

# Security Tools for Common Criteria Testing

**Quang Trinh, SAIC**  
**11<sup>th</sup> ICCC - Antalya, Turkey**

**21 September 2010**

- Why use tools?
- Category of tools
- Common Criteria testing
  - Functional
  - Penetration
- Analysis of tools
  - Criteria
  - Recommended Tools
- Conclusions

- Why use tools during Common Criteria (CC) testing?
  - Simplify complex manual tasks
  - Reduce time and effort
  - Provide more systematic approach
  - Result in less mundane human errors\*

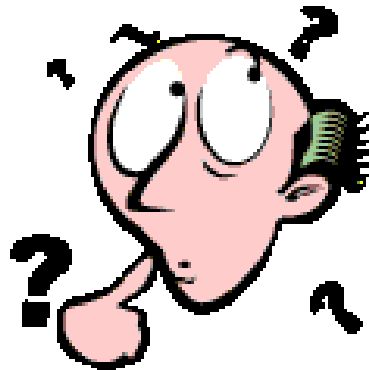
The “how” will be discussed in later slides. For example, present information in useful fashion to make analysis easier.

\* - NOT eliminate all human errors

This presentation will categorize the different types of security tools, describe their common uses during CC testing, and rank their practicability and effectiveness for testing. The purpose is to show how specific tools can make life easier during CC testing.

**Disclaimer:** This presentation is not meant to advertise any particular security tool or validate the performance of any specific security tool. There will be no disclosure of vendor or SAIC proprietary tools.

Over 300 security tools for network discovery, scanning and sniffing, password cracking, fuzzing, remote access testing, computer forensics, integrity checker, vulnerability assessment and penetration testing.



Fortunately, organizations such as National Institute for Standards and Technology (NIST) and SANS<sup>1</sup> have already defined the different categories.

1. (SysAdmin, Audit, Network, Security)

# Category of tools

Technique	Type of Tool
Review	Network Sniffing
	File Integrity Checking
Target Identification and Analysis	Application Security Testing
	Network Discovery
	Network Port and Service Identification
	Vulnerability Scanning
	Wireless Scanning
Target Vulnerability Validation	Password Cracking
	Remote Access Testing
	Penetration Testing

Reference: NIST SP800-115 [1]

SANS
Planning and Recon
Scanning
Exploitation
Password Attacks
Wireless Attacks
Web App Attacks

Reference: SANS [2]

BackTrack
Information Gathering
Network Mapping
Vulnerability Identification
Penetration
Privilege Escalation
Maintaining Access
Radio Network
VOIP & Telephony Analysis
Digital Forensics
Reverse Engineering

## SAIC CCTL

- Information Gathering Tools
- Data Capture Tools
- Data Generation Tools
- Identifying Vulnerability Tools
- Penetration Tools
- Web Application Security Tools
- Other Miscellaneous Tools

## ▪ Information Gathering Tools

Tool	Description
Nmap/Zenmap, Amap	Ports, protocols, and services scanner.
AccessEnum (part of Sysinternals)	Windows access permissions enumerator.
IKE-Scan	Discover, fingerprint, and test IPSec VPN servers.
P0f*, Xprobe2*	Operating system fingerprinting.
Traceroute*, Tracert*:	Discover route between two systems.
Netstumbler*:	Detect wireless network and access points.

\* - Not as practical (e.g., more for systems certification)

