

Appendix A: Further Reading/Resources

Attack Trees

- Attack trees: Modeling Security Threats, Bruce Schneier, Dr. Dobbs Journal, <https://www.schneier.com/paper-attacktrees-ddj-ft.html>
- Investigative Tree Models, Rodney Caudle, SANS Reading Room <https://www.sans.org/reading-room/whitepapers/incident/investigative-tree-models-33183>
- Attack Tree Analysis, Terrance Ingoldsby, Red Team Journal <http://redteamjournal.com/2009/01/attack-tree-analysis/>
- Fundamentals of Capabilities-based Attack Tree Analysis, Terrance Ingoldsby, Amenaza Technologies Limited <http://www.amenaza.com/downloads/docs/AttackTreeFundamentals.pdf>
- ADTool: Security Analysis with Attack-Defense Trees, Barbara Kordy, et.al. <http://satoss.uni.lu/members/sjouke/papers/KoKoMaSc13.pdf>
- ADTool, opensource, University of Luxemburg, <http://satoss.uni.lu/members/piotr/adtool/ADTool-1.4-jar-with-dependencies.jar>
- Secur/Tree, licensed, Amenaza Technologies, <http://www.amenaza.com/>
- AttackTree, licensed, Usograph, <http://www.isograph.com/software/attacktree/>

Data Diodes

- All Diodes Are Not Equal http://www.owlcti.com/pdfs/whitpapers/All_Diodes_Are_Not_Equal.pdf
- Tactical Data Diodes in Industrial and Automation and Control System <http://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automationcontrol-systems-36057>
- Secure Cross Boarder Information Sharing Using One-way Data Transfer Systems http://www.owlcti.com/pdfs/CrossBorderinfoSaring_ISGIG_r01n_coverincl.pdf

Proxy Servers

- Squid <http://www.squid-cache.org/Intro/>

Netflow

Below is a short list of OpenSource tools for NetFlow and NetFlow analysis.

- NTop - <http://www.ntop.org/>

Ntop is a traffic analyser that runs on most UNIX variants and Microsoft Windows. In addition, ntop includes Cisco NetFlow and sFlow support.

- FlowScan - <http://pages.cs.wisc.edu/%7Eplonka/FlowScan/>

FlowScan processes IP flows recorded in cflowd format raw flow files and reports on what it finds.

- JKFlow - <http://jkflow.sourceforge.net/>

JKFlow is a XML-configurable Flowscan perl module for reading/analyzing your NetFlow data.

- EHNT - <http://ehnt.sourceforge.net/>

Extreme Happy NetFlow Tool (EHNT) turns streams of Netflow data into something useful and human-readable.

- Nfdump - <http://nfdump.sourceforge.net/>

Tools to dump NetFlow data from pcap files.

- NfSen - <http://nfsen.sourceforge.net/>

Web front end for data produced by Nfdump.

- SiLK - <http://tools.netsa.cert.org/>

The Network Situational Awareness (NetSA) group at CERT has developed and maintains a suite of open source tools for monitoring large-scale networks using flow data.

Host Based Intrusion Systems (HIDS)

- OSSEC - <http://www.ossec.net>

Open source host-based intrusion detection system.

- Tiger - <http://www.nongnu.org/tiger/>

An integrity checker.

- AIDE - <https://wiki.archlinux.org/index.php/AIDE>

Advanced intrusion detection environment.

- SAMHAIN - <http://www.la-samhna.de/samhain/>

File integrity/host-base IDS.

- AFICIK - <http://afick.sourceforge.net/>

Another file integrity checker.

Honeypots

- SCADA Honeynets - <http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3130&context=etd>

Web Application Firewalls



The following is a short discussion of some of the OpenSource WAFs available on the web:
<http://www.fromdev.com/2011/07/opensource-web-application-firewall-waf.html>.

- AQTRONIX WebKnight - <https://www.aqtronix.com/?PageID=99>

AQTRONIX WebKnight is an application firewall for IIS and other web servers and is released under the GNU General Public License. More particularly it is an ISAPI filter that secures your web server by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

- ESAPI - https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=Home

ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications. The ESAPI libraries are designed to make it easier for programmers to retrofit security into existing applications. The ESAPI libraries also serve as a solid foundation for new development.

- IronBee - <https://www.ironbee.com>

IronBee is a universal web application security framework. Think of IronBee as a framework for developing a system for securing web applications - a framework for building a web application firewall (WAF) if you will.

- Jumperz_net - <http://guardian.jumperz.net/index.html>

JUMPERZ_NET is an open source application layer firewall for HTTP/HTTPS. It works as a reverse proxy server. It analyzes all HTTP/HTTPS traffic against rule-based signatures and protects web servers and web applications from attack. When unauthorized activity is detected, JUMPERZ_NET can disconnect the TCP connection before the malicious request reach the web server.

- ModSecurity - <http://www.modsecurity.org/>
https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

- Smoothwall - <http://www.smoothwall.org/about/>

The Smoothwall Open Source Project was set up in 2000 to develop and maintain Smoothwall Express - a Free firewall that includes its own security-hardened GNU/Linux operating system and an easy-to-use web interface.

- WebCastellum - <http://mvnrepository.com/artifact/org.webcastellum/webcastellum/1.8.3>

Java-based Open Source WAF (Web Application Firewall) to include inside a web application in order to protect it against attacks like SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Parameter Manipulation and many more.

Application Whitelisting

- Lumension - <http://www.lumension.com>
- Bit9 - <http://www.bit9.com>
- Savant Protection - <http://www.savantprotection.com>

Security Controls

- Center for Internet Security - <http://www.cisecurity.org/>
- SANS “Twenty Critical Controls for Effective Cyber Defense” - <http://www.sans.org/critical-security-controls/cag4-1.pdf>
- SANS “Top Cyber Security Risks” - <http://sans.org/top-cyber-security-risks/>
- Australian Defense Signals Directorate (DSD.gov.au) “Top 35 Mitigation Strategies” - <http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm>

Note: As of April 2013, the Top 4 Strategies to Mitigate Targeted Cyber Intrusions are mandatory for Australian Government agencies. A guide for implementation for the top four: <http://www.dsd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm>

Incident Response Checklists and Documents

- SANS Incident Handler’s Handbook - <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>
- SANS Sample Incident Handling Forms - <https://www.sans.org/score/incident-forms>
- Information Security Cheat Sheets from Lenny Zeltzer - <https://zeltser.com/cheat-sheets/>

The Top Cyber Threat Intelligence Feeds

- [AlienVault.com](#): Multiple sources including large honeynets that profile adversaries.
- [CrowdStrike.com](#): Advanced threat intel as part of their threat protection platform.
- [Cyveillance.com](#): Unique feeds on threat actors: indications of criminal intent.
- [EmergingThreats.net](#): A variety of feeds.
- [FireEye.com](#): DTI- Dynamic Threat Intelligence service.
- [HackSurfer.com](#) (SurfWatch): Insights tailored to your business.
- [HexisCyber.com](#): Feed supports automated actions.
- [InternetIdentity.com](#): Threat feeds from their big data solution ActiveTrust.
- [iSightPartners.com](#): ThreatScape series.
- [LookingGlass.com](#): Maps of infrastructure, connectivity and ownership, plus threat intel.
- [MalwareCheck.org](#): Intelligence on any URL.
- [MalwareDomains.com](#): A list of domains known to be associated with malware.
- [RedSkyAlliance.com](#): A vetted team of corporate computer incident responders and security professionals.

- RecordedFuture.com: Organizes information from the Internet.
- SecureWorks.com: Provides feeds and also instruments networks.
- Symantec.com: DeepInsight feeds on a variety of topics including reputation.
- Team-Cymru.com: Threat intelligence plus bogon lists.
- ThreatConnect.com by Cyber Squared: Focused on information sharing.
- ThreatGrid.com: Unified malware analysis. Now part of Cisco.
- ThreatIntelligenceReview.com: Updated reviews of threat intelligence sources.
- ThreatStop.com: Block Botnets by IP reputation.
- ThreatStream.com: Famous team. Multiple sources in interoperable platform.
- ThreatTrack.com: Stream of malicious URLs,IPs and malware/phishing related data.
- Verisigninc.com: iDefense feeds highly regarded by some key institutions.

Government Sources of Threat Intelligence

- Industrial Control Systems Computer Emergency Response Team (ICS_CERT) - <https://ics-cert.us-cert.gov/ICS-CERT-Feeds>
ICS-CERT offers feeds for alerts, advisories, joint security awareness reports, and monthly monitors.
- The Defense Cyber Crime Center (DC3) - <http://dc3.mil/>
Provides daily context on the cyber threat and incidents via newsletters and their Twitter feed.
- US Computer Emergency Response Team (US-CERT) - <https://www.us-cert.gov/>
Responds to major incidents and analyzes threats. Shares information on vulnerabilities via alerts and announcements. Large body of tips and awareness items useful to your cyber threat intelligence program.
- European Union Agency for Network and Information Security (ENISA) - <http://www.enisa.europa.eu/>
Tremendous references, publications, media.
- FBI Cyber Crime - <http://www.fbi.gov/about-us/investigate/cyber>
News on latest cases plus testimony of FBI seniors to Congress on cybercrime topics.
- InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S. <https://www.infragard.org>.

Threat Intelligence Reports

- [Checkpoint Security Report](#): Yearly insights into threat actions especially malware and botnets

- [Versign iDefense Cyber Threats and Trends](#): Provides overview of key cyber security trends over the last year.
- [Cisco Midyear Security Report](#): Adversary trends from a Cisco perspective.
- [Symantec Intelligence Report](#): Annual and monthly editions.
- [Verizon Data Breach Investigations Report](#): Insights and analysis broadly collaborated across the community.
- [Ponemon Institute Cost of Breach Study](#): Annual report on economics of breach and recovery.
- [CyberEdge Cyber Threat Report](#): Survey's IT professionals regarding state of defenses and perception of threat.
- [Mandiant M-Trends Report](#): At times overshadowed by DBIR, but full of good info.

