HAKIN9 ON DEMAND

Vol.1 No.7
Issue 07/2012(7) ISSN: 1733-7186

WIRESHARK
SHARKS ON THE WIRE

SPECIAL PUBLICATION 70+ PAGES

BOB BOSEN ON WIFI COMBAT ZONE

STEVE WILLIAMS DESCRIBES HOW TO CAPTURE/DECODE 802.11 TRAFFIC

WILLIAM F. SLATTER III SHOWS HOW TO SOLVE "ATTRIBUTION PROBLEM"

HAI LI DISCUSSES ANALYZING A WIRELESS PROTOCOL

PLUS

LEARN MORE ABOUT WIRESHARK!
PEDRO MORENO SANCHEZ AND ROGELIO MARTINEZ PEREZ
SHOWS HOW TO USE COOJA SIMULATOR TOGETHER

Using Wireshark

and Other Tools to as an Aid in Cyberwarfare and Cybercrime

Attempting to Solve the "Attribution Problem" – Using Wireshark and Other Tools to as an Aid in Cyberwarfare and Cybercrime for Analyzing the Nature and Characteristics of a Tactical or Strategic Offensive Cyberweapon and Hacking Attacks.

One of the main disadvantages of the hyperconnected world of the 21st century is the very real danger that countries, organizations, and people who use networks computer resources connected to the Internet face because they are at risk of cyberattacks that could result in anything ranging from denial service, to espionage, theft of confidential data, destruction of data, and/or destruction of systems and services. As a recognition of these dangers, the national leaders and military of most modern countries have now recognized that the potential and likely eventuality of cyberwar is very real and many are preparing to counter the threats of cyberwar with modern technological tools using strategies and tactics under a framework of cyberdeterrence, with which they can deter the potential attacks associated with cyberwarfare.

What is Cyberwarfare?

During my studies prior to and as a student in this DET 630 – Cyberwarfare and Cyberdeterrence course at Bellevue University, it occurred to me that considering the rapid evolution of the potentially destructive capabilities of cyberweapons and the complex nature of cyberdeterrence in the 21st century, it is now a critical priority to integrate the cyberwarfare and cyberdeterrence plans into the CONOPS plan. Indeed, if the strategic battleground of the 21st century has now expanded to include cyberspace, and the U.S. has in the last five years ramped up major military commands, training, personnel, and capabilities to support cyberwarfare and cyberdeterrence capabilities, the inclusion of these capabilities should now be a critical priority of the Obama administration if has not already happened.

How large a problem is this for the United States?

Without the integration of cyberwarfare and cyberdeterrence technologies, strategies, and tactics into the CONOPS Plan, the national command authorities run a grave risk of conducting a poorly planned offensive cyberwarfare operation that could precipitate a global crisis, impair relationships with its allies, and potentially unleash a whole host of unintended negative and potentially catastrophic consequences. In non-military terms, at least four notable cyberspace events caused widespread damages via the Internet because of the rapid speed of their propagation, and their apparently ruthless and indiscriminant selection of vulnerable targets. They are 1) the Robert Morris worm (U.S. origin, 1988); 2) the ILOVEYOU worm (Philippines origin, 2000); the Code Red worm (U.S. origin, 2001); and the SQL Slammer worm (U.S. origin, 2003). If not executed with great care and forethought, a cyberweapons could potentially unleash even greater damage on intended targets and possible on unintended targets that were connected via the Internet.