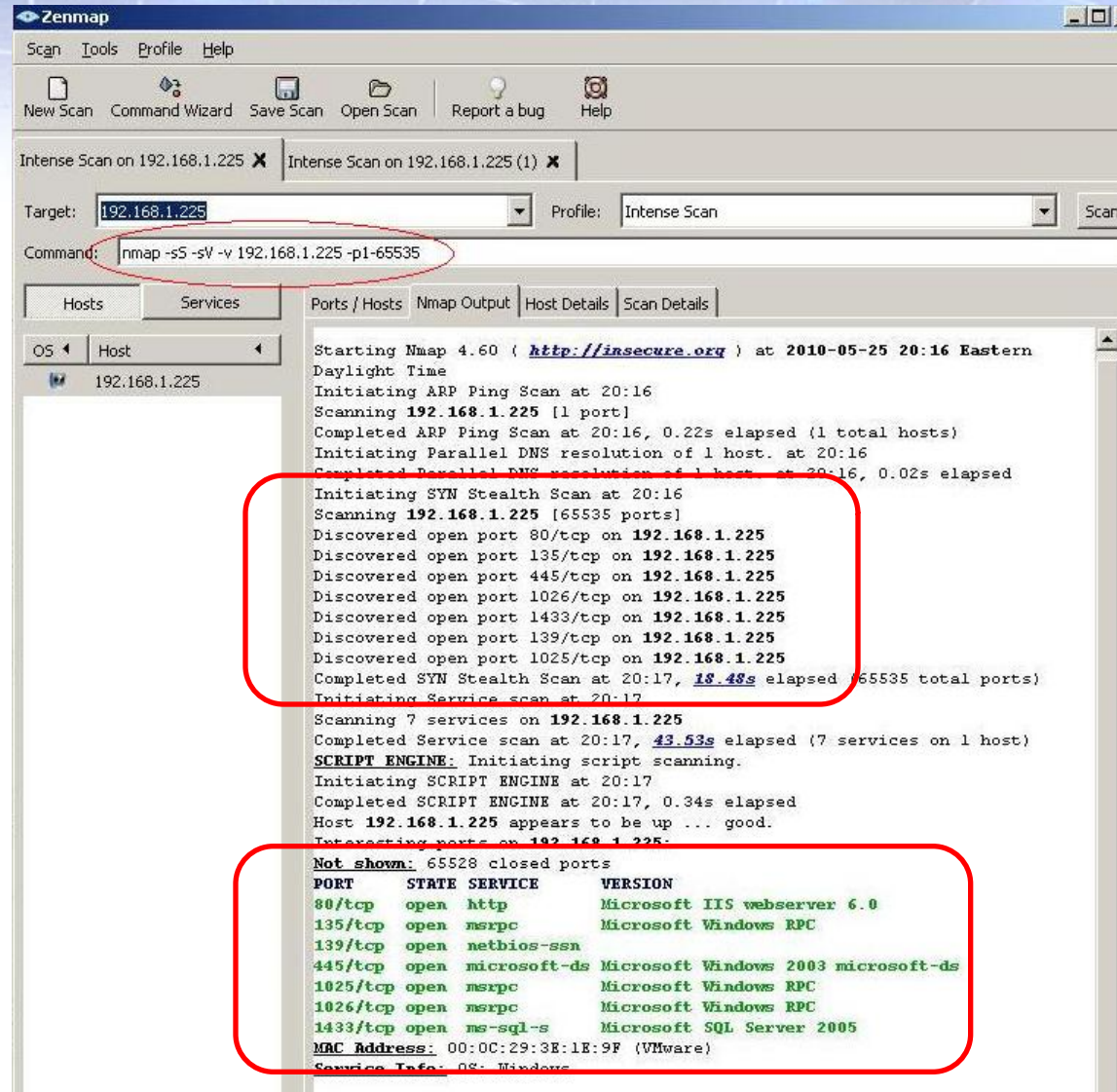
# Category of tools

- Zenmap

Command

Opened Ports

Identified Services



The screenshot shows the Zenmap application window. The 'Command' field is highlighted with a red circle and contains the command: `nmap -sS -sV -v 192.168.1.225 -p1-65535`. The 'Nmap Output' pane shows the scan results, with the discovered open ports section highlighted by a red circle. Below that, the 'Identified Services' table is also highlighted by a red circle.

```

Starting Nmap 4.60 ( http://insecure.org ) at 2010-05-25 20:16 Eastern Daylight Time
Initiating ARP Ping Scan at 20:16
Scanning 192.168.1.225 [1 port]
Completed ARP Ping Scan at 20:16, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:16
Completed Parallel DNS resolution of 1 host. at 20:16, 0.02s elapsed
Initiating SYN Stealth Scan at 20:16
Scanning 192.168.1.225 [65535 ports]
Discovered open port 80/tcp on 192.168.1.225
Discovered open port 135/tcp on 192.168.1.225
Discovered open port 445/tcp on 192.168.1.225
Discovered open port 1026/tcp on 192.168.1.225
Discovered open port 1433/tcp on 192.168.1.225
Discovered open port 139/tcp on 192.168.1.225
Discovered open port 1025/tcp on 192.168.1.225
Completed SYN Stealth Scan at 20:17, 18.48s elapsed (65535 total ports)
Initiating Service scan at 20:17
Scanning 7 services on 192.168.1.225
Completed Service scan at 20:17, 43.53s elapsed (7 services on 1 host)
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 20:17
Completed SCRIPT ENGINE at 20:17, 0.34s elapsed
Host 192.168.1.225 appears to be up ... good.
Interesting ports on 192.168.1.225:
Not shown: 65528 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS webserver 6.0
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows [un]ix SMB 1.0
445/tcp    open  microsoft-ds  Microsoft Windows 2003 microsoft-ds
1025/tcp   open  msrpc          Microsoft Windows RPC
1026/tcp   open  msrpc          Microsoft Windows RPC
1433/tcp   open  ms-sql-s      Microsoft SQL Server 2005
MAC Address: 00:0C:29:3E:1E:9F (VMware)
Service Info: OS: Windows
  
