)
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.275: [|tcp] (frag 9593:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 9593:4@16)
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.678: [|tcp] (frag 25130:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 25130:4@16)
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.344: [|tcp] (frag 33396:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 33396:4@16)
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.478: [|tcp] (frag 61393:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 61393:4@16)
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.1001: [|tcp] (frag 49516:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 49516:4@16)
17:02:59.718110 10.10.10.102.2307 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.884: [|tcp] (frag 28697:16@0+)
17:02:59.718110 10.10.10.10 > 10.10.10.102: (frag 28697:4@16)
17:02:59.718110 10.10.10.10.45974 > 10.10.10.102.47557: [|tcp] (frag 23275:16@0+)
17:02:59.728110 10.10.10.10 > 10.10.10.102: (frag 23275:4@16)
17:02:59.728110 10.10.10.10.45974 > 10.10.10.102.6145: [|tcp] (frag 62912:16@0+)
17:02:59.728110 10.10.10.10 > 10.10.10.102: (frag 62912:4@16)
17:02:59.728110 10.10.10.102.6003 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.275 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.678 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.344 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.478 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.1001 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.884 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.47557 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
17:02:59.728110 10.10.10.102.6145 > 10.10.10.10.45974: R 0:0(0) ack 1402132342 win 0
```

Scan for Services

- nmap –v –g53 –sS –P0 –O –p 1-65535 –o firewall.out ip_address
  - –v: verbose mode, nmap returns additional information
  - –g53: sets the source port number utilized for the scans
  - –sS: conducts a SYN scan
  - –P0: do not conduct pings before scanning
  - –p 1-65535: ports to be scanned
  - –o firewall.out: output file to send the results to
  - ip_address: the IP address to be scanned

Hping2 Options (1)

- The following are the more commonly utilized hping options:
  - -h: help
  - -c: the number (count) of packets to send
  - -n: numeric output only, no resolution for host names
  - -V: verbose output
  - -D: debug
  - -a: alternative source IP address
  - -k: keep constant

Hping2 Options (2)

- -f: split the packet into fragments
- -y: set the don't fragment IP flag (You can perform MTU path discovery with this option.)
- -o: set the Type of Service (TOS)
