

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

👆 Su	perScan 3.00		
?		Hostname Lookup	Configuration
	127.0.0.1	Lookup	Port list setup
	Resolved	Me Interfaces	
rScan	IP Start 127.0.0.1 Stop 127.0.0.1 PrevC NextC 1254 ✓ Ignore IP zero ✓ Ignore IP 255 Extract from file	Scan type Ping Resolve hostnames 400 Image: Show host responsive pings 400 Image: Show host responsive pings Connect Ping only 2000 Image: Every port in list Read All selected ports in list 4000 All ports from 1 65535	Scan ing Q- 0 nning Q- 0 olving Q- 0 0 0 0 0 0 0 0 0 0 0 0 0
Supe	Max T Min		Active hosts Open ports Save Collapse all Expand all Prune

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-fingerprintingarticle.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

Sased 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: [ltcp] (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: [ltcp] (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: [ltcp] (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 > 10.10.10.45974: 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: [ltcp] (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 > 10.10.10.10.26145: [ltcp] (frag 62912:16@0+) $17:02:59.728110 \ 10.10.10.10 > 10.10.102:$ (frag 62912:4@16) 17:02:59.728110 10.10.10.102.6003 > 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 > 10.10.10.45974: R 0:0(0) ack 1402132342 win 0 17:02:59.728110 10.10.10.102.884 > 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: . 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

📶 Broadcom NetXtreme Gig	abit Ethernet Driver (Microsoft's Packet Scheduler) : Capturing - Wireshark 👘 🔳 🗖 🔯
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp
	Wireshark: Capture Options
Eilter:	Capture Interface: Adapter for generic dialup and VPN capture: \Device\NPF_GenericDialupAdapter
No Time So	Link-layer header type: Ethernet V Buffer size: 1 m megabyte(s) Wireless Settings
17 36.975127 1 18 59.996079 0 Step 1: Selecting	✓ Capture packets in promiscuous mode 1195 > 80 [ACK] S □ Limit each packet to 68 bytes Capture Filter: ▼
 ➡ Frar "Capture, Options" ➡ Ethe or Ctrl+K brings up 	Capture File(s) File: Browse Display Options Update list of packets in real time .b:<5:32:43 (00:06:1b)
Int; the screen to the Int; the screen to the Trai right. Hyp;	Use multiple files .200 (192.168.3.200) Next file every 1 megabyte(s) Next file every 1 minute(s) Hide capture info dialog .200 (192.168.3.200)
Step 2: Select your options and click	Ring buffer with 2 files Stop capture after 1 file(s) Name Resolution Enable MAC name resolution Step 3: The "Wireshark: Capture" screen tracks after 1 packet(s) Enable network name resolution The number and type of
	Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s) Image: megabyte(s)<
0000 00 06 1b c5 32 4 0010 00 43 08 68 00 0 0020 03 c8 00 50 04 3 0030 27 60 e7 93 00 0	Help Start Gancel It places are Start Gancel S. displayed on the main %F window. %F window. %F
0040 39 2c 5b 22 6e 6	5f 6f 70 22 5d 0a 5d 0a 5d 0a 0d 9,["noop "].].]
Broadcom NetXtreme Gigabit Etherr	net Driver (Microsoft's Packet Schedul P: 18 D: 18 M: 0

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

🚨 Tenable Nessus Vulnerability Scanner

ESSUS²

_ 🗆 🛛



Nessus



Welcome to Nessus Vulnerability Scanner

Nessus is a complete network vulnerability scanner which includes high-speed checks for thousands of the most commonly updated vulnerabilities, a wide variety of scanning options, an easy-to-use interface, and effective reporting.

You can start a new scan by selecting "Start Scan Task". All scan results will be automatically saved, and you can open them again by selecting "View Reports".

🛃 🛛 Start Scan Task

🔁 View Reports

Copyright © 2003-2007 Tenable Network Security, All rights reserved.



ŝ	N-Stalker Web Application	Security Scanner 2006 - Free Edition (plus XSS Scanner)		
1112	Eile Options Tools About				
	Scan <u>W</u> izard <u>P</u> olicies - Profile	- Current Profile Default Config			
2	Web Security Audit Policies	Choose a Scan Policy			
STATES CON	Default Policies Default Policies Default Policies Default Policies Custom Policies				
	N	Stalker SECURITY SPECIALISTS	\boxtimes		
2012220	Developm Stage 1 of include C	nent / QA of SDLC - These are the policy templates for Devel ross-Site scripting and SQL Injection, Buffer Overl	lopment and QA Security analysis. These rules flow test cases, Parameter Tampering rules.		
	2 Infrast Stage 2 (deploying signature	Free Cross-Site Scr of SDLC - These are the policy templates for Deplo g web applications in production level. These rules to check for vulnerabilities in web servers and 3	ipting (XSS) Scanner included wment and Infrastructure. To be used while include the most complete database of attack rd-party packages (The N-Stealth Database).		
	Audit /	Command Prompt			- 🗆 🗙
	Stage 3 of most con Tamperin	D:\Tools\nikto\nikto-1.36> -***** SSL support not ava	perl nikto.pl ilable (see docs for SSL ins	tall instructions) ***	•**
		- Nikto 1.36/1.37 - + ERROR: No host specified	www.cirt.net		
	J_ Do not show	Options: Cgidirs+	Scan these CGI dirs: 'none	', 'all', or a value]	like
	Status: Ready	'/cgi/' -cookies -evasion+ -findonly	print cookies found ids evasion technique find http(s) ports onl	(1-9, see below) y, don't perform a ful	ll sc
		-Format	save file (-o) Format:	htm, csv or txt (assu	umed)
		-generic	force full (generic) s	can	-