```

- **Data Capture Tools**

Tool	Description
Wireshark/tshark	Network sniffing and protocol analyzer with friendly user GUI. Tools can also sniff wireless communication.
tcpdump	Network sniffing and packet analyzer command line tool.
ssldump	SSLv3 and TLS network protocol analyzer. If provided keying material, can decrypt and display the application data traffic.

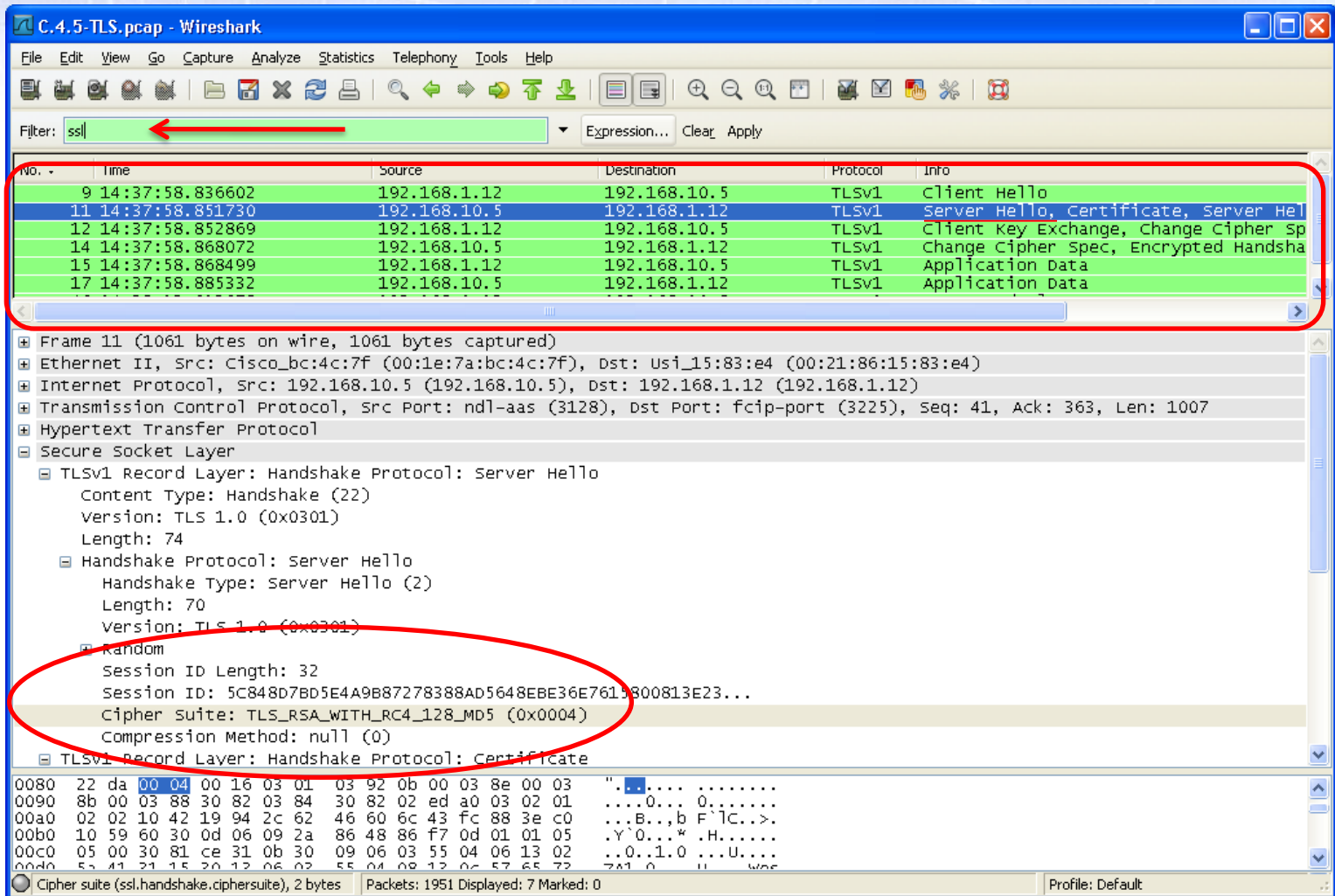
# Category of tools

- Wireshark

Filter

Packets

Details



The screenshot shows the Wireshark interface with the following components:

- Filter:** The filter bar contains the text `ssl`, with a red arrow pointing to it.
- Packets:** A list of captured packets is shown, with packets 9 through 17 highlighted in green. A red box encloses this list.
- Details:** The details pane shows the structure of the selected packet (Frame 11). A red oval highlights the `Random` section, which includes:
  - Session ID Length: 32
  - Session ID: 5c848d7bd5e4a9b87278388ad5648ebe36e7619800813e23...
  - Cipher suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)
  - Compression Method: null (0)

- **Data Generation Tools**

Tool	Description
hping3	Network packet crafting and probing command line utility (similar to nemesis).
scapy	Interactive packet manipulation program.
tcpreplay	Replay PCAP files at arbitrary speeds on network.
netcat	General-purpose TCP and UDP network initiator and listener.

# Category of tools

- hping3