Other Not So Obvious Challenges for Cyberweapons and Cyberdeterrence

The cyberspace threat and vulnerability landscape is notable in that it is continually dynamic and shifting. Those who are responsible for protecting assets in cyberspace have many more challenges on their hands than their military counterparts who utilize weapons like guns, explosives, artillery, missiles, etc. For example, there are by some estimates over 350 new types of malware that are manufactured each month. There are also monthly patch updates to most Microsoft software and operating systems, and phenomena such as evil hackers and zero-day exploits are apparently never ending. Therefore, the inclusion of cyberweapons and cyberdeterrence capabilities into the CONOPS Plan would require more frequent, rigorous, complex, and integrated testing to ensure that it was always effective and up to date. In the dynamic world of cyberspace with it's constantly shifting landscape of new capabilities, threats and vulnerabilities, the coordination of the constant refresh and testing of a CONOPS Plan that integrated these cyberwarfare and cyberdeterrence capabilities would be no small feat. In addition, constant intelligence gathering and reconnaissance would need to be performed on suspected enemies to ensure that our cyberweapons and cyberdeterrence capabilities would be in constant state of being able to deliver the intended effects for which they were designed.

Is it a problem for other countries?

The careful planning and integration of cyberweapons and cyberdeterrence is likely a challenge for every country with these capabilities. For example, much is already known about our potential adversaries, such as Russia, China and North Korea, but what is perhaps less understood is the degree to which they have been successful in integrating cyberwarfare and cyberdeterrence capabilities into their own national war plans. Nevertheless, due to the previous extensive experience of Russia and the U.S. with strategic war planning, it is more likely that each of these countries stand the greatest chance of making integrating cyberwarfare and cyberdeterrence capabilities into their respective war plans. Yet, as far back as June 2009, it was clear that the U.S. and Russia were unable to agree on a treaty that would create the terms under which cyberwarfare operations could and would be conducted (Markoff, J. and Kramer, A. E., 2009).

Is it problematic for these countries in the same ways or is there variation? What kind?

Every country that is modern enough to have organizations, people, and assets that are connected to computers and the Internet faces similar challenges of planning and managing cyberweapons and cyberdeterrence, and the poorer the country, the more significant the challenges. For example, when a small group of hackers from Manila in the Philippines unleashed the ILOVEYOU worm on the Internet in 2000, it caused over $2 billion in damages to computer data throughout the world. Agents from the FBI went to Manila to track down these people and investigate how and why the ILOVEYOU worm catastrophe occurred. To their surprise, they learned that each of these hackers who were involved could successfully escape prosecution because there were no laws in the Philippines with which to prosecute them. So actually most countries lack the technological and legal frameworks with which to successfully build a coordinated effort to manage the weapons and strategies of cyberwarfare and cyberdeterrence, despite the fact that most now embrace cyberspace with all the positive economic benefits it offers for commerce and communications.

What are the consequences to the U.S. and others if this threat is left unchecked?

As stated earlier, without the careful integration of cyberwarfare and cyberdeterrence technologies, strategies, and tactics into the CONOPS Plan, the national command authorities run a grave risk of launching a poorly planned offensive cyberwarfare operation that could precipitate a global crisis, impair relationships with its allies, and potentially unleash a whole host of unintended negative and potentially catastrophic consequences.

What consequences has the threat already produced on American/global society?

I believe that yes, the absence of well-defined cyberwarfare and cyberdeterrence strategies and tactics in the CONOPS Plan has already produced some situations that have either damaged America's image abroad, or that could imperil its image and have far more negative consequences. For example, operates such as Stuxnet, Flame, Duque, etc., might have either been better planned or possibly not executed at all if cyberwarfare and cyberdeterrence strategies and tactics were defined in the CONOPS Plan. Also, the news media indicated during the revolution in Libya that resulted in the fall of Qaddafi, cyberwarfare operations were considered by the Obama administration. The negative reactions and repercussions on the world stage might have far outweighed any short term advantages that could have resulted from a successful set of cyberattacks against Libyan infrastructure assets that were attached to computer networks. Again, a comprehensive CONOPS Plan that included well-defined cyberwarfare and cyberdeterrence strategies and tactics could have prevented such possible cyberattacks from even being considered, and it could have prevented the news of the possible consideration being publicized in the press (Schmitt, E. and Shanker, T., 2011). Without such restraint and well-planned deliberate actions, the U.S. runs the risk of appearing like the well-equipped cyber bully on the world stage, and an adversary who is willing to unleash weapons that can and will do crippling damage to an opponent, using technologies that are rapid, decisive, and not well-understood by those for whom they are intended. A similar effect and world reaction might be if U.S. Army infantry troops were equipped with laser rifles that emitted deadly laser blasts with pinpoint precision across several hundred yards.