- -d: sets the data size of the packet
- -E *filename*: use the *filename* file to complete the data in the packet
- -j or J: dumps the received packet in hex or printable characters, respectively

Hping2

File Edit Settings Help

```
[root@localhost hping2]# ./hping2 -c 2 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 flags=RA DF seq=0 ttl=255 id=0 win=0 rtt=0.3 ms
len=40 ip=127.0.0.1 flags=RA DF seq=1 ttl=255 id=0 win=0 rtt=0.3 ms

--- 127.0.0.1 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.3 ms
[root@localhost hping2]# hping -c 2 -j 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 flags=RA DF seq=0 ttl=255 id=0 win=0 rtt=0.3 ms
                0000 0000 0000 0000 0000 0000 0800 4500
                0028 0000 4000 ff06 7dcd 7f00 0001 7f00
                0001 0000 08fd 0000 0000 49eb 4484 5014
                0000 1a62 0000

len=40 ip=127.0.0.1 flags=RA DF seq=1 ttl=255 id=0 win=0 rtt=0.2 ms
                0000 0000 0000 0000 0000 0000 0800 4500
                0028 0000 4000 ff06 7dcd 7f00 0001 7f00
                0001 0000 08fe 0000 0000 4ed6 e449 5014
                0000 75b0 0000


--- 127.0.0.1 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.3 ms
[root@localhost hping2]#
```

Fragmentation with Hping

- Fragmentation testing
  - hping2 –V –I eth0 --data 40 --count 3 --syn –p 22 ip_address