- #hping3 -b 192.168.135.208** //send packets with bad UDP/TCP checksum

- #hping3 192.168.4.41 --seqnum -p 139 -S -i u1 -l eth0**

HPING uaz (eth0 192.168.4.41): S set, 40 headers + 0 data bytes

2361294848 +2361294848

2411626496 +50331648

2545844224 +134217728

2713616384 +167772160

2881388544 +167772160

3049160704 +167772160

3216932864 +167772160

3384705024 +167772160

//analyze whether TCP sequence number is predictable

- #hping3 192.168.135.208 -a <<fakeaddress>>** //send packets with fake source address

- #hping3 -S 192.168.4.41 -a 10.1.1.1 -p ++21**

- #hping3 -P 192.168.4.41 -d 80 -p 80 -E /home/don/test.sig**

## ▪ Identify Vulnerability Tools

Tool	Description
Nessus, Tenable**	Vulnerability scanner.
Nikto2/Wikto	Web vulnerability scanner.
IKEProbe	Determine vulnerabilities in the pre-shared key implementation.
OpenSSL-Scanner	Scan for remote exploit for KEY_ARG overflow in OpenSSL 0.9.6d or older.
Saint**	Vulnerability scanner.
Retina eEye Security Scanner**	Vulnerability scanner.

\*\* - Commercial Tools



## ▪ Penetration Tools

Tool	Description
Metasploit	Free and open-source exploitation framework.
CoWPAtty, Aircrack-ng	WPA and WEP pre-shared key cracker.
PSK-Crack	Crack IKE aggressive mode pre-shared keys.
OpenSSL-To-Open	Perform remote exploit for KEY_ARG overflow in OpenSSL 0.9.6d or older.
THC Hydra*	Perform password guessing attacks against network services.
John the Ripper*	Offline password cracker.