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





Dumpsec

👍 Somarsoft Du	mpSec (formerly DumpAcl)	- \\BC-WIN (local)			
File Edit Search	Report View Help				
Path (except	Select Computer		Account	0wn	Permission
	Refresh	F5			
	Permissions Report Options				
	Dump Permissions for File Syste	m			
	Dump Permissions for Registry				
	Dump Permissions for Printers				
	Dump Permissions for Shares				
	Dump Permissions for Shared Di	rectory			
	Dump Permissions for All Shared	Directories			
	Dump Users as column				
	Dump Users as table	I			
	Dump Groups as column				
	Dump Groups as table				
	Dump Users as table fast (name	s only)			
	Dump Policies				
	Dump Rights	I			
	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





Ele 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	🕌 Wel	🛎 WebScarab									
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 Intp://statse.webtrendslive.cor Intp://www.google.analytics.cc Intp://www.googleadservices. Intp://www.isaca.org:80/ Intp://www.isaca.org:80/ ID T Date Method Host Path Parameters Status Origin Possi 6 2007/10/17 GET http://www.isaca.org:80 // /// dcsrullw/300000krp4se9uv ?&dcsdat=1192 200 OK Proxy 5 2007/10/17 GET http://www.isaca.org:80 // // dcsrullw/300000krp4se9uv ?&dcsdat=1192 200 OK Proxy 4 2007/10/17 GET http://www.isaca.org:80 // // dcsrullw/300000krp4se9uv ?&dcsdat=1192 200 OK Proxy 2 3 2007/10/17 GET http://www.isaca.org:80 // // carullw/300000krp4se9uv	<u>File View T</u> ools <u>H</u> elp										
Summary Messages Proxy Manual Request WebServices Spider Extensions Tree Selection filters conversation list Url Methods Status Possible Inj Injection Set-Cookie Comments Scripts Intp://statse.webtrendslive.cor Intp://www.google-analytics.cc Intp://www.googleadservices. Intp://www.googleadservices. Intp://www.isaca.org:80/ ID v 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 4 2007/10/17 GET http://www.isaca.org:80 /Graphics/Home_template/i 200 OK Proxy 3 2007/10/17 GET http://www.isaca.org:80 /Graphics/Home_template/i ?&dcdsdat=1192 200 OK Proxy 3 2007/10/17 GET http://www.google-analyti /_utcrulw300000k/p4se9uv ?&dcdsdat=1192 200 OK Proxy 3 2007/10/17 GET http://www.google-analyti /_utcrulw300000k/p4se9uv ?&dcdsdat=1192 200 OK </th <th>XSS/C</th> <th colspan="9">XSS/CRLF SessionID Analysis Scripted Fragments Fuzzer Compare Search</th>	XSS/C	XSS/CRLF SessionID Analysis Scripted Fragments Fuzzer Compare Search									
Tree Selection filters conversation list Url Methods Status Possible Inj Injection Set-Cookle Comments Scripts Intp://www.google-analytics.cc Intp://www.google-analytics.cc Intp://www.googleadservices. Intp://www.googleadservices. Intp://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://www.isaca.org:80 //Graphics/Home_template/i 200 OK Proxy 4 2007/10/17 GET http://www.isaca.org:80 //Gesrullw300000kry4se9uv ?&dcsdat=1192 200 OK Proxy 3 2007/10/17 GET http://www.google-analyti /_utm.gif ?utmw=1&utm 200 OK Proxy 1 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?Section=Secur 200 OK Proxy 2 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?Section=Secur	Su	nmary	Messag	jes Proxy		Manual Request	We	ebServices	Spider	Extensio	ns
Url Methods Status Possible Inj Injection Set-Cookie Comments Scripts http://www.google-analytics.cc http://www.googleadservices. http://www.isaca.org:80/ ID r Date Method Host Path Parameters Status Origin Poss Date Method Host Path Parameters Status Origin Poss Dote Method Host Path Parameters Status Origin Poss Control of thtp://www.isaca.org:80 //Graphics/Home_template/I 200 0 K Proxy 2007/10/17 GET http://statse.webtrendsliv /dcsrullw300000krp4se9uv ?&dcsdat=1192 200 0 K Proxy 2007/10/17 GET http://www.googleadservi /pagead/conversion/106961 ?andom=1192	🔲 Tre	e Selection fi	lters conve	ersation list							