  - hping2 –V --frag –I eth0 --data 40 --count 3 --syn –p 22 ip_address
    - –V: verbose mode
    - –I eth0: interface name
    - --data 40: data size
    - --count 3: packet count
    - --syn: sets the SYN flag
    - –p 22: sets the destination port
    - ip_address: sets the destination address
    - --frag: split packets in more fragments

Tcpdump/Windump

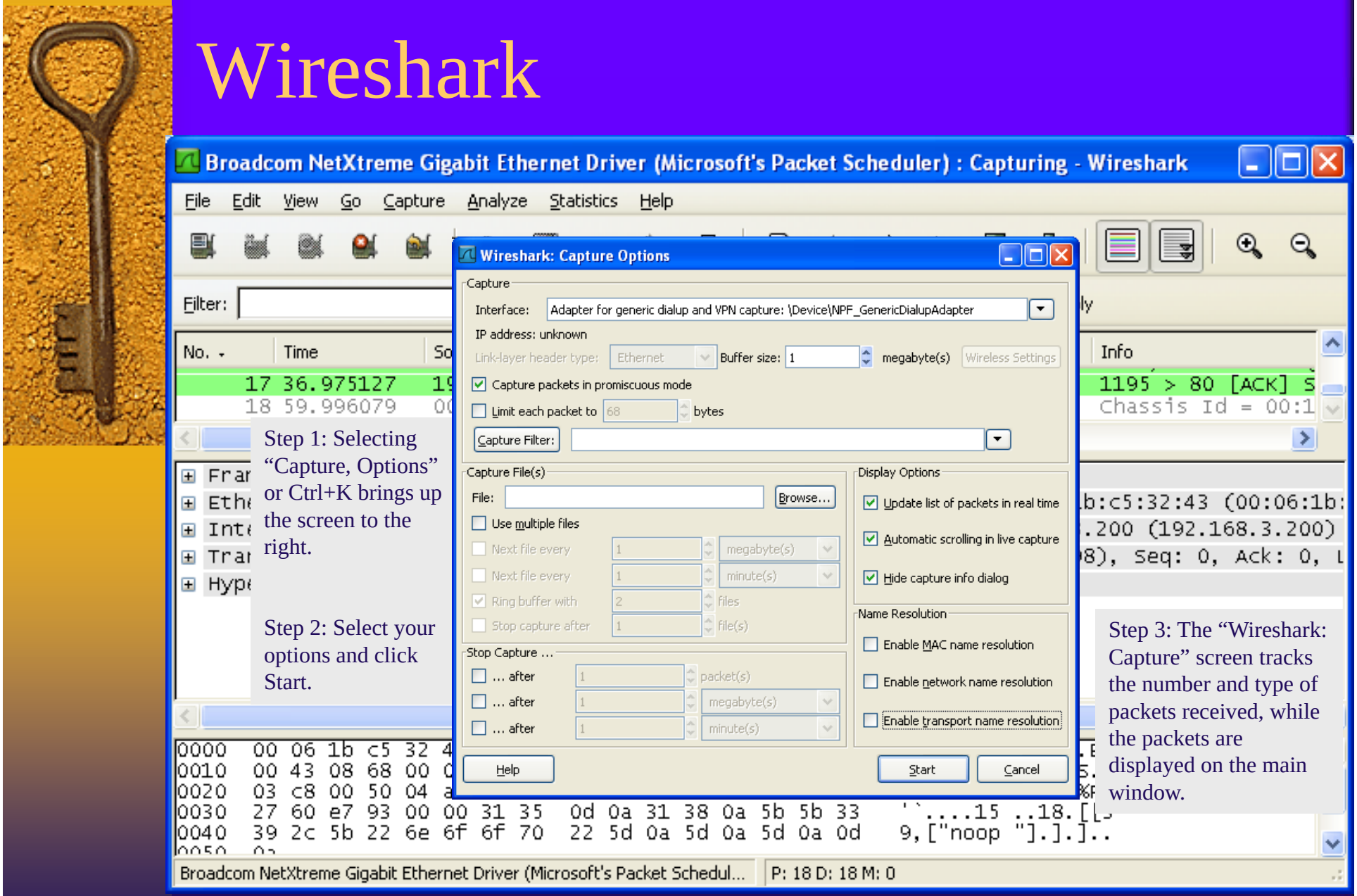
- Capture data from the wire

```
22:55:09.908986 10.10.10.4.4125 > 10.10.10.1.ssh: S 1959695011:1959695011(0) win 5840 <mss
        1460,sackOK,timestamp 229493[|tcp]> (DF)
22:55:09.908986 10.10.10.1.ssh > 10.10.10.4.4125: S 2896899209:2896899209(0) ack 1959695012 win 5792 <mss
        1460,sackOK,timestamp 2245851[|tcp]> (DF)
22:55:09.908986 10.10.10.4.4125 > 10.10.10.1.ssh: . ack 1 win 5840 <nop,nop,timestamp 229493 2245851> (DF)
22:55:09.918986 10.10.10.1.ssh > 10.10.10.4.4125: P 1:26(25) ack 1 win 5792 <nop,nop,timestamp 2245852
        229493> (DF)
22:55:09.918986 10.10.10.4.4125 > 10.10.10.1.ssh: . ack 26 win 5840 <nop,nop,timestamp 229494 2245852> (DF)
22:55:09.918986 10.10.10.4.4125 > 10.10.10.1.ssh: P 1:25(24) ack 26 win 5840 <nop,nop,timestamp 229494
        2245852> (DF)
22:55:09.918986 10.10.10.1.ssh > 10.10.10.4.4125: . ack 25 win 5792 <nop,nop,timestamp 2245852 229494> (DF)
```

TCPDump's Role

- Keep a sniffer on the wire to verify the 'real' results