\* - Not as useful (again, more for systems certification)

## ▪ Web Application Security Tools

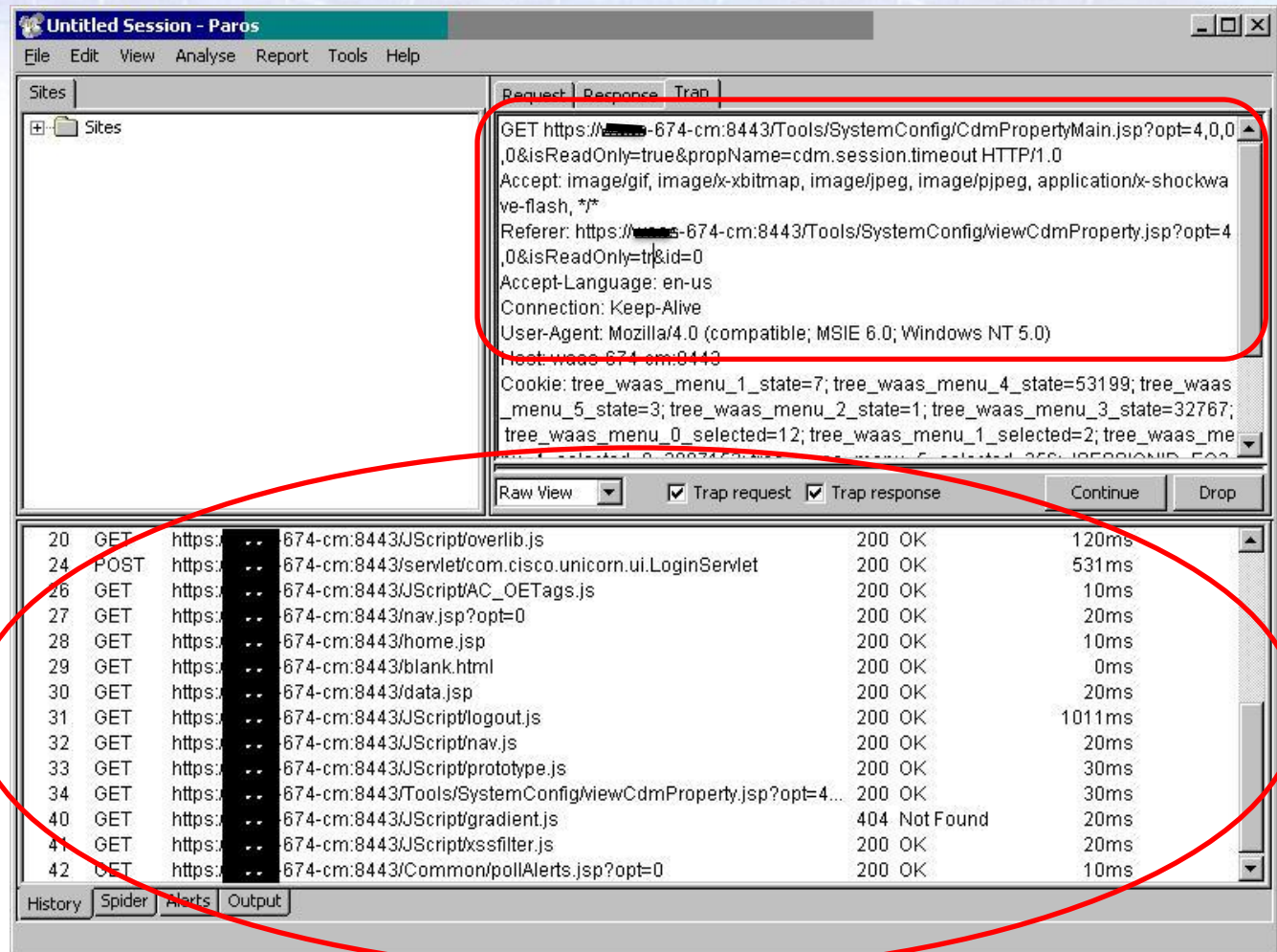
Tool	Description
Paros Proxy	Non-transparent proxy for fine-grained manipulation of HTTP and HTTPS sessions. Includes web vulnerability scanning feature.
WebScarab	Intercepting proxy for reviewing and modifying requests and responses.
Httpprint_GUI	Web server fingerprinting
SPI Dynamics WebInspect**	Web applications and services vulnerability scanner.