Has this threat evolved or changed over time or is it relatively constant? If it has evolved or changed, exactly how has that change happened and what political consequences have emerged from them?

The threat has certainly rapidly evolved over time. Since Stuxnet was released in 2010, countries and the general public are now aware of some of the offensive, strategic and destructive capabilities and potential of cyberweapons (Gelton, T., 2011).

The changes that produced Stuxnet and other recent, more modern cyberweapons were a national resolve to excel in the cyberwarfare area, coupled with excellent reconnaissance on desired targets, and partnering with computer scientists in Israel. The political consequences are not well understood yet, except to say that the U.S. and Israel are probably less trusted and suspected of even greater future capabilities, as well as having

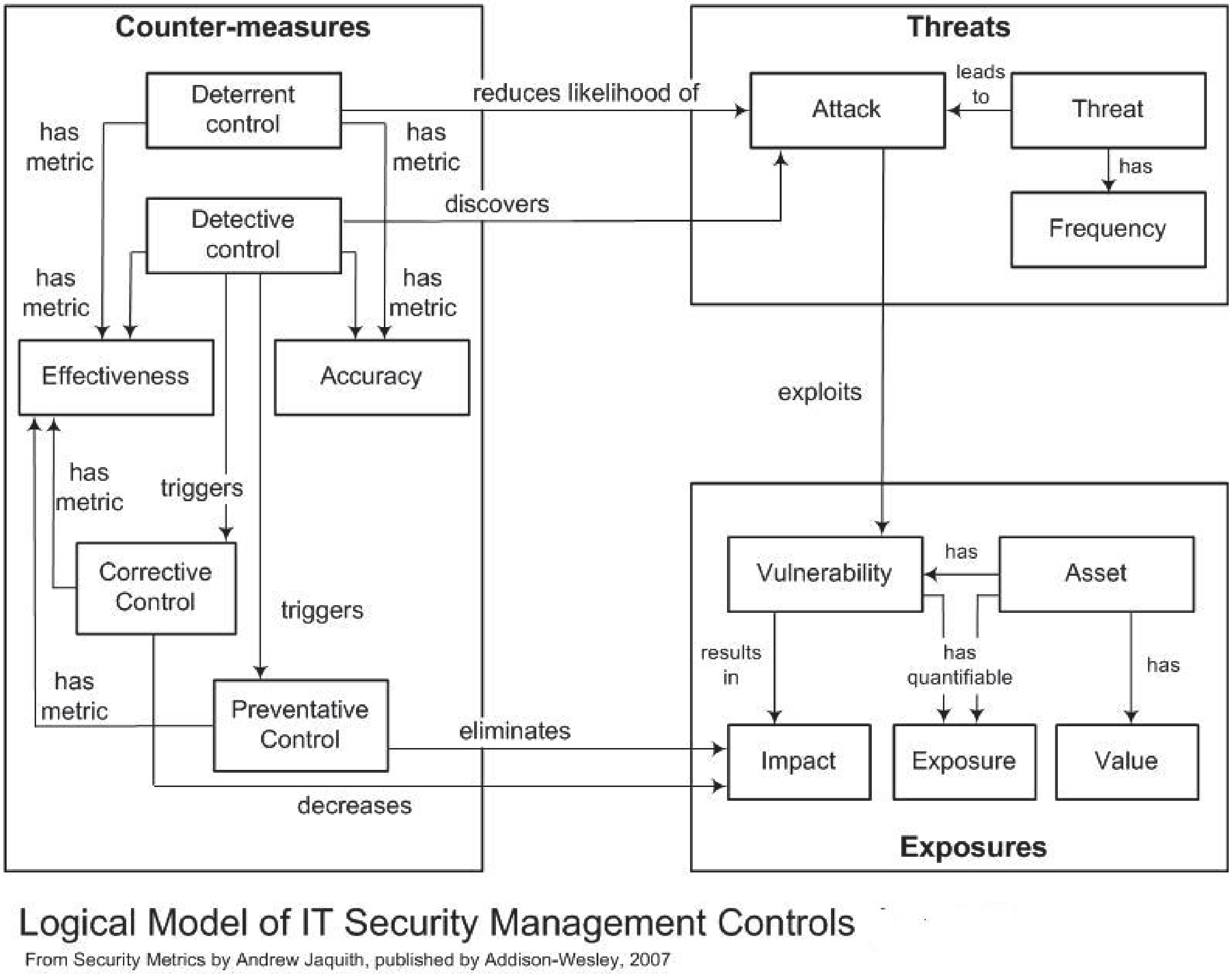
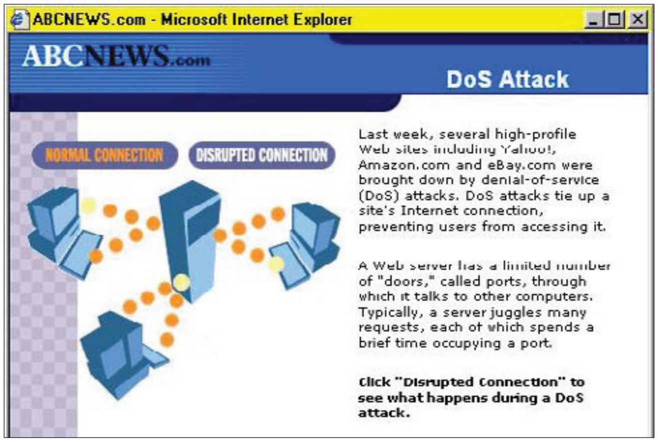