Security Awareness Training Resources – The Human aspect of Cyber Security

Available online resources for Security Awareness Training (this list is not all inclusive):

Source	URL	Type	Cost
ICS-CERT Virtual Learning Portal	https://ics-cert-training.inl.gov	Training, Materials	FREE
DHS National Cyber Security Awareness	http://www.dhs.gov/national-cyber-security-awareness-month	Toolkit, Materials	FREE
DOD IASE Training	http://iase.disa.mil/eta/Pages/index.aspx	Videos	FREE
National Cyber Security Alliance	https://www.staysafeonline.org/	Materials	FREE
Multi State Information Sharing and Analysis Center	http://msisac.cisecurity.org/	Materials	FREE
Phish Me	http://phishme.com/	Phishing Test	\$
SANS: IT Information Security Awareness Training	http://www.securingthehuman.org/utility	Toolkit, Training, Materials	FREE/\$
SecureWorks	http://www.secureworks.com/	Training, Materials	\$
Knowbe4	http://www.knowbe4.com/	Training, Materials	\$
MSI Simple Phish	http://microsolved.com/free-tools.html	Phishing Test	FREE
PhishBox	http://www.phishingbox.com/	Phishing Test	\$
OpenDNS quiz	https://www.opendns.com/phishing-quiz/	Training	FREE
Native Intelligence	http://www.nativeintelligence.com/	Videos, Newsletters, Materials	FREE

Other Miscellaneous Documents

Commands

- [Unix_Commands.pdf - https://www.cmu.edu/computing/accounts/storage/afs-unix/commands.html](https://www.cmu.edu/computing/accounts/storage/afs-unix/commands.html)

Incident Handling

- [LM-White-Paper-Intel-Driven-Defense.pdf - http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf](http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf)
- [OIG-13-027-A.pdf - https://www.oig.doc.gov/oigpublications/oig-13-027-a.pdf](https://www.oig.doc.gov/oigpublications/oig-13-027-a.pdf)

manuals,tutorials,etc

- [Armitage Tutorial - Cyber Attack Management for Metasploit.pdf - http://www.fastandeasyhacking.com/manual](http://www.fastandeasyhacking.com/manual)
- [bpf_syntax.pdf - http://biot.com/capstats/bpf.html](http://biot.com/capstats/bpf.html)
- [ScadaHacker.com library - https://scadahacker.com/library/index.html](https://scadahacker.com/library/index.html)
- [Hacking - Meterpreter Cheat Sheet.pdf - https://scadahacker.com/library/Documents/Cheat_Sheets/Hacking%20-%20Meterpreter%20Cheat%20-%20Sheet.pdf](https://scadahacker.com/library/Documents/Cheat_Sheets/Hacking%20-%20Meterpreter%20Cheat%20-%20Sheet.pdf)
- [Hacking - NMap Quick Reference Guide.pdf - https://scadahacker.com/library/Documents/Cheat_Sheets/Hacking%20-%20NMap%20Quick%20Reference%20Guide.pdf](https://scadahacker.com/library/Documents/Cheat_Sheets/Hacking%20-%20NMap%20Quick%20Reference%20Guide.pdf)
- [Port Scanning ICS Networks.pdf - http://www.samuraistfu.org/resources/Port%20Scanning%20ICS%20Networks.pdf?attredirects=0&d=1](http://www.samuraistfu.org/resources/Port%20Scanning%20ICS%20Networks.pdf?attredirects=0&d=1)
- [Understanding SCADAs Modbus Protocol.pdf - http://www.samuraistfu.org/resources/Understanding%20SCADAs%20Modbus%20Protocol.pdf?attredirects=0&d=1](http://www.samuraistfu.org/resources/Understanding%20SCADAs%20Modbus%20Protocol.pdf?attredirects=0&d=1)
- [JStebelton_BPF.pdf - http://www.infosecwriters.com/text_resources/pdf/JStebelton_BPF.pdf](http://www.infosecwriters.com/text_resources/pdf/JStebelton_BPF.pdf)
- [SANS_Meterpreter_Cheat_Sheet.pdf - https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf](https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf)
- [SCADA Honeynets - http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3130&context=etd](http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3130&context=etd)
The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats, Susan Wade, 2011, Iowa State University
- [snort_manual.pdf - https://www.snort.org/documents/snort-users-manual](https://www.snort.org/documents/snort-users-manual)
- [Wireshark_Display_Filters.pdf - http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf](http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf)
- [wireshark_user-guide - https://www.wireshark.org/download/docs/user-guide-a4.pdf](https://www.wireshark.org/download/docs/user-guide-a4.pdf)

Network Headers

- common_ports.pdf - http://packetlife.net/media/library/23/common_ports.pdf
- ipv6_tcpip_pocketguide.pdf - https://www.sans.org/security-resources/ipv6_tcpip_pocketguide.pdf
- packetlife.net.pdf – <http://packetlife.net/library/cheat-sheets/>
Variety of guides/cheat sheets for network protocols and tools.

Below are documents created by 301 Instructors. Detailed information can be found at <https://www.sans.org/security-resources/tcpip.pdf>

- ICMP_Message_Format.pdf -
- IP_header.pdf
- Link_Layer_Headers.pdf
- TCP_header.pdf
- UDP_Header.pdf
- Encapsulation_of_data.pdf – Encapsulation of data in TCP Packets – additional information can be found at http://www.tcpipguide.com/free/t_IPDatagramEncapsulation.htm

Tools (lists created by instructors)

- kalitools.htm - List of tools on the ICSCERT kali-linux iso.
- Tools.htm – List of Open Source software tools use in cyber defense.



Appendix B: Opensource Pcap Compatible Tools

List of OpenSource pcap compatible tools (probably incomplete!)

****IX Based Tools**

<u>Name</u>	<u>Website</u>
Argus	http://www.qosient.com/argus/
Barnyard2	http://www.securixlive.com/barnyard2/
Bro	http://bro-ids.org/
Chaosreader	http://chaosreader.sourceforge.net/
Daemonlogger	http://www.snort.org/snort-downloads/additional-downloads#daemonlogger
Driftnet	http://www.ex-parrot.com/~chris/driftnet/
Etherape	http://etherape.sourceforge.net/
Libpcap	http://www.tcpdump.org/
Mergecap	http://www.wireshark.org/docs/man-pages/mergcap.html
Moloch	https://github.com/aol/moloch
Net::Pcap	http://search.cpan.org/~kcarnut/Net-Pcap-0.05/Pcap.pm
Net::Pcap::Easy	http://search.cpan.org/~jettero/Net-Pcap-Easy-1.4207/Easy.pod
Netsniff-ng	http://netsniff-ng.org/
Nftracker	https://github.com/gamlinux/nftracker
Ngrep	http://ngrep.sourceforge.net/
OSSEC	http://www.ossec.net/
Pcapcat	http://blog.kiddaland.net/dw/pcapcat
Reassembler	http://isc.sans.edu/diary.html?storyid=13282
Securityonion	http://code.google.com/p/security-onion/
Smart.pl	http://safemap.sourceforge.net/
Sniffit	http://sniffit.sourceforge.net/
Snort	http://www.snort.org/
Suricata	http://www.openinfosecfoundation.org/index.php/download-suricata
Tcpdump	http://www.tcpdump.org/
Tcpick	http://tcpick.sourceforge.net/
Tcpreplay	http://tcpreplay.synfin.net/
Tcpslice	http://sourceforge.net/projects/tcpslice/
Tcpstat	http://www.frenchfries.net/paul/tcpstat/
Tcpextract	http://tcpextract.sourceforge.net/
Tshark	http://www.wireshark.org/docs/man-pages/tshark.html
Vortex	http://sourceforge.net/projects/vortex-ids/
Wireshark	http://www.wireshark.org/
Xplico	http://www.xplico.org/

Windows Based Tools

Name	**IX tool	Website
Windump	Tcpdump	http://www.winpcap.org/windump/
Winpcap	Libpcap	http://www.winpcap.org
Wnetp::Pcap	Net::Pcap	http://www.bribes.org/perl/wnetpcap.html
Winsnort	Snort	http://www.winsnort.com/
Wireshark	Wireshark	http://www.wireshark.org/



Appendix C: Understanding the Hacker's Mind



Most of our students have some kind of engineering background, either developing physical widgets or virtual writing computer programs. Their training, thought processes, and work experiences are to make the widget work. Their “pay” is how well the widget works.

A hacker has just the opposite mindset. They want to understand how the widget works and most importantly what flaws it has. These flaws can be either design flaws and/or implementation flaws. Once they know and understand the flaws, they can develop attacks using that knowledge. There aren't just bad hackers. There are also good hackers. We call them Cybersecurity Researchers.

There are three problems that we face in cybersecurity:

1. There are more of them (bad guys) than there are of us.
2. It takes time (=money) to identify vulnerabilities and mitigation techniques.
3. Sometimes you just have to upgrade to a new product.

One of the comments we often get from students is that they feel we are teaching them how to attack their environment instead of defending it. Actually this is not the case if you think about how a sports coach prepares their team for the next game. In most cases, the team watches movies of the opposing team to understand how they play and what techniques they have mastered. Many coaches will tell you that you cannot have a strong defense if you don't understand the offense.