  - tcpdump –i eth0 –n –vvv –w output.txt
    - Listen on interface eth0
    - Do not convert addresses to names
    - Print in very, very verbose mode
    - Save the output to output.txt
  - tcpdump –r output.txt
    - Read the file created

Wireshark



Step 1: Selecting "Capture, Options" or Ctrl+K brings up the screen to the right.

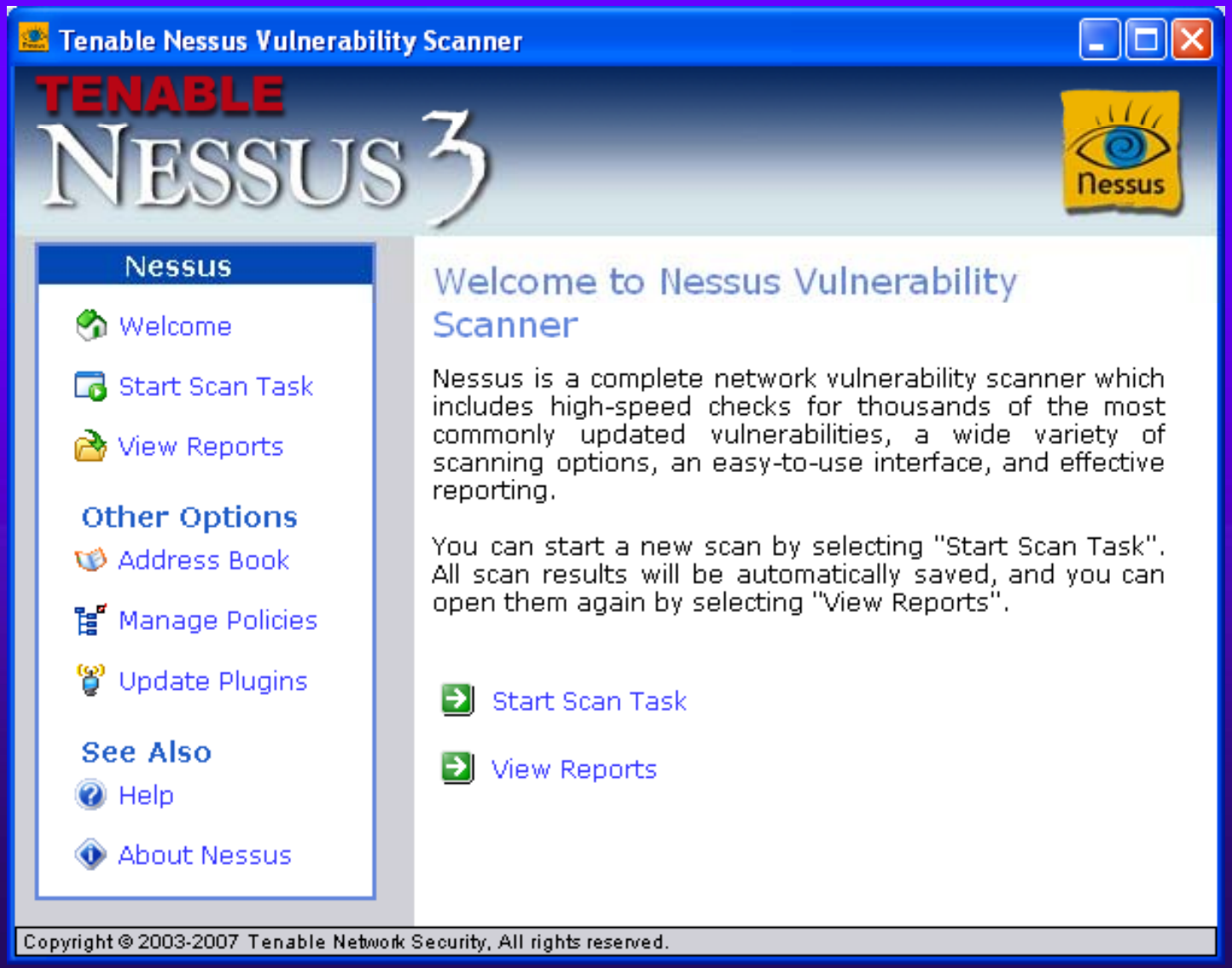
Step 2: Select your options and click Start.

Step 3: The "Wireshark: Capture" screen tracks the number and type of packets received, while the packets are displayed on the main window.

Strategy

- Identify Devices
- Understand Vulnerabilities and Risks
- Assess and Secure the Perimeter
- **Assess and Secure the DMZ**
- Assess and Secure the Internal Environment

Vulnerability Assessments



N-Stalker and Nikto

Strategy

- Identify Devices
- Understand Vulnerabilities and Risks
- Assess and Secure the Perimeter
- Assess and Secure the DMZ
- **Assess and Secure the Internal Environment**

NDiff

- Options available

```
# ndiff
  ndiff     [-b|-baseline <file-or-:tag>]   [-o|-observed <file-or-:tag>]
            [-op|-output-ports <ocufx>]   [-of|-output-hosts <nmc>]
            [-fmt|-format <terse | minimal | verbose | machine | html | htmle>]
```

Open
Closed
Filtered
Unfiltered
Unknown

New hosts
Missing hosts
Changed hosts