\*\* - Commercial tools

# Category of tools

- Paros Proxy

Trap request and response



The screenshot shows the Paros Proxy interface with the following details:

- Request Tab:**

```

GET https://[redacted]-674-cm:8443/Tools/SystemConfig/CdmPropertyMain.jsp?opt=4,0,0
_0&isReadOnly=true&propName=cdm.session.timeout HTTP/1.0
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwa
ve-flash, */*
Referer: https://[redacted]-674-cm:8443/Tools/SystemConfig/viewCdmProperty.jsp?opt=4
_0&isReadOnly=tr&id=0
Accept-Language: en-us
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: waas-674-cm:8443
Cookie: tree_waas_menu_1_state=7; tree_waas_menu_4_state=53199; tree_waas
_menu_5_state=3; tree_waas_menu_2_state=1; tree_waas_menu_3_state=32767;
tree_waas_menu_0_selected=12; tree_waas_menu_1_selected=2; tree_waas_me
nue_4_selected=9; tree_waas_menu_5_selected=250; JSSESSIONID=500

```
- Response Tab:** (Empty)
- Request List:**

No.	Method	URL	Status	Reason	Time
20	GET	https://[redacted]-674-cm:8443/JScript/overlib.js	200	OK	120ms
24	POST	https://[redacted]-674-cm:8443/servlet/com.cisco.unicorn.ui.LoginServlet	200	OK	531ms
26	GET	https://[redacted]-674-cm:8443/JScript/AC_OETags.js	200	OK	10ms
27	GET	https://[redacted]-674-cm:8443/nav.jsp?opt=0	200	OK	20ms
28	GET	https://[redacted]-674-cm:8443/home.jsp	200	OK	10ms
29	GET	https://[redacted]-674-cm:8443/blank.html	200	OK	0ms
30	GET	https://[redacted]-674-cm:8443/data.jsp	200	OK	20ms
31	GET	https://[redacted]-674-cm:8443/JScript/logout.js	200	OK	1011ms
32	GET	https://[redacted]-674-cm:8443/JScript/nav.js	200	OK	20ms
33	GET	https://[redacted]-674-cm:8443/JScript/prototype.js	200	OK	30ms
34	GET	https://[redacted]-674-cm:8443/Tools/SystemConfig/viewCdmProperty.jsp?opt=4...	200	OK	30ms
40	GET	https://[redacted]-674-cm:8443/JScript/gradient.js	404	Not Found	20ms
41	GET	https://[redacted]-674-cm:8443/JScript/xssfilter.js	200	OK	20ms
42	GET	https://[redacted]-674-cm:8443/Common/pollAlerts.jsp?opt=0	200	OK	10ms

## Other Miscellaneous Tools

Tool	Description
Firewalk	Network auditing tool to determine firewall filters.
fragrouter	Route network traffic in a way to elude most network IDS/IPS.
CIRT Fuzzer	Generate and send random data of various size to detect user data validation flaws.
WinHex	Disk editor for Windows.
Fortify SCA~, RATS~, Flawfinder~	Scan C, C++, Perl, PHP, and/or Python code for common programming errors such as buffer overflow and TOCTOU race conditions.

~ - Part of development process [3]

- **Functional Testing** – Provides assurance that the TSF functions as claimed in the Security Target and behaves as described in the design documentation.
- **Penetration Testing** – Attempts to identify exploitable vulnerabilities and weakness in the design and/or implementation of the TSF.

- **Functional Testing**

<b>Description</b>	<b>Security Functional Requirement</b>	<b>Tools</b>
Verify SSL/TLS and SSH handshake and encrypted data.	FPT_ITT/ITC/ITI, FTP_TRP, FTP_ITC, FCS_COP, etc.	Wireshark, ssldump
Test information flow policy and ACL filter rules.	FDP_IFC, FDP_IFF, FAU_GEN	Firewalk, hping3, nc
Verify residual data protection and disk/file encryption	FDP_RIP, disk/file encryption extended SFRs	WinHex
Test fragmentation rules and re-assembly.	FDP_IFF, IDS/FW PP extended SFRs	hping3/nemesis, fragrouter