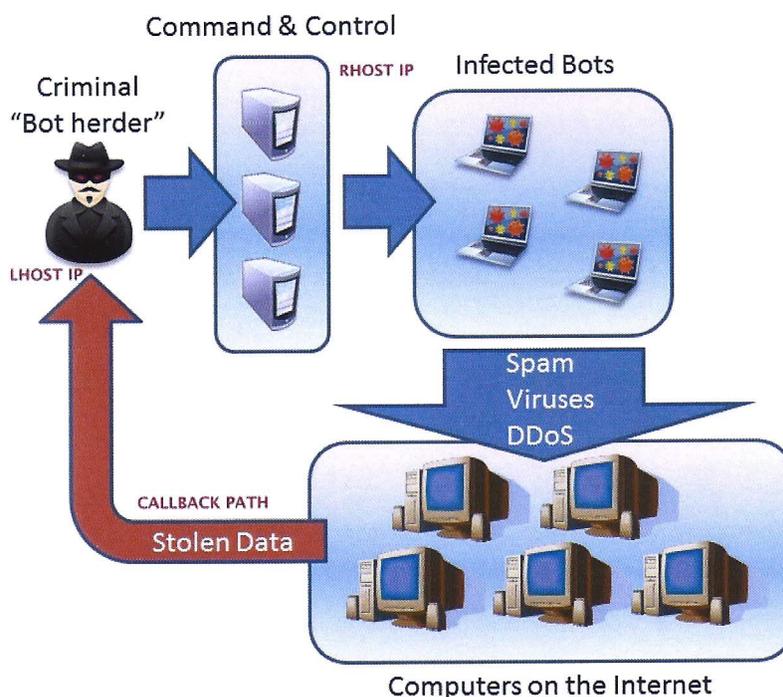
This is the same teaching methodology we use. Throughout the course, we have been providing information on techniques to better understand your environment and the methodology used by the attacker community.

In the previous session you were introduced to a hacking tool called Metasploit. One thing to keep in mind is that any serious hacking community, such as Advanced Persistent Threats (APTs), will not be using Metasploit. They will be using their own set of tools. Most of the anti-virus packages have signatures for the Metasploit/Meterpreter modules. However, the attack methodology is the same regardless of the tools an attacker has at his/her disposal.

How Metasploit works! The 'Bot Net'

The figure below shows the general idea of a botnet. A botnet is a collection of zombie computers, ones that act on someone else's behalf. They have been compromised and set up to act as forwarders for malware, etc. Most systems that have been compromised and set up in this fashion are home-based systems where the owner has not shown due diligence in keeping their

system patched and up to date. Kaspersky Labs and Symantec maintain that these botnets have become the largest threat to the internet at large.



Let's take a look from a defensive point of view how Metasploit/Meterpreter work in a botnet environment. Do you remember the two major variables you had to set when you working with Metasploit/Meterpreter?

RHOST was set to the 'victims' IP-address.

LHOST you set to your local IP-address.

The relationship of these is shown in the diagram above. The **LHOST** IP address is often referred to as the callback address. The **RHOST** address is the zombie you want to compromise, thus providing a pivot point to move onto your next victim. The **LHOST** (callback) address is the address of the attacker, NOT the **RHOST** (zombie). The **RHOST** address shows up in logs as the **SRC** address of the traffic. The **LHOST** only shows up in the logs when there is traffic (information going out).

The other piece of information that can be useful in locating a callback address is the destination port number used by the malware. Callbacks can use a variety of port numbers outside of the traditional 80 or 8080 used by typical HTTP traffic. Identifying outbound traffic to weird destination ports can help in identifying not only the callback address(s) but also in some cases the malware that has been deployed.

A wealth of information on detection techniques can be found on the SANS.org reading-room (<http://www.sans.org/reading-room>). Another great area of the SANS.org website is the collection of student papers that were prepared for certifications and graduate credits. One of the interesting papers is "*Assessing Outbound Traffic to Uncover Advanced Persistent Threat*" by Beth E. Binde, Russ McRee, and Terrence J. O'Connor, 5/22/2011. (<http://www.sans.edu/student-files/projects/JSP-Binde-Mcree-OConnor.pdf>)

PCAP/Network Forensics

Network forensics involves the capture, recording, and analysis of network events in order to discover the evidence of security attacks or other problem incidents. Until you do the forensics, you cannot make the judgment call as to the nature of the event. Packet capture provides the raw evidence of the event, but it still takes a human to understand what the data is telling them.

When working with packet captures, always have a goal in mind. Network captures contains so much information that you can quickly start going down the wrong path if you do not prioritize your goals. Some items you will be analyzing in a packet capture are:

1. Pattern matching – Identify and filter all of the packets of interest by matching specific values or protocol meta data.
2. List conversations – List all of the conversation streams of interest. (*Note: these may also be called sessions.*)
3. Export – Isolate and export the specific conversations of interest.
4. Draw conclusions – Extract files or other information, analyze, and compile data about the event.

Below are a couple of definitions to help you understand the rest of this section.

Conversation – Two-way data exchange of a network between to computers. This is sometimes referred to as a session.

Flow - Either side of the conversation; client → server or server → client.

Some tools that are available to help in pcap forensics are:

- **Wireshark/tshark** is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- **NetworkMiner** is a free open-source tool that collects data (such as forensic evidence) about hosts on the network rather than collecting data regarding the traffic on the network.
- **Tcpdump** is a common packet analyzer that runs under the UNIX command line. It allows the user to capture and display TCP/IP or other packets being transmitted or received over a network.
- **Windump** is a version of **tcpdump** for the Windows-based operating systems.
- **Tcpflow** is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis and debugging. Each TCP flow is stored in its own file. Thus, the typical TCP flow will be stored in two files, one for each direction of the conversation. Tcpflow can also process stored tcpdump packet flows.
- **Tcpextract** – A tool for extracting files from a network conversation.
- **Argus** is an advanced comprehensive network traffic monitoring system that can produce flow data of all the flows in the packet stream. This is similar to Tcpflow.

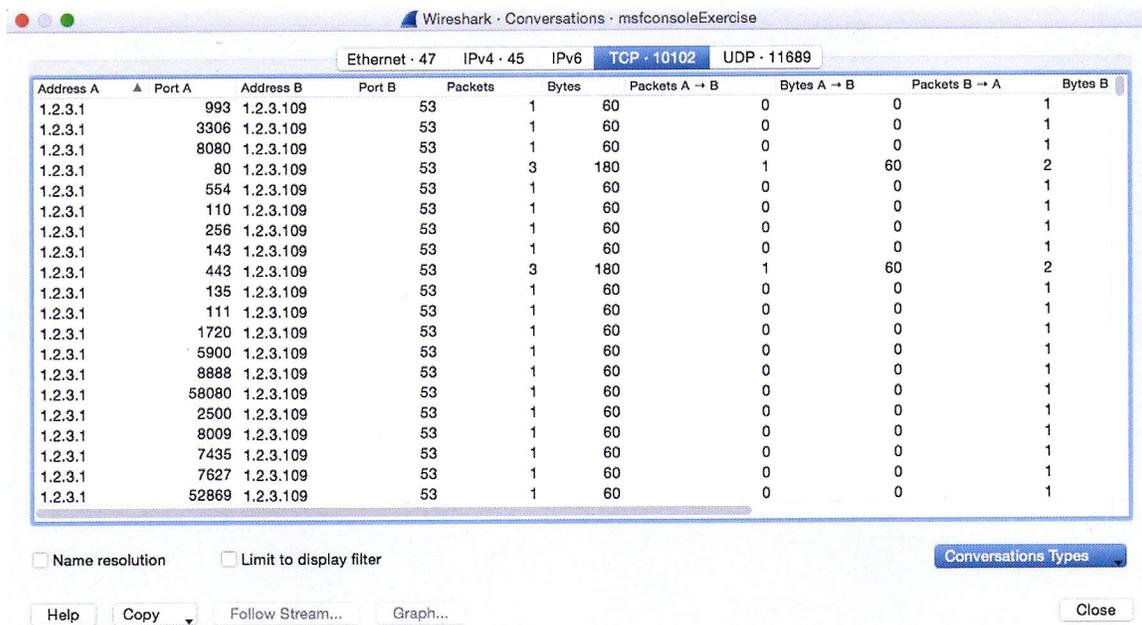
Demonstration of Wireshark and Network Miner

The next few sections are exercises for you to try out your detective skills and figure out the answers to the puzzles. One of the most useful options in Wireshark is the capability to *Follow TCP Stream*. This option actually splits out the two data flows so you can see the whole picture instead of just bits and bytes. Remember: **red** is the client, and blue is the server's response.

Conversations

Another way to view communications on the stream, is by looking at the Conversations.

After opening your pcap file (msfconsoleExercise.pcap), click on *Statistics -> Conversations* in the top menu. You will see a screen similar to the one below.



The screenshot shows the Wireshark interface with the 'Conversations' window open. The window title is 'Wireshark · Conversations · msfconsoleExercise'. The filter is set to 'Ethernet · 47 IPv4 · 45 IPv6 TCP · 10102 UDP · 11689'. The table below shows the details of the conversations.

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B
1.2.3.1	993	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	3306	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	8080	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	80	1.2.3.109	53	3	180	1	60	60	2
1.2.3.1	554	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	110	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	256	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	143	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	443	1.2.3.109	53	3	180	1	60	60	2
1.2.3.1	135	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	111	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	1720	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	5900	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	8888	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	58080	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	2500	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	8009	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	7435	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	7627	1.2.3.109	53	1	60	0	0	0	1
1.2.3.1	52869	1.2.3.109	53	1	60	0	0	0	1

Below the table are several controls: Name resolution, Limit to display filter, a 'Conversations Types' dropdown menu, and buttons for 'Help', 'Copy', 'Follow Stream...', 'Graph...', and 'Close'.

This particular screen will show individual conversations between two ip addresses based on unique port combination. Note the source port (Port A) changes while the destination port (Port B) remains the same. What would be an explanation for this?

You can select a stream and then click on *Follow Stream* at the bottom of the screen and see the same output as you would by selecting *Follow TCP Stream* from the packet list.