- http://www.vinecorp.com/ndiff/

Ndiff Output

Netscape 6

File Edit View Search Go Bookmarks Tasks Help

New Hosts
Missing Hosts
Changed Hosts

New Hosts

[previously un-observed hosts found in the more rec
-- all interesting ports shown]

172.16.222.1			
Port	Protocol	Service Name	State
139	tcp	netbios-ssn	open
6000	tcp	X11	open

back to top

Missing Hosts

[previously observed hosts missing from the more re
-- no original ports shown]

Document: Done (0.931 secs)

Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Missing Hosts

[previously observed hosts missing from the more recent scan
-- no original ports shown]

172.16.222.2			
Port	Protocol	Service Name	State
139	tcp	netbios-ssn	open
6000	tcp	X11	open

back to top

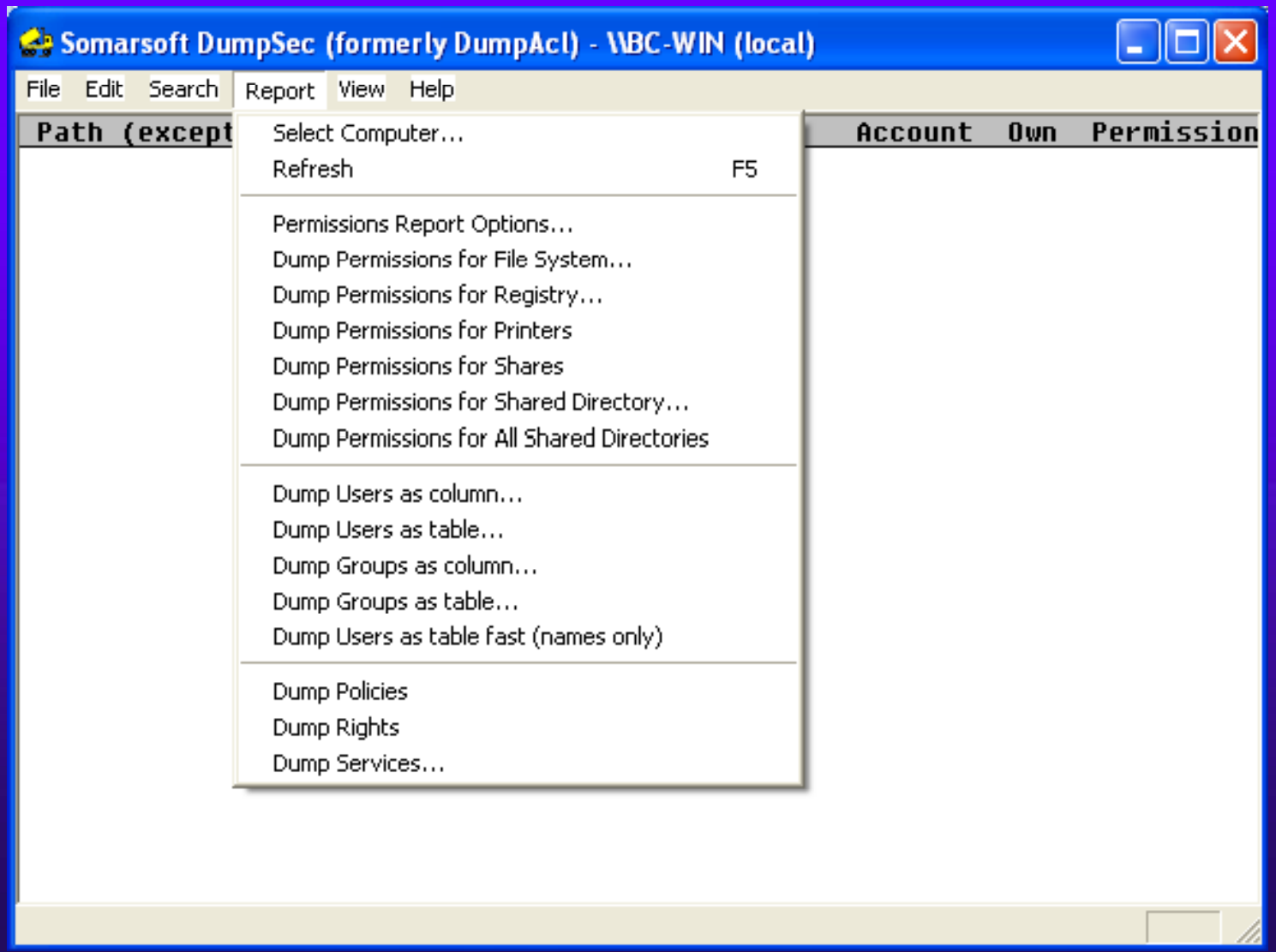
Changed Hosts

[hosts which have changed since the original scan
-- interesting changed ports shown]

172.16.222.128				
Port	Protocol	Service Name	Original State	Observed State
21	tcp	ftp	unknown	open
172.16.222.136				
Port	Protocol	Service Name	Original State	Observed State
80	tcp	http	unknown	open

Document: Done (0.931 secs)

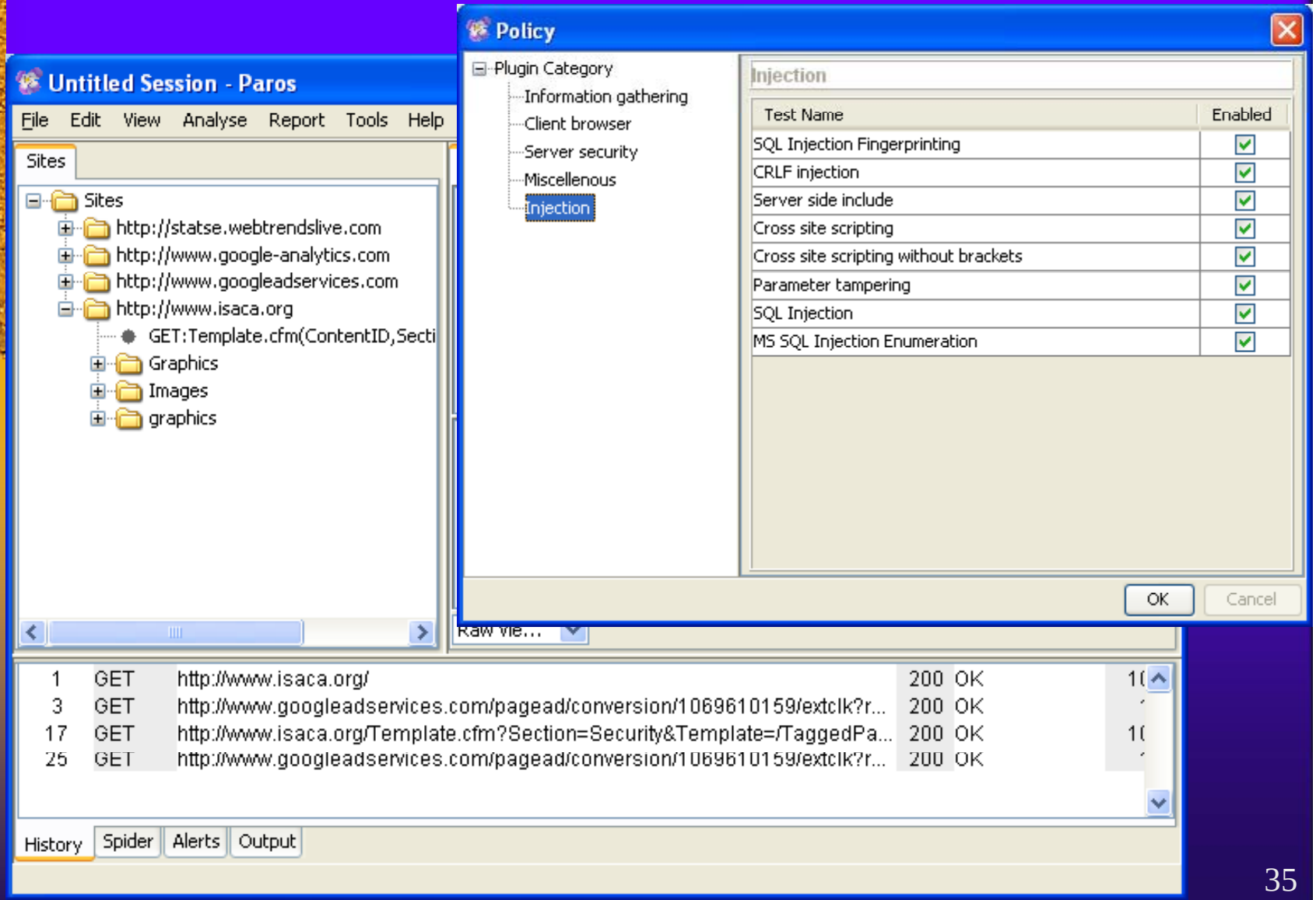
Dumpsec


Somarsoft DumpSec (formerly DumpAcl) - \\BC-WIN (local)
File
Edit
Search
Report
View
Help
Path (except
Account
Own
Permission
Select Computer...
Refresh
F5
Permissions Report Options...