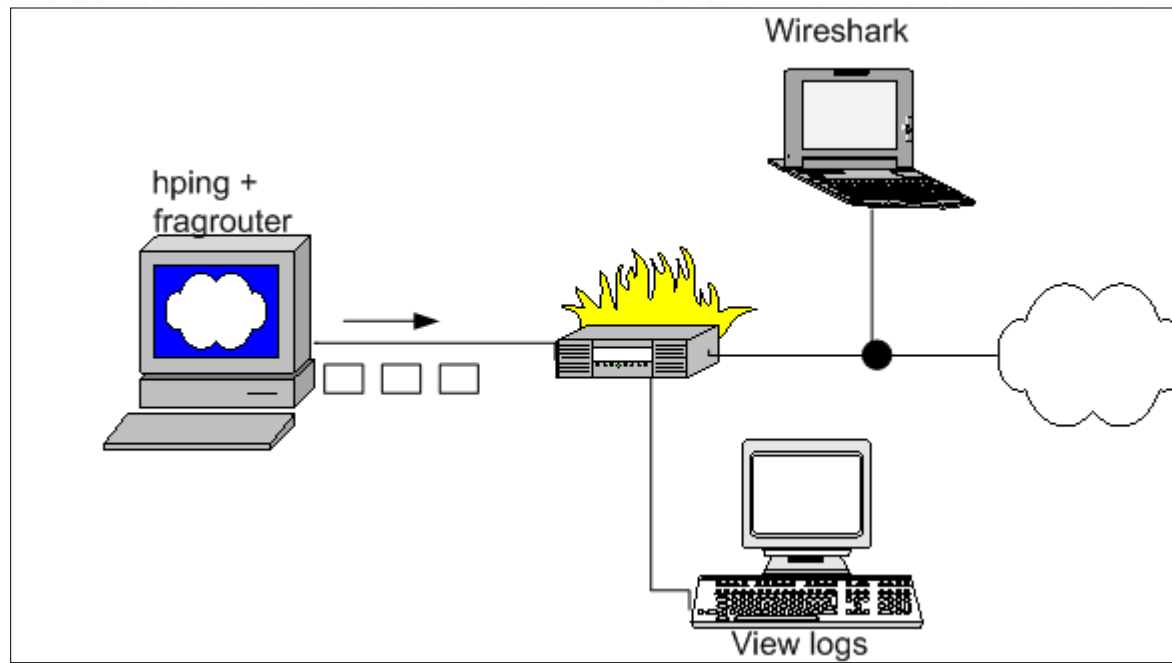
- Penetration Testing

Description	Tool
Confirm that only required ports, services, and protocols are open and accessible.	Nmap, Amap, Nessus, Tenable, Saint, etc.
Validate the correct and non-vulnerable versions are implemented (e.g., SSHv2).	Nmap, Amap, Nessus, Tenable, Saint, etc.
Search for sensitive data (e.g., passwords, keys, audit data) in encrypted communication or disk.	Wireshark, tcpdump, WinHex, dd
Scan for web vulnerability (e.g., XSS, SQL injection, poor user data validation) or outdated web server.	Nitko2, Witko, Paros Proxy, WebInspect
Scan for vulnerable IPSec implementation.	IKEProbe