Finding HTTP Requests

In a packet capture which contains http traffic, you can easily see the requests that were made. From the top menu, click on *Statistics -> HTTP -> Requests*.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
HTTP Requests by HTTP Host	3				0.0000	100%	0.0100	1009.882
1.2.3.110:8080	3				0.0000	100.00%	0.0100	1009.882
/melinda/payload	1				0.0000	33.33%	0.0100	1010.301
/melinda	2				0.0000	66.67%	0.0100	1009.882

Display filter: Apply

Help Copy Save as... Close

Export Objects

Another useful feature of Wireshark, is Export Objects. With this you can see and save out files that are in the pcap from either SMB, HTTP, TFTP or DICOM. To see the HTTP objects in this pcap, click on *File -> Export Objects -> HTTP*.

Wireshark File Edit View Go Capture Analyze Statistics Telephony Help

msfconsoleExercise.pcap

No.	Time	Protocol	Length	Info
1	2.000000	BROWSER	243	Host Announceme
2	2.000000	DHCP	342	DHCP Discover -
3	2.000000	BROWSER	243	Host Announceme
4	2.000000	NBNS	92	Name query NB S
5	2.000000	ARP	60	Who has 192.168
6	2.000000	NBNS	92	Name query NB S
7	2.000000	BROWSER	255	Local Master An
8	2.000000	BROWSER	252	Domain/Workgrou
9	2.000000	ARP	60	Who has 192.168
10	2.000000	NBNS	92	Name query NB S
11	2.000000	ARP	60	Who has 192.168

File menu options:

- Open (⌘O)
- Open Recent
- Merge...
- Import from Hex Dump...
- Close (⌘W)
- Save (⌘S)
- Save As... (⇧⌘S)
- File Set
- Export Specified Packets...
- Export Packet Dissections
- Export Packet Bytes...
- Export PDUs to File...
- Export SSL Session Keys...
- Export Objects
 - DICOM...
 - HTTP... (1944 bits)
 - SMB...
 - TFTP
- Print... (⌘P)

Packet list details:

- Frame 1: 243 bytes on wire (1944 bits) captured (1944 bits) on interface 0
- Ethernet II, Src: Intel (08:00:27:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.0.255 (192.168.0.255), Dst: 192.168.0.255 (192.168.0.255)
- User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
- NetBIOS Datagram Service
- SMB (Server Message Block Protocol)

Packet	Hostname	Content Type	Size	Filename
41315	1.2.3.110:8080	text/html	40 kB	melinda
41424	1.2.3.110:8080	application/octet-stream	73 kB	payload

Above you can see the files found in the pcap that were transferred via HTTP. Click on any of the files, then *Save* to save them for future analysis or you can click on *Save All* to save all the files.

SMTP Example – Wireshark TCP Stream

1. What is the login and password in this stream?
2. Who is the sender?
3. Who is the recipient?
4. What is the subject of the email?
5. What is the content of the email?

```

EHLO XPCLIENT
250-exchdc1.dotnetzone.com Hello [XP-CLIENT]
250-XEXCH50
250-HELP
250-ETRN
250-DSN
250-SIZE 0
250-AUTH LOGIN
250-AUTH=LOGIN
250-STARTTLS
250 TLS
AUTH LOGIN
334 VXNlcm5hbWU6
c2ltb24=
334 UGFzc3dvcmQ6
cGFzc3dvcmQ=
235 LOGIN authentication successful
MAIL FROM: <Simon@dotnetzone.com>
250 OK - mail from <Simon@dotnetzone.com>
RCPT TO: <Simon@dotnetzone.com>

```

250 OK - Recipient <Simon@dotnetzone.com>
DATA
354 Send data. End with CRLF.CRLF
Message-ID: <000d01c62923\$ab372570\$0101a8c0@XPCLIENT>
From: "TEST-Imap" <Simon@dotnetzone.com>
To: <Simon@dotnetzone.com>
Subject: Test#2
Date: Sat, 4 Feb 2006 00:40:54 -0000
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----=_NextPart_000_000A_01C62923.A7B94950"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----=_NextPart_000_000A_01C62923.A7B94950

Content-Type: text/plain;

charset="koi8-r"

Content-Transfer-Encoding: quoted-printable

Test #2

-----=_NextPart_000_000A_01C62923.A7B94950

Content-Type: text/html;

charset="koi8-r"

Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<HTML><HEAD>

<META http-equiv=3DContent-Type content=3D"text/html; charset=3Dkoi8-r">

<META content=3D"MSHTML 6.00.2900.2523" name=3DGENERATOR>

<STYLE></STYLE>

</HEAD>

<BODY bgColor=3D#ffffff>

<DIV>Test #2</DIV></BODY></HTML>

-----=_NextPart_000_000A_01C62923.A7B94950-

HTTP Example – Wireshark TCP Stream

1. What is the URL that was requested?
2. What browser was used to view this page?
3. What Operating System was used?
4. What was the referring page?
5. What error did the server return?

GET /maint HTTP/1.1

Host: 172.25.105.40

User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.9)

Gecko/20100401 Ubuntu/9.10 (karmic) Firefox/3.5.9

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

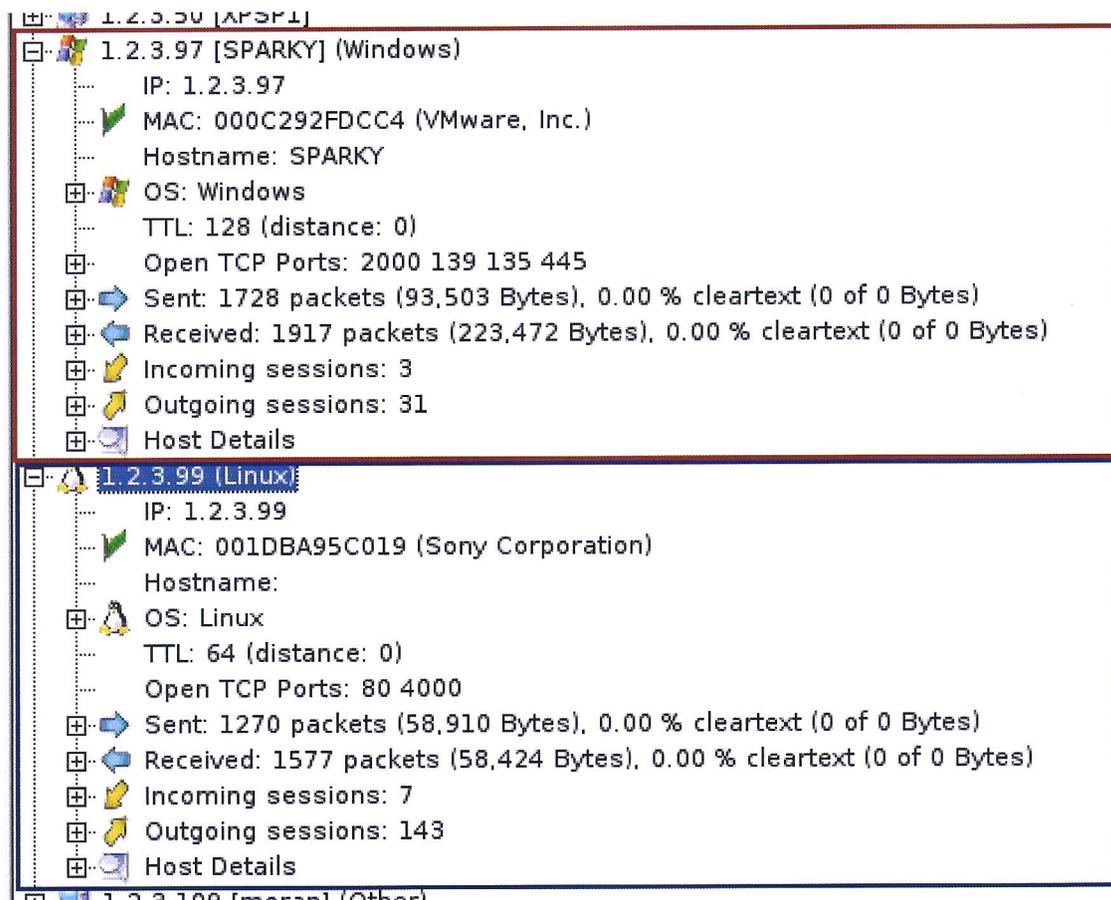
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://172.25.105.40/user/
Cookie: lng=en; PHPSESSID=kkicr6bb10ae3h0ejnlk2ucdm1
Cache-Control: max-age=0

HTTP/1.1 401 Authorization Required
Date: Sat, 01 May 2010 18:13:49 GMT
Server: Apache/2.2.3 (CentOS)
WWW-Authenticate: Basic realm="Restricted Area"
Content-Length: 479
Connection: close
Content-Type: text/html; charset=iso-8859-1

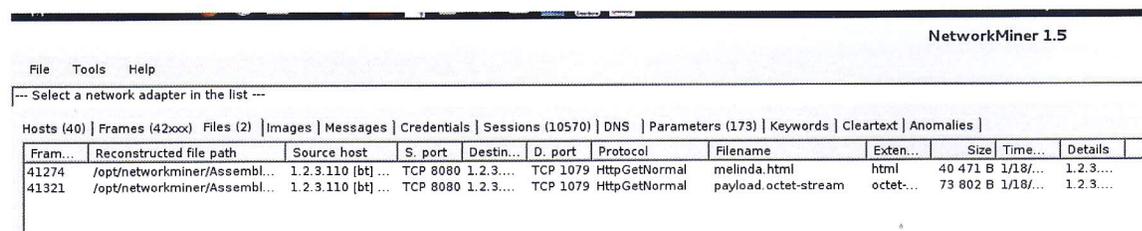
```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Authorization Required</title>
</head><body>
<h1>Authorization Required</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.2.3 (CentOS) Server at 172.25.105.40 Port
80</address>
</body></html>
```

Network Miner

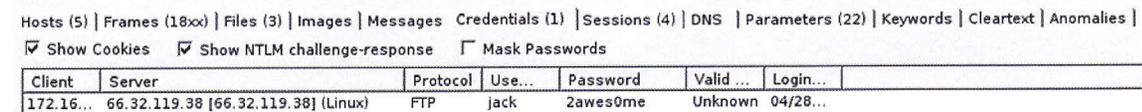
The “**Hosts**” tab displays all hosts involved in the pcap file. Network Miner will do host identification, OS resolution, session identification.