Dump Permissions for File System...
Dump Permissions for Registry...
Dump Permissions for Printers
Dump Permissions for Shares
Dump Permissions for Shared Directory...
Dump Permissions for All Shared Directories
Dump Users as column...
Dump Users as table...
Dump Groups as column...
Dump Groups as table...
Dump Users as table fast (names only)
Dump Policies
Dump Rights
Dump Services...

Web Applications

- Many proxy based tools exist
  - Paros – Default port 8080
  - WebScarab – Default port 8008
- Scan for “customized” application vulnerabilities
- Specialize tests based on the developed application

Paros


Untitled Session - Paros
File Edit View Analyse Report Tools Help
Sites
Sites
http://statse.webtrendslive.com
http://www.google-analytics.com
http://www.googleadservices.com
http://www.isaca.org
GET:Template.cfm(ContentID,Secti
Graphics
Images
graphics
Policy
Plugin Category
Information gathering
Client browser
Server security
Miscellenous
Injection
Injection
Test Name
Enabled
SQL Injection Fingerprinting
CRLF injection
Server side include
Cross site scripting
Cross site scripting without brackets
Parameter tampering
SQL Injection
MS SQL Injection Enumeration
OK
Cancel
1 GET http://www.isaca.org/ 200 OK
3 GET http://www.googleadservices.com/pagead/conversion/1069610159/extclk?r... 200 OK
17 GET http://www.isaca.org/Template.cfm?Section=Security&Template=/TaggedPa... 200 OK
25 GET http://www.googleadservices.com/pagead/conversion/1069610159/extclk?r... 200 OK
History
Spider
Alerts
Output

WebScarab

WebScarab

File View Tools Help

XSS/CRLF | SessionID Analysis | Scripted | Fragments | Fuzzer | Compare | Search

Summary | Messages | Proxy | Manual Request | WebServices | Spider | Extensions

Tree Selection filters conversation list

Url	Methods	Status	Possible Inj...	Injection	Set-Cookie	Comments	Scripts
http://statse.webtrendslive.cor							
http://www.google-analytics.c(							
http://www.googleadservices.							
http://www.isaca.org:80/							

ID	Date	Method	Host	Path	Parameters	Status	Origin	Poss
6	2007/10/17...	GET	http://www.isaca.org:80	/Graphics/Home_template/i...		200 OK	Proxy	
5	2007/10/17...	GET	http://statse.webtrendsliv...	/dcsrullw300000kvp4se9uv...	?&dcsdat=1192...	200 OK	Proxy	
4	2007/10/17...	GET	http://statse.webtrendsliv...	/dcsrullw300000kvp4se9uv...	?&dcsdat=1192...	200 OK	Proxy	
3	2007/10/17...	GET	http://www.google-analyti...	/__utm.gif	?utmwv=1&utm...	200 OK	Proxy	
2	2007/10/17...	GET	http://www.googleadservi...	/pagead/conversion/106961...	?random=1192...	200 OK	Proxy	
1	2007/10/17...	GET	http://www.isaca.org:80	/Template.cfm	?Section=Secur...	200 OK	Proxy	

Used 4.85 of 63.56MB

Summary

- Overview of the auditor's role
- Strategy for Network Audits
- Stimulus-Response Testing
- Examples of key tools and techniques used to conduct stimulus-response testing

Conclusion

- Quality Network Audits are hard to do well, but it is possible with the right strategies and tools!

More Information and Resources

- SANS Audit 507
  - http://www.sans.org/athome/
  - https://www.sans.org/registration/register.php?conferenceid=7191
- www.tcpdump.org
- www.wireshark.org
- www.insecure.org/nmap/download.html
- www.nessus.org
- www.insecure.org/nmap/nmap-fingerprinting-article.html
- www.nstalker.com
- www.cirt.net/code/nikto.shtml
- www.vinecorp.com/ndiff/
- www.systemtools.com/download/dumpacl.zip
- www.owasp.org
- www.parosproxy.org/index.shtml