Figure 1. *Logical Model of IT Security Management Controls (Jacquith, 2007)*

the will to use them. Again, having well-planned cyberwarfare and cyberdeterrence strategies and tactics defined in the CONOPS Plan might indeed, restrain such possibly reckless decisions as to unleash cyberweapon attacks without what the world might consider the correct provocation.

Final Thoughts about Cyberwarfare Operations

In the words of Deb Radcliff, in an article published in SC Magazine in September 2012, "we are already in a cyberwar" (Radcliff, D., 2012). But as I was performing my research, it occurred to me that a country like the U.S., might in the future unleash such a devastating cyberattack that it could cripple the enemy's ability to communicate surrender. I think that the moral implications of such circumstances need to be justly considered as a matter of the laws of war, because if a country continues to attack an enemy that has indicated that they are defeated and want to surrender, this shifts the moral ground from which the U.S. may have it was conducting its cyberwarfare operations. This is one other unintended consequence of cyberwarfare and one that needs to be carefully considered.



Last week, several high-profile Web sites including Yahoo!, Amazon.com and eBay.com were brought down by denial-of-service (DoS) attacks. DoS attacks tie up a site's Internet connection, preventing users from accessing it.

A Web server has a limited number of "doors," called ports, through which it talks to other computers. Typically, a server juggles many requests, each of which spends a brief time occupying a port.

Click "Disrupted Connection" to see what happens during a DoS attack.