The “Files” tab displays all files found in the pcap file. These files can be downloaded for further examination.



The “credentials” tab will display any usernames and passwords found in the pcap file. Network miner will decode any encoded password.



Hands On-Exercises

Exercise 1: Find the Conversations using Wireshark and Tshark

Goals:

Use Wireshark and Tshark to identify conversations in a pcap.

Using Wireshark

1. Using Wireshark, open the pcap file:
 - a) /root/Desktop/pcap_files/forensic-pcaps/netforensics_evidence02.pcap
2. Click on Statistics -> Conversations
 - a) How many conversations are there?
 - i) IP 6
 - ii) TCP 2
 - iii) UDP 7

Using Tshark

Tshark uses the -z conv,<protocol> argument where the <protocol> can be:

ip IPv4 addresses

ipv6 IPv6 addresses

tcp TCP/IP socket pairs Both IPv4 and IPv6 are supported

udp UDP/IP socket pairs Both IPv4 and IPv6 are supported

3. To find IP conversations run the following command

```
tshark -q -z conv,ip -r /root/Desktop/pcap_files/forensic-pcaps/netforensics_evidence02.pcap
```

4. Repeat the above command substituting tcp and udp for ip.

5. You can output the tshark results to a text file by running the following command.

```
tshark -q -z conv,ip -r /root/Desktop/pcap_files/forensic-pcap/netforensics_evidence02.pcap >
```

6. How does the results compare with the information from Wireshark?
7. What do you think is the importance of seeing the conversations?

Exercise 2: Ann Skips Bail

File: /root/Desktop/pcap_files/forensics-pcaps/netforensics_evidence02.pcap

After being released on bail, Ann Dercover disappears. Fortunately, investigators were carefully monitoring her network activity before she skipped town.

“We believe Ann may have communicated with her cohort, Mr. X, before she left,” says the police chief. “The packet capture may contain clues to her whereabouts.”

You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence.

NOTE: You will use Network Miner for this Exercise

1. Open the pcap in NetworkMiner.
 - a. How many email messages are in this pcap?
 - b. How many files are in this pcap
 - c. How many hosts are involved?
 - d. What are the Operating systems used by the hosts? You can summarize by OS.
2. What is Ann’s email address?
3. What is Ann’s cohort’s email address? (hint: second email)
4. What two items did Ann tell her cohort to bring?
5. What is the NAME of the attachment Ann sent to her cohort?

Extra Credit

6. What is Ann’s email password? (hint: Network Miner)
7. In what CITY and COUNTRY is their rendezvous point?

Exercise 3: Ms. Moneymany's Mysterious Malware.

File: /root/Desktop/pcap_files/forensics-pcaps/netforensics_evidence05.pcap

The scenario:

It was a morning ritual. Ms. Moneymany sipped her coffee as she quickly went through the email that arrived during the night. One of the messages caught her eye, because it was clearly spam that somehow got past the email filter. The message extolled the virtues of buying medicine on the web and contained a link to the on-line pharmacy. "Do people really fall for this stuff?" Ms. Moneymany thought. She was curious to know how the website would convince its visitors to make the purchase, so she clicked on the link.

The website was slow to load, and seemed to be broken. There was no content on the page. Disappointed, Ms. Moneymany closed the browser's window and continued with her day.

She didn't realize that her Windows XP computer just got infected.

You are the forensic investigator. You possess the network capture (PCAP) file that recorded Ms. Moneymany's interactions with the website. Your mission is to understand what probably happened to Ms. Moneymany's system after she clicked the link. Your analysis will start with the PCAP file and will reveal a malicious executable.

NOTE: You will use NetworkMiner and Wireshark for this exercise.

1. As part of the infection process, Ms. Moneymany's browser downloaded two Java applets. What were the names of the two .jar files that implemented these applets?
2. What was Ms. Moneymany's user id on her computer? (hint: guid)
3. What was the name of the executable that was downloaded?
4. What was the starting URL of this incident? In other words, on which URL did Ms. Moneymany probably click?

Answer Key

Exercise 2

1. Open the pcap in Network Miner.
 - a. How many email messages are in this pcap? 2
 - b. How many files are in this pcap? 5
 - c. How many hosts are involved? 14
 - d. What are the operating systems used by the hosts? You can summarize by OS – Windows.
2. What is Ann's email address?
 - a. sneakyg33k@aol.com
3. What is Ann's cohort's email address?
 - a. mistersecretx@aol.com
4. What two items did Ann tell her cohort to bring?
 - a. A fake passport and a bathing suit
5. What is the NAME of the attachment Ann sent to her cohort?
 - a. secretrendezvous.docx
6. What is Ann's email password (hint: base64)?
 - a. 558r00lz
7. In what CITY and COUNTRY is their rendez-vous point?
 - a. Playa del Carmen, Mexico

Exercise 3

1. As part of the infection process, Ms. Moneymany's browser downloaded two Java applets. What were the names of the two .jar files that implemented these applets?
q.jar, sdfg.jar
2. What was Ms. Moneymany's user id on her computer?
ADMINISTRATOR
3. What was the name of the executable that was downloaded?
file.exe
4. What was the starting URL of this incident? In other words, on which URL did Ms. Moneymany probably click?
<http://nrtjo.eu/true.php>

Appendix D: More Tshark and TCPdump

For our examples, we will be analyzing the packet capture file *pcap_files/mfsconsoleExercise.pcap*.

Finding the buffer overflow for INL tag-server

Using *tcpdump* and then *tshark* we want to find all of the packets that contain the buffer overflow for the INL tag-server.

Reviewing the ICSCERT bulletin on the INL tag-server, we know the following information:

- Tag server port is 2000
- Normal payload size is 17 bytes thus anything over this size can be considered a buffer overflow.

Before we continue, we need to know how to filter out info from headers

`proto[x:y]` : will start filtering from byte x for y bytes. `ip[2:2]` would filter bytes 3 and 4 (first byte begins by 0)

`proto[x:y] & z = 0` : will match bits set to 0 when applying mask z to `proto[x:y]`

`proto[x:y] & z != 0` : some bits are set when applying mask z to `proto[x:y]`

`proto[x:y] & z = z` : every bits are set to z when applying mask z to `proto[x:y]`

`proto[x:y] = z` : `p[x:y]` has exactly the bits set to z

NOTE: The relational Operators are: >, <, >=, <=, =, !=

Using tcpdump

What we know so far:

- TCP protocol
- port 2000
- payload length > 17 bytes is indicative of a buffer overflow
- **PUSH** flag set (Only packets with data have the **PUSH** flag set, usually)

From the IP header, we can extract the Total Length of the packet and also the length of the IP header.

From the TCP header, we can extract the length of the TCP header.

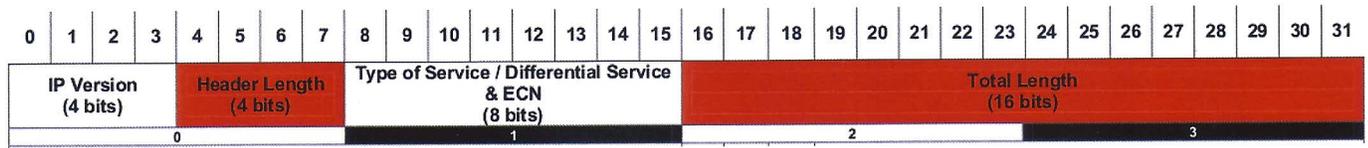
We will need to do some bit/byte masking to get the information we want.

The length of the payload (data) in the packet is then:

$$\text{Payload Length} = \text{Total Packet Length} - (\text{IP Header Length} + \text{TCP Header Length})$$

We can use BPF primitives to extract the necessary data:

From the IP header:



- Total packet length is in bytes 2 -3 of the ip header (**ip[2:2]**)
- Length of IP header is in byte 0 (**ip[0]&0x0f**)*4

NOTE:

The first four bits (0-3) in byte 0 contain 4, since we are using IPv4. The second four bits are the header length in 8-byte WORDS. Normally this value is 5, so the ip header length is 20 bytes.

From the TCP header:



[HINT: An anagram for the TCP flags: Unskilled Attackers Pester Real Security Folk]

- The TCP header length is in the upper 4 bits of byte 12, again expressed as 8-byte words (**tcp[12]&0xf0**)*4
- The **PUSH** flag is bit 4 of byte 13 in TCP header (**tcp[13] & 8 = 8**).

Using a **text editor (e.g gedit)** to create the following BPF expression file. Save the file as **buffer_overflow.bpf**.

```
dst host 1.2.3.97 and
(tcp and port 2000 ) and
(tcp[13] & 8 = 8) and
(ip[2:2] - ((ip[0]&0x0f)*4) + ((tcp[12]&0xf0)*4) > 17)
```

Then run tcpdump as follows in a terminal window:

```
tcpdump -n -A -r pcap_files/msfconsoleExercise.pcap -F buffer_overflow.bpf
```

The **-A** option tells tcpdump to print each packet in ASCII.
(note the output is piped to fold to make it readable!)