ID r Date Method Host Path Parameters Status Origin Poss 6 2007/10/17 GET http://www.isaca.org:80 / 200 OK Proxy Proxy 5 2007/10/17 GET http://statse.webtrendslive./dcsrullw300000kvp4se9uv ?&dcsdat=1192 200 OK Proxy 4 2007/10/17 GET http://www.isaca.org:80 //Graphics/Home_template/i 200 OK Proxy Proxy 5 2007/10/17 GET http://statse.webtrendsliv /dcsrullw300000kvp4se9uv ?&dcsdat=1192 200 OK Proxy Proxy 4 2007/10/17 GET http://www.google.analyti /_utm.gif ?utm.w=1&utm 200 OK Proxy 2 2007/10/17 GET http://www.google.analyti /_utm.gif ?utm.w=1&utm 200 OK Proxy 1 2007/10/17 GET http://www.isaca.org.80 //Template.cfm ?section=Secur 200 OK Proxy 2 2007/10/17 GET http://www.isaca.org.80 //Template.cfm ?section=Secur 200 OK Proxy 1 2007/10/17 GET		Url		Methods	Statu	is Possible Inj	Injection	Set-Cookie	Comments	Scripts	
http://www.google-analytics.cc http://www.googleadservices. http://www.isaca.org:80/ ID T 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://www.googleadservi /dcsrullw300000kvp4se9uv ?&dcsdat=1192 200 OK Proxy 3 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 1 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?Section=Secur 200 OK Proxy 1 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?Section=Secur 200 OK Proxy <td>~⊟</td> <td>http://statse.v</td> <td>/ebtrendsliv</td> <td>100.9</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>i</td>	~⊟	http://statse.v	/ebtrendsliv	100.9							i
Inttp://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/ 200 OK Proxy 5 2007/10/17 GET http://statse.webtrendsliv /dcsrullw300000kvp4se9uv ?&dcsdat=1192 200 OK Proxy 4 2007/10/17 GET http://www.googleadservi /_utm.gif ?utmw=1&utm 200 OK Proxy 3 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	▶ 🗖	http://www.go	ogle-analyt	tics.cc							
Image: 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://www.isaca.org:80 /Graphics/Home_template/i 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 ?utmw=1&utm 200 OK Proxy 2 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?section=Secur 200 OK Proxy 1 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?section=Secur 200 OK Proxy	← 🗖	http://www.go	ogleadserv	/ices.							
ID T 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 ?utm.w=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 4 III IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	∾ 🗖	http://www.isa	aca.org:80/								
ID T 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 1 5 2007/10/17 GET http://statse.webtrendsliv /dcsrullw300000kvp4se9uv ?&dcsdat=1192 200 OK Proxy 1 4 2007/10/17 GET http://statse.webtrendsliv /dcsrullw300000kvp4se9uv ?&dcsdat=1192 200 OK Proxy 1 3 2007/10/17 GET http://www.google-analyti /utm.gif ?utmw=1&utm 200 OK Proxy 1 2 2007/10/17 GET http://www.googleadservi /pagead/conversion/106961 ?random=1192 200 OK Proxy 1 1 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?Section=Secur 200 OK Proxy 1											
ID r 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://statse.webtrendsliv /utm.gif ?utm.w=1&utm 200 OK Proxy 1 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 1 2007/10/17 GET http://www.isaca.org:80 /Template.cfm ?Section=Secur 200 OK Proxy 1 Used 4.85 of 63.56MB	A										
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 ?utmw=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	ID 🗸	Date	Method	Host		Path		Parameters	Status	Origin	Poss
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 ?utmw=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 Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur Image: Section = Secur	6	2007/10/17	GET	http://www.isaca.c	irg:80	/Graphics/Home_t	template/i		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 ?utmw=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	5	2007/10/17	GET	http://statse.webtr	endsliv	/dcsrullw300000k	/p4se9uv	?&dcsdat=1192.	200 OK	Proxy	
3 2007/10/17 GET http://www.google-analyti /_utm.gif ?utm.w=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	4	2007/10/17	GET	http://statse.webtr	endsliv	/dcsrullw300000k	/p4se9uv	?&dcsdat=1192.	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	3	2007/10/17	GET	http://www.google	-analyti	/utm.gif		?utmwv=1&utm.	. 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 ■ ■ ■ ■	2	2007/10/17	GET	http://www.google	adservi	/pagead/conversic	n/106961	?random=1192.	. 200 OK	Proxy	
Image: Constraint of the second se	1	2007/10/17	GET	http://www.isaca.c	rg:80	/Template.cfm		?Section=Secur.	200 OK	Proxy	
Used 4.85 of 63.56MB											
Used 4.85 of 63.56MB	•										•
		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