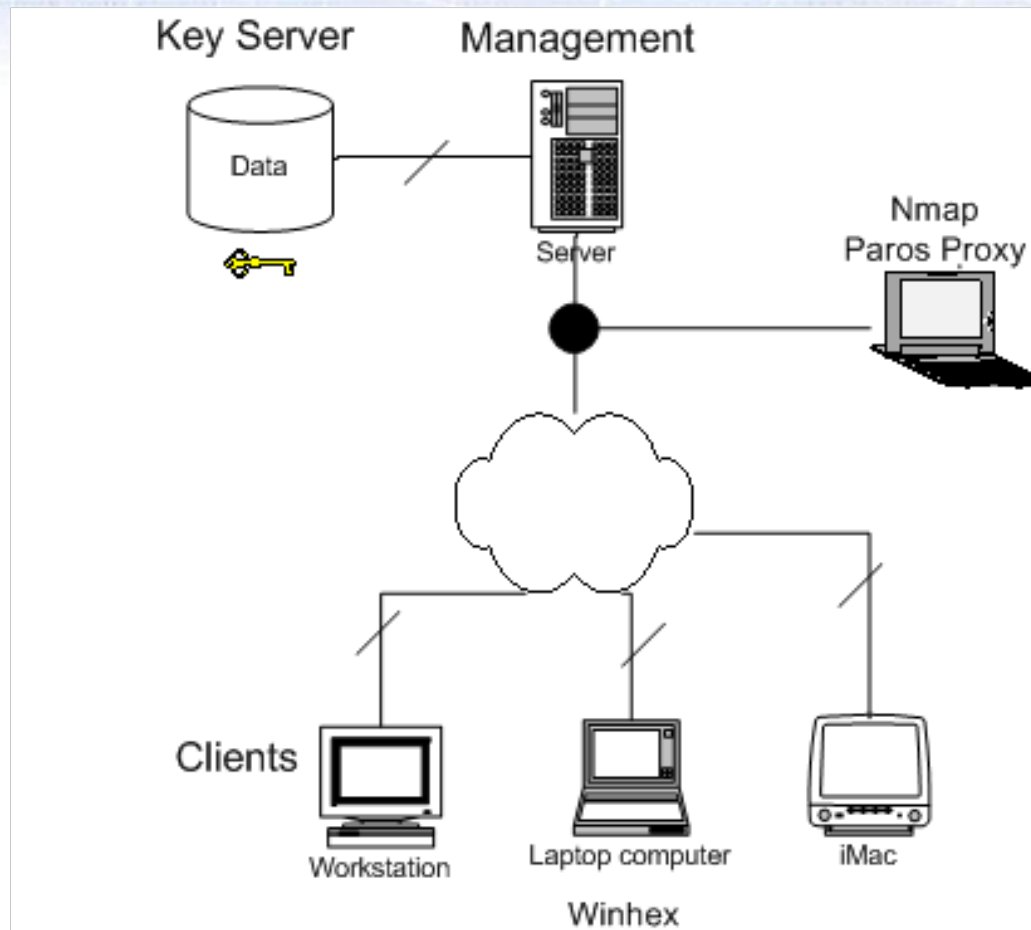
- Penetration Testing

Description	Tool
Validate and confirm positive results finding.	Metasploit, PSK-Crack, Aircrack-ng, etc.
Generate and send malformed data packets (e.g., illegal fragment, violate RFCs, large data).	hping3, Nemesis, scapy, fragrouter
Attempt to cause resource exhaustive DoS attackers or replay attacks.	tcpreplay, fuzzer, Nessus
Perform session hijacking, web session manipulation, or man-in-the-middle attack.	Paros Proxy, WebScarab, etc.
Search for unprotected TSF files or data on the operating system.	AccessEnum

# Common Criteria testing



Example Test Configuration #1



Example Test Configuration #2

- Criteria
  - Security Functional Requirements
  - Practical use during CC testing
  - Ease and frequency of uses
  - Cost

**NOTE:** This list is by no means comprehensive and should not be misconstrued as to prohibit or discourage other tools from being use during CC testing.

- Top 10 Recommended Tools for CC Testing
  1. Wireshark
  2. Nmap
  3. Nessus/Tenable
  4. Nikto2/Wikto
  5. hping3 or scapy
  6. Paros Proxy or WebScarab
  7. Metasploit
  8. Firewalk
  9. fragrouter
  10. WinHex

- Security tools are beneficial to CC evaluation
- Define the different category of tools and explain how they are used for functional and penetration testing.
- For CC testing, some tools are better than others
  - Pre-certification phase
  - During certification phase
  - After certification phase
- Recommended tools for CC testing
- Please send me any tools you like to recommend

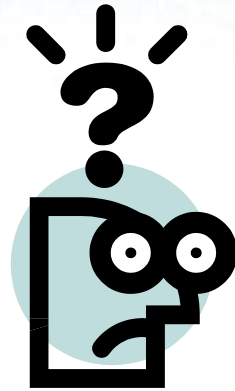
Quang Trinh

SAIC Accredited Testing & Evaluation Labs,  
Common Criteria Evaluator and FIPS Tester

[Quang.M.Trinh@saic.com](mailto:Quang.M.Trinh@saic.com)

<http://www.saic.com/infosec/testingaccreditation/>

Questions?



**Thank You**

1. NIST Special Publication 800 – 115 (Technical Guide to Information Security Testing and Assessment), <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>
2. SANS Network Penetration Testing and Ethical Hacking, SEC-560
3. Common Criteria and Source Code Analysis Tools: Competitors or Complements, Adam O' Brien, Oracle