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# tcpdump -n -r pcap_files/msfconsoleExercise.pcap -A -F buffer_overflow.bpf | fold -bs -w 100
reading from file pcap_files/msfconsoleExercise.pcap, link-type EN10MB (Ethernet)
14:49:13.312853 IP 1.2.3.110.45873 > 1.2.3.97.2000: Flags [P.], seq 1669353586:1669354157, ack
960812944, win 92, options [nop,nop,TS val 583985 ecr 95620], length 571
E..o._@.@.vW...n...a.l..c.Pr9D.....\.....
-O.=$.}.....@'.....I....F.....).Q..?f.J.*.%..t..(.4B,.<7Kg..
.....t$....1w
...]$....5Nq
Q9...Y...K|R.[.6+.Z..Ts.
....i.Ir...T'u..`h..9..N.....+.....:Wp1.0...n/~,8D.....'.I."..^.....n...r/.,W.....{(n.....v.
.....f.O.....MPl
.....o.....9..Um..|..K$....t...$.ds/.ZcP.....)v.....{...-DjRt.....)F.2.....Y...;.....>.&.j.q
....+...{.}V...
.|H...eG!..M....."!....9p.k.i..h....=pG.v7|%x=..g.B.....z..f-...0.K<@./.....C.,.G.N
...%5.=..?7....4g.I...B*.GN.,F$.@...
16:00:00.623258 IP 1.2.3.109.53508 > 1.2.3.97.2000: Flags [P.], seq 765614453:765615024, ack
1933571008, win 5840, length 571
E..c.&@.H...m...a....-Yus?.P...j...SYNC5.....{.t4.y$.<...z...).$......%aw<.9.C.....Fv
.@.5?J-K.....g.H/.=A.f..NOG...t$.Z1..K.#.x1z.....0.....q.....,Jvu.{...xa.
...'.Qq...?'"...tq.;.p.&b .-...p..m.R...'\...z}.p.A..i1.....n...o..E.9,..N'....
...`.....Ic7Yl...J`...1G..!/(..).F.s....K.s.yk/.1..`5.M.....@...G`8.....G...G.....*Fc....PY
.....nPN.|.....6u-T..z..9LOAl.F...7.A.]...L....?....r....."##dRLG...}5.i....).GF.
..gH2.
I..f..=%...-...J..0..?.....K.$/.w.....r..0....gF...I.{:..H.4
...-5B.f<'G...
root@kali:~#

```

There are two buffer overflow packets in the pcap. One from **1.2.3.110:45873** and the other from **1.2.3.109:53508**.

Using tshark

Tshark is the command line version of *wireshark*. It can be used in scripts to dissect packet captures where a GUI tool can not be used.

NOTE: See <https://www.wireshark.org/docs/man-pages/tshark.html> or execute `man tshark` at a command prompt for more information on tshark.

You can NOT use BPF capture filters in tshark/wireshark if you are reading pcap capture file. However, I can use **tshark** with **wireshark** display filters to accomplish the same thing. The filter is quite a bit simpler than the BPF equivalent.

(tcp.port == 2000) and (tcp.flags.push == 1) and (data.len > 17)

Here is the output from tshark for the tag server buffer-overflow we just looked at with tcpdump.

```

root@kali:~# cat bufferoverflow.shark
(ip.dst == 1.2.3.97) and (tcp.port == 2000) and (tcp.flags.push == 1) and ( data.len > 17 )
root@kali:~# tshark -n -r pcap_files/msfconsoleExercise.pcap -Y "`cat bufferoverflow.shark`" 2> /dev/null
25 57.705796 1.2.3.110 -> 1.2.3.97 TCP 637 45873 > 2000 [PSH, ACK] Seq=1 Ack=38 Win=5888 Len=571
TSval=583985 TSecr=95620
42701 4305.016201 1.2.3.109 -> 1.2.3.97 TCP 625 53508 > 2000 [PSH, ACK] Seq=1 Ack=38 Win=5840 Len=571

```



List IP conversations with tshark

Listing conversations with tcpdump is a pain! Since tshark is related to wireshark, we can take advantage of its list conversations ability.

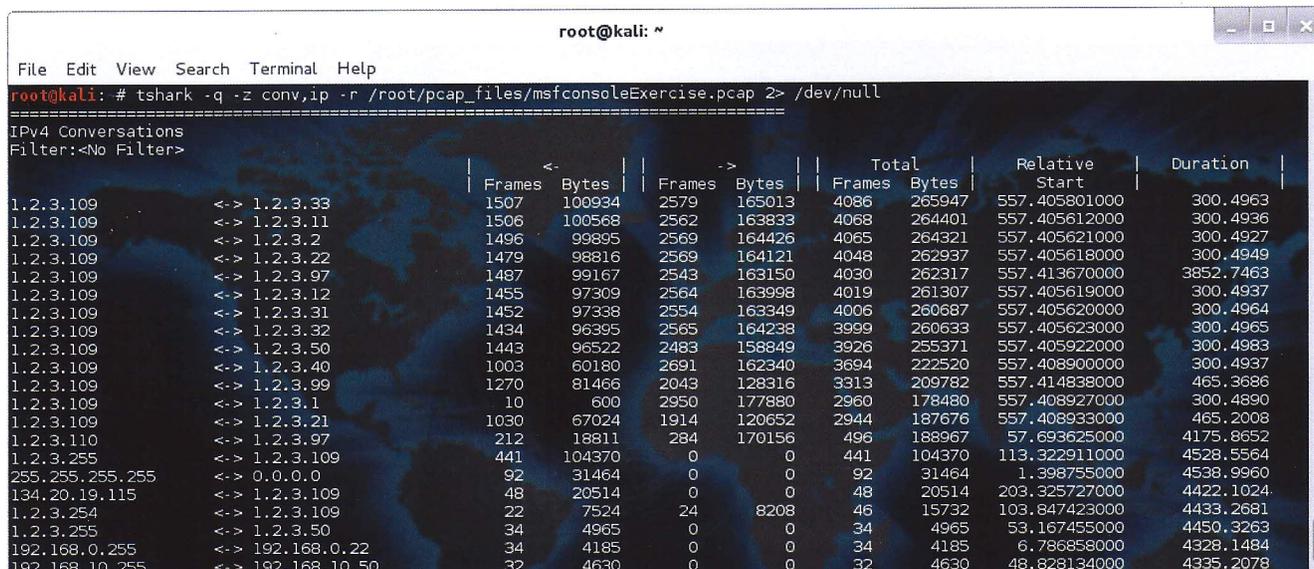
With tshark I can use the `-z conv,<protocol>` argument. The `<protocol>` can be:

- eth Ethernet addresses (MAC address level)
- fc Fibre Channel addresses
- fddi FDDI addresses
- ip IPv4 addresses
- ipv6 IPv6 addresses
- ipx IPX addresses
- tcp TCP/IP socket pairs Both IPv4 and IPv6 are supported
- tr Token Ring addresses
- udp UDP/IP socket pairs Both IPv4 and IPv6 are supported

Run the following command in a terminal window to display all conversations.

```
tshark -q -z conv,ip -r /root/pcap_files/msfconsoleExercise.pcap 2> /dev/null
```

Note: the command writes any error messages to /dev/null aka "no where".



```
root@kali: ~
File Edit View Search Terminal Help
root@kali: # tshark -q -z conv,ip -r /root/pcap_files/msfconsoleExercise.pcap 2> /dev/null
=====
IPv4 Conversations
Filter:<No Filter>
=====
```

		Frames	Bytes	Frames	Bytes	Frames	Bytes	Relative Start	Duration
1.2.3.109	<-> 1.2.3.33	1507	100934	2579	165013	4086	265947	557.405801000	300.4963
1.2.3.109	<-> 1.2.3.11	1506	100568	2562	163833	4068	264401	557.405612000	300.4936
1.2.3.109	<-> 1.2.3.2	1496	99895	2569	164426	4065	264321	557.405621000	300.4927
1.2.3.109	<-> 1.2.3.22	1479	98816	2569	164121	4048	262937	557.405618000	300.4949
1.2.3.109	<-> 1.2.3.97	1487	99167	2543	163150	4030	262317	557.413670000	3852.7463
1.2.3.109	<-> 1.2.3.12	1455	97309	2564	163998	4019	261307	557.405619000	300.4937
1.2.3.109	<-> 1.2.3.31	1452	97338	2554	163349	4006	260687	557.405620000	300.4964
1.2.3.109	<-> 1.2.3.32	1434	96395	2565	164238	3999	260633	557.405623000	300.4965
1.2.3.109	<-> 1.2.3.50	1443	96522	2483	158849	3926	255371	557.405922000	300.4983
1.2.3.109	<-> 1.2.3.40	1003	60180	2691	162340	3694	222520	557.408900000	300.4937
1.2.3.109	<-> 1.2.3.99	1270	81466	2043	128316	3313	209782	557.414838000	465.3686
1.2.3.109	<-> 1.2.3.1	10	600	2950	177880	2960	178480	557.408927000	300.4890
1.2.3.109	<-> 1.2.3.21	1030	67024	1914	120652	2944	187676	557.408933000	465.2008
1.2.3.110	<-> 1.2.3.97	212	18811	284	170156	496	188967	57.693625000	4175.8652
1.2.3.255	<-> 1.2.3.109	441	104370	0	0	441	104370	113.322911000	4528.5564
255.255.255.255	<-> 0.0.0.0	92	31464	0	0	92	31464	1.398755000	4538.9960
134.20.19.115	<-> 1.2.3.109	48	20514	0	0	48	20514	203.325727000	4422.1024
1.2.3.254	<-> 1.2.3.109	22	7524	24	8208	46	15732	103.847423000	4433.2681
1.2.3.255	<-> 1.2.3.50	34	4965	0	0	34	4965	53.167455000	4450.3263
192.168.0.255	<-> 192.168.0.22	34	4185	0	0	34	4185	6.786858000	4328.1484
192.168.10.255	<-> 192.168.10.50	32	4630	0	0	32	4630	48.828134000	4335.2078

List all TCP conversations