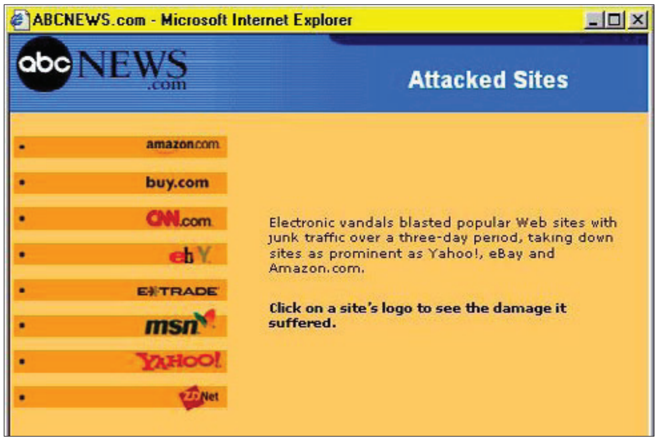
Figure 2. *Denial of Service Attack diagram from ABC news in February 2000*

To further understand the relationship of threats, counter-measures, and exposures in cyberspace, I have included this diagram by Jaquith, shown Figure 1.

The Attribution Problem

One of the most perplexing issues of cyberwarfare and cybercrime is the fact that attackers can and very often will use software and other servers from which to launch their attacks. Because of the way the Internet was designed its end-to-end nature of IP communications using other computers to launch attacks is not that difficult. In fact, the computers that actually perform the attacks are called "zombies" as they are configured with remote control programs that are manipulated by the attackers. The recipients can do forensic analysis and determine which "zombie" computers sent the attacks, however, it is practically impossible to collect the data about who the person or persons that originated the attacks. Thus, it is very difficult to attribute the original cause of the attack, hence the name the "attribution problem." In cyberwarfare, this is particularly difficult, because the National Command Authorities would want to understand to whom and where they should employee the cyberwarfare capable units of the U.S. Military to launch a punishing retaliatory cyberattack.

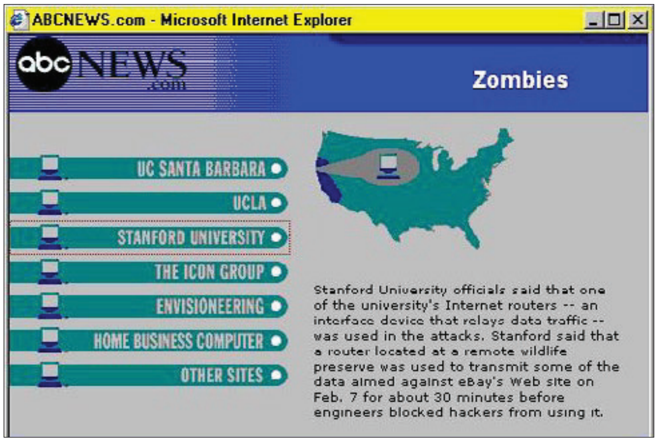
The most common type of attack for "zombie" computers is known as the distributed denial of service attack or DDoS attack. In February 2000, the first sensational wave of DDoS attacks were launched from "zombie" computers that were physically located at major universities in California. The following figures provide some of the details about those attacks and which companies were the targets (Figure 2-4).



Electronic vandals blasted popular Web sites with junk traffic over a three-day period, taking down sites as prominent as Yahoo!, eBay and Amazon.com.

Click on a site's logo to see the damage it suffered.

Figure 3. *Denial of Service Attack Victims diagram from ABC news in February 2000*



Stanford University officials said that one of the university's Internet routers -- an interface device that relays data traffic -- was used in the attacks. Stanford said that a router located at a remote wildlife preserve was used to transmit some of the data aimed against eBay's Web site on Feb. 7 for about 30 minutes before engineers blocked hackers from using it.

Figure 4. *Denial of Service Attack Zombies diagram from ABC news in February 2000*

Recent Cyber Attacks

As recently as September 23, 2012 – September 30, 2012, cyber attacks in the form of distributed *denial of service* (DDOS) attacks from the Middle East against several major U.S. banks based have publicly demonstrated the ire of the attackers and also the vulnerabilities of banks with a customer presence in cyberspace (Strohm and Engleman, 2012).