```
tshark -q -z conv,tcp -r /root/pcap_files/msfconsoleExercise.pcap 2> /dev/null
```

```
root@kali: ~
```

		<-		->		Total		Relative	Duration
		Frames	Bytes	Frames	Bytes	Frames	Bytes	Start	
1.2.3.110:krb524	<-> 1.2.3.97:socks	107	10381	124	7453	231	17834	1015.479349000	3218.0795
1.2.3.110:http-alt	<-> 1.2.3.97:asprovotalk	44	3180	82	118950	126	122130	1009.878234000	70.5361
1.2.3.110:krb524	<-> 1.2.3.97:ams	35	3290	38	2288	73	5578	57.710903000	531.3555
1.2.3.110:http-alt	<-> 1.2.3.97:amt-esd-prot	18	1285	29	40188	47	41473	4097.506572000	65.4946
1.2.3.99:http	<-> 1.2.3.109:domain	4	240	6	360	10	600	557.418533000	94.6073
1.2.3.110:45873	<-> 1.2.3.97:cisco-sccp	3	247	7	1035	10	1282	57.693625000	0.0131
1.2.3.109:53508	<-> 1.2.3.97:cisco-sccp	4	271	5	865	9	1136	4305.003981000	105.1560
1.2.3.110:krb524	<-> 1.2.3.97:ansoft-lm-1	5	428	4	242	9	670	4098.043169000	0.0147
1.2.3.99:terabase	<-> 1.2.3.109:domain	3	180	6	360	9	540	559.525713000	94.6005
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	569.920454000	0.0014
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	568.668405000	0.0012
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	567.348697000	0.0011
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	566.095304000	0.0011
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	564.842299000	0.0012
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	563.590699000	0.0012
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	561.133954000	0.0011
1.2.3.1:http	<-> 1.2.3.109:domain	2	120	1	60	3	180	559.879516000	0.0013
1.2.3.12:cap	<-> 1.2.3.109:domain	2	120	1	60	3	180	559.373836000	0.0003
1.2.3.109:domain	<-> 1.2.3.33:chargen	1	60	2	120	3	180	559.043686000	0.0001
1.2.3.1:https	<-> 1.2.3.109:domain	2	120	1	60	3	180	558.624455000	0.0013
1.2.3.109:domain	<-> 1.2.3.33:daytime	1	60	2	120	3	180	558.495521000	0.0002

Notice that the *names* of the common ports are displayed instead of the port *number*. Sometimes this can be helpful, but it can cause a lot of unnecessary DNS traffic on your network when tshark resolves all the host ip addresses to host names. The other problem is that the tools guess at what the protocol name is. If you have your own service running on that port (as is the case with the tag server), the port name will not be of value.

To resolve these issues, use the parameter “-n” (“do not resolve”). Here is the same data presented without name resolution.

```
root@kali: ~/Desktop
```

```
root@kali:~/Desktop# !tshark
tshark -q -z conv,tcp -r /root/pcap_files/msfconsoleExercise.pcap -n 2> /dev/null
```

```
=====  
TCP Conversations  
Filter:<No Filter>
```

		<-		->		Total		Relative	Duration
		Frames	Bytes	Frames	Bytes	Frames	Bytes	Start	
1.2.3.110:4444	<-> 1.2.3.97:1080	107	10381	124	7453	231	17834	1015.479349000	3218.0795
1.2.3.110:8080	<-> 1.2.3.97:1079	44	3180	82	118950	126	122130	1009.878234000	70.5361
1.2.3.110:4444	<-> 1.2.3.97:1037	35	3290	38	2288	73	5578	57.710903000	531.3555
1.2.3.110:8080	<-> 1.2.3.97:1082	18	1285	29	40188	47	41473	4097.506572000	65.4946
1.2.3.99:80	<-> 1.2.3.109:53	4	240	6	360	10	600	557.418533000	94.6073
1.2.3.110:45873	<-> 1.2.3.97:2000	3	247	7	1035	10	1282	57.693625000	0.0131
1.2.3.109:53508	<-> 1.2.3.97:2000	4	271	5	865	9	1136	4305.003981000	105.1560
1.2.3.110:4444	<-> 1.2.3.97:1083	5	428	4	242	9	670	4098.043169000	0.0147
1.2.3.99:4000	<-> 1.2.3.109:53	3	180	6	360	9	540	559.525713000	94.6005
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	569.920454000	0.0014
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	568.668405000	0.0012
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	567.348697000	0.0011
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	566.095304000	0.0011
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	564.842299000	0.0012
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	563.590699000	0.0012
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	561.133954000	0.0011
1.2.3.1:80	<-> 1.2.3.109:53	2	120	1	60	3	180	559.879516000	0.0013

Appendix E: Industry-based Information Sharing and Analysis Centers (ISACs)

<http://www.isaccouncil.org/memberisacs.html>

Industry	ISAC	Description
Aviation	Aviation ISAC (A-ISAC)	<p>The Aviation Information Sharing and Analysis Center (A-ISAC) provides an aviation-focused information sharing and analysis function to help protect aviation businesses, operations, and services globally. Our mission is to analyze and share timely, relevant, and actionable information as it pertains to threats, vulnerabilities, and incidents. The A-ISAC is a non-profit organization and membership is open to trusted private sector companies engaged in aviation business globally.</p>
Defense Industrial Base	DIB-ISAC	<p>The DIB ISAC was created to address an all hazards approach to securing the DIB Supply Chain. Trusted and effective Threat Collaboration is a critical component of the DIB ISAC deliverable to its member firms and it is essential that the ISAC provide the member firms' cyber analyst or security officers a broad, multi-sector view of emerging threats that may extend well beyond the analyst's respective organizational domain. DIB ISAC analyst threat intelligence sharing and collaboration is made possible within their respective firm (intra-organization), amongst like organizations which comprise the DIB ISAC (intra-sector), across multiple and diverse industry sectors (cross-sector), and between private and public sector organizations. The DIB ISAC use of a proven Threat Collaboration platform provides the highly secure, real-time trust bridge through which participating analysts are able to anonymously share threat intelligence with their industry and government peers. Using The ISAC's Platform, the DIB ISAC participating firm's cyber analysts and security officers leverage the scale and expertise of the extended analyst community to identify and evaluate emerging threats while collectively developing actionable plans to defeat those threats. The DIB ISAC uses a regional outreach to ensure that tier two and Three companies receive actionable threat intelligence and can also share such intelligence with partner firms. The ISAC also provides assistance in responding to and recovery from manmade and natural disasters.</p>

Industry	ISAC	Description
Emergency Services	Emergency Management & Response ISAC (EMR-ISAC)	The mission of the EMR ISAC is to collect and analyze critical infrastructure protection and resilience information having potential relevance for Emergency Services Sector departments and agencies and to synthesize and disseminate the information to leaders, owners, and operators of the emergency services.
Electric Sector	Electric Sector ISAC (ES-ISAC)	The ES-ISAC serves the Electricity Sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures. It is the job of the ES-ISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants take protective actions.
Financial Services (Global)	Financial Services ISAC (FS-ISAC)	The FS-ISAC is the only industry forum for collaboration on critical security threats facing the financial services sector. When attacks occur, early warning and expert advice can mean the difference between business continuity and widespread business catastrophe. Members of the Financial Services Information Sharing and Analysis Center (FS-ISAC) receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber security threats.
Information Technology	Information Technology ISAC (IT-ISAC)	The Information Technology Information Sharing and Analysis Center (IT-ISAC) is a trusted community of security specialists from companies across the Information Technology industry dedicated to protecting the Information Technology infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to quickly and properly address them. The IT-ISAC also communicates with other sector specific ISACs, enabling members to understand physical threats, in addition to cyber based threats. Taken together, these services provide members a current and coherent picture of the security of the IT infrastructure.

Industry	ISAC	Description
Maritime	Maritime Security ISAC	The Maritime Security ISAC, is a non-profit, member driven organization representing ocean carriers, cruise lines, port facilities and terminals, logistics providers, importers, exporters and related maritime industries throughout the world. Our mission is to advance the security of the United States and the international maritime community by representing maritime interests before government bodies; acting as liaison between industry and government; disseminating timely information; encouraging and assisting in the development of industry-specific technologies; and convening educational and informational conferences for our membership and government partners.
Local and State Governments	Multi-State ISAC (MS-ISAC)	The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a collaborative state and local government-focused cyber security entity that is significantly enhancing cyber threat prevention, protection, and response and recovery throughout the states of our nation. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cyber security readiness and response in each state/territory and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between and among the states, territories and with local government
Communications	Communications ISAC (NCC)	The Communications ISAC mission is to facilitate voluntary collaboration and information sharing among government and industry in support of Executive Order 12472 and the national critical infrastructure protection goals of Presidential Decision Directive 63 (PDD-63); to gather information on vulnerabilities, threats, intrusions, and anomalies from multiple sources and perform analysis with the goal of averting or mitigating impact upon the telecommunications infrastructure.
Healthcare	National Health ISAC (NH-ISAC)	The NH-ISAC serves to protect the nation's healthcare and public health critical infrastructure against security threats and vulnerabilities. The mission of the NH-ISAC is to ensure and preserve the public trust by advancing the integrity and cybersecurity protection of the nation's healthcare and public health sector's critical infrastructure.

Industry	ISAC	Description
Nuclear	Nuclear Energy Institute (NEI)	The Nuclear Energy Institute (NEI) is the policy organization of the nuclear energy and technologies industry and participates in both the national and global policy-making process. NEI's objective is to ensure the formation of policies that promote the beneficial uses of nuclear energy and technologies in the United States and around the world
Oil and Gas	ONG-ISAC	ONG-ISAC is the central reservoir of cyber threat information for the oil and natural gas industry. It protects the industry's exploration and production, transportation, refining, and delivery systems from cyber-attacks through the analysis and sharing of timely and trusted cyber intelligence. As an industry owned and operated organization, ONG-ISAC provides a pipeline for members to share information anonymously across its membership, increasing the speed, quality, and flow of cyber intelligence.
Public Transit	Public Transit ISAC (PT-ISAC)	The PT-ISAC is a trusted, sector-specific entity which provides to its constituency a 24/7 Security Operating Capability that established the sector's specific information/intelligence requirements for incidences, threats and vulnerabilities. Based on its sector-focused subject matter analytical expertise, the ISAC then collects, analyzes, and disseminates alerts and incident reports It provides to its membership and helps the government understand impacts for their sector. It provides an electronic, trusted ability for the membership to exchange and share information on all threats, physical and cyber, in order to defend public transportation systems and critical infrastructure. This includes analytical support to the Government and other ISACs regarding technical sector details and in mutual information sharing and assistance during actual or potential sector disruptions, whether caused by intentional or natural events.

Industry	ISAC	Description
Real Estate ISAC (RE-ISAC)	Real Estate ISAC	<p>Since the World Trade Center Attacks in September 2001, high-profile office properties, apartment buildings, shopping malls and hotels all have been identified as potential terrorist targets at one time or another. In response, industry organizations have worked with government officials to prevent, detect and respond to terrorist threats and malicious incidents. The Real Estate ISAC, a not-for-profit organized by The Real Estate Roundtable and announced in February 2003, represents both a coordinated and an elevated response to these issues. The ISAC is a public-private partnership between the U.S. real estate industry and federal homeland security officials. The partnership facilitates information sharing on terrorist threats, warnings, incidents, vulnerabilities and response planning - to counter terrorism and protect buildings and the people who occupy and use them.</p>
Research & Education	Research & Education ISAC (REN-ISAC)	<p>The REN-ISAC mission is to aid and promote cyber security operational protection and response within the higher education and research (R&E) communities. The mission is conducted within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large. REN-ISAC serves as the R&E trusted partner for served networks, the formal U.S. ISAC community, and in other commercial, governmental, and private security information sharing relationships.</p>
Supply Chain	Supply Chain ISAC (SC-ISAC)	<p>The Supply Chain ISAC offers the most comprehensive forum for collaboration on critical security threats, incidents and vulnerabilities to the global supply chain. Its mission is to facilitate communication among supply chain dependent industry stakeholders, foster a partnership between the private and public sectors to share critical information, collect, analyze and disseminate actionable intelligence to help secure the global supply chain, provide an international perspective through private sector subject matter experts and help protect the critical infrastructure of the United States.</p>

Industry	ISAC	Description
Surface Transportation	Surface Transportaion ISAC (ST-ISAC)	The ST-ISAC was formed at the request of the Department of Transportation. The ISAC provides a secure cyber and physical security capability for owners, operators and users of critical infrastructure. Security and threat information is collected from worldwide resources, then analyzed and distributed to members to help protect their vital systems from attack. The ISAC also provides a vehicle for the anonymous or attributable sharing of incident, threat and vulnerability data among the members. Members have access to information and analytical reporting provided by other sources, such as the U.S. and foreign governments; law enforcement agencies, technology providers and international computer emergency response teams (CERTs).
Water	WaterISAC	The Water Information Sharing and Analysis Center (WaterISAC) was authorized by Congress in 2002 and created and managed by the water sector. Its mission is to keep drinking water and wastewater utility managers informed about potential risks to the nation's water infrastructure from contamination, terrorism and cyber threats. The mission has been expanded to help utilities respond to and recover from all hazards. Funded by subscriber fees and matching federal funds, WaterISAC links members through a secure online portal. The subscriber base includes water utilities and state and federal agencies dealing with security, law enforcement, intelligence, the environment and public health.

Appendix F: WHO TO CONTACT

For training-related questions	cssp_training@hq.dhs.gov
For general ICS-related cyber activity	ics-cert@hq.dhs.gov
For general ICS questions	OPA@hq.dhs.gov
To request access to the ICS-CERT secure portal	ics-cert@hq.dhs.gov
To report an ICS incident	ics-cert@hq.dhs.gov
To report an ICS software vulnerability	ics-cert@hq.dhs.gov
To request a copy of the Cybersecurity Evaluation Tool (CSET)	CSET@hq.dhs.gov
To request onsite assistance	CSET@hq.dhs.gov
For Industrial Control Systems Joint Working Group (ICSJWG) inquiries	icsjwg@hq.dhs.gov
ICS-CERT Web site	www.ics-cert.us-cert.gov
ICS-CERT Cybersecurity Operations Center	(877) 776-7585
National Cybersecurity and Communications Integration Center (NCCIC)	(888) 282-0870 or info@us-cert.gov

Appendix G: ACRONYM LIST

ACE	Arbitrary Code Execution
ACK	TCP header bit – Acknowledge
ACL	Access Control List
AD	Active Directory
AE	Alarms and Events
AIX	IBM Advanced Interactive eXecutive operating system
ALDS	Application Log Detection System
AMD	Advanced Micro Devices, Inc.
API	Application Programming Interfaces
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
AS	Automation System
ASCII	American Standard Code for Information Interchange
ASLR	Address Space Layout Randomization
ATM	Asynchronous Transfer Method
BASE	Basic Analysis and Security Engine
BIOS	Basic Input/Output System boot loader
Botnet	Collection of Internet connected programs that communicate to perform tasks
BPF	Berkeley Packet Filter
BPL	Broadband over Power Line
BSD	Berkeley Software Distribution Unix operating system derivative
CDMA	Code Division Mobile Access
CERT	Computer Emergency Response Team
CIP	Common Industrial Protocol
COM	Component Object Model
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CPX	Common Complex Data
CSET	Cyber Security Evaluation Tool
CVE	Common Vulnerabilities and Exposures
DA	Data Access
DARPA	Defense Advanced Research Projects Agency (formally ARPA)
DCOM	Distributed Component Object Model
DCS	Distributed control system
DDoS	Distributed Denial of Service



DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DMS	Distributed Management System
DMZ	Demilitarized Zone
DNP3	Distributed Networking Protocol 3.0
DNS	Domain Name System
DoS	Denial of Service
DX	Data eXchange
EMS	Energy Management System
FCC	Federal Communications Commission
FEP	Front-End Processor
FIN	TCP header bit – no more data from sender
FTP	File Transfer Protocol
GMS	Generation Management System
GPL	General Public License
GPO	Group Policy Objects
GSM	Global System for Mobile communications
GUI	Graphic User Interface
HAD	Historical Data Access
HD	Host Discovery
HIDS	Host Intrusion Detection System
HMI	Human-Machine Interface
HP	Hewlett Packard
HTTP	Hypertext Transfer (or Transport) Protocol
IANA	Internet Assigned Numbers Authority
ICCP	Inter-Control Center Communications Protocol
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IL	Instruction List
IMAP	Internet Message Access Protocol
I/O	Inputs and Outputs
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export

IPS	Intrusion Prevention System
IRC	Internet Relay Chat
ISO	International Organization for Standardization
iso	Disk archive image
IT	Information Technology
JDLR	Just Doesn't Look Right
LAN	Local Area network
LBNL	Lawrence Berkeley National Laboratory
LD	Ladder Diagram
LO	Learning Objective
MAC	Media Access Control
Mac OS X	Apple Macintosh Unix-based Operating System
MBAP	Modbus Application Protocol
MMC	Microsoft Management Console
MMS	Manufacturing Message Specification
Modicon	Modular Digital Controller
MS	Metasploit
MSF	Metasploit Framework
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
Netflow	Network Flow Data
NIC	Network Interface Card
NIDS	Network Intrusion Detection Systems
Nmap	Network Mapper
NTP	Network Time Protocol
NVT	Network Vulnerability Test
ODVA	Open DeviceNet™ Vendors Association
OLE	Object Linking and Embedding
OPC	Object Linking and Embedding for Process Control
OPC-UA	Object Linking and Embedding for Process Control – Unified Architecture
OpenVAS	Open Vulnerability Assessment System
OS	Operating System
OSI	Open Systems Interconnection
OSII	Open Systems International Incorporated
OU	Organizational Unit
PAC	Process Automation Controller
PCAP	Packet Capture
PCS	Process Control System



PHP	Hypertext Preprocessor
P&ID	Process and Instrumentation Diagram
PID	Proportional-Integral-Derivative
PID	OS Process Identifier
PLC	Programmable Logic Controllers
POP	Post Office Protocol
PS	Port Scanning
RARP	Reverse Address Resolution protocol (obsolete)
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RFC	Request for Comments
RPC	Remote Procedure Call
RST	TCP header bit – reset the connection
RTU	Remote Terminal/Telemetry Unit
SAL	Security Access Level
SCADA	Supervisory Control and Data Acquisition
SFC	Sequential Function Charts
SIS	Safety Instrumental System
SLA	Service (or Security) Level Agreement
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Security Sockets Layer
ST	Structured Text
SYN	TCP headerbit – Synchronize sequence numbers
SYSLOG	Standard for computer message logging exchange
TASE.1	Tele-control Application Service Element-1
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	Unified Architecture
UCA	Utility Communications Architecture
UCS	Utility Communications Specification
UDP	User Datagram Protocol
URL	Uniform (or universal) resource locator
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network

WAN Wide Area Network
XD eXecute Disable
Xi eXpress interface
XMLDA Extensible Markup Language Data Access

Last updated 1/4/2016 with revision 4 modification 03.