How do you know?

It's not always intuitively obvious, but if your network is slowing down or computers or other devices attached to your network are acting strangely, you could be under attack. But it's best to use analysis tools to understand what is really going on.

Free Tools You Can Use

This section covers three free tools that you can use to understand network activity on your network in greater detail.

Wireshark

Wireshark is a free, open source packet analysis tool that evolved from its predecessor, Ethereal.

Table 1. *Wireshark Documentation – Packet Analysis Capabilities for Captured Packets*

The menu items of the "Packet List" pop-up menu

Item	Identical to main menu's item:	Description
Mark Packet (toggle)	Edit	Marklunmark a packet.
Ignore Packet (toggle)	Edit	Ignore or inspect this packet while dissecting the capture file.
Set Time Reference (toggle)	Edit	Set/reset a time reference.
Manually Resolve Address		Allows you to enter a name to resolve for the selected address.
Apply as Filter	Analyze	Prepare and apply a display filter based on the currently selected
item.		
Prepare a Filter	Analyze	Prepare a display filter based on the currently selected item.
Conversation Filler	-	This menu item applies a display filter with the address nformationflonitly selected packet. E.g. the IP mein enttywill eta filter to show the trafficbetweenthe two IP addresses of the current packet. XXX - add a new section describing this better.
Cobrize Conversation	-	This menu item uses adisplayfilterwiththe address infounaticei from the selected packet to build a new colorizing rule.
SCTP	-	Allows ycii to analyze and prepare a filter for this SCTP associafion.
Follow TCP Stream	Analyze	Allows you to view all the data on a TCP streambetw een a pair of noles.
Follow UDP Stream	Analyze	Allows you to view all the data on a UDP datazrain stnain b etw een a pair of nodes.
Follow SSL Stream	Analyze	Same as "Follow TCP Sbeanz" but for SSL. XXX - add a new ection descnbing this better.

Copy/ Summary (Text)	-	Copy the surtunny fields as displayed to the clipboard, as tab-separated text.
Copy/ Summary (CSV)	-	Copy the summary fields as displayed to the clipboard, as conuna-separated text.
Copy/ As Filter	-	Prepare a display filterbased on the currently selected item aid copy that filter to tle clipboard.
Copy/ Byter (Offset Hex)	-	Copy the packet bytes to the clipboard in hexdump-like format, butwitlrut the text partion.
Copy/ Byter (Pantable Text Only>)	-	Copy the packet bytes to the clipboard as ASCII text, excludin; non-pzintab le characters.
Copy/ Wier (Hex Stream)	-	Copy the packet bytes to the clipboard as an unpuirtuated list of hex digits.
Copy/ Byter (Binary Stream)	-	Copy the packet bytes to the clipboard as raw binary. The data is stored intly clipboard as MIME-tyre "application/octet-stteam".

Decode As...	Analyze	Change or apply a new relationbetween two dissectors.
Print…	File	Print packets.
Show Packet in New Window	View	Display the selected packet ma new window.

Wireshark is notable for its ability to quickly, capture and display traffic in a real time sequential way, and allow this traffic to be displayed, broken down at the packet level by each level of the OSI model, from the physical layer up through the application layer. The traffic can also shows the senders and the receivers of each packet, and can be easily summarized with the selection of a few menu choices. The first figure below is from a table in the Wireshark documentation, and the figures that follow are from an actual Wireshark session where about 500,000 packets were collected for summarization and analysis. All this data can also be saved for later analysis.

Wireshark will run on both Windows-based platforms and Mac OS X platforms. This is the website location where you can find Wireshark: *http://www.wireshark.org/download.html* (Table 1 and Figure 5-8).

Ostinato

Ostinato is a free, open source-based packet generator that can be used to conduct network experiments, particularly for packet analysis in conjunction with a tool such as Wireshark. It is easy to install, configure and use. Figure 8 shows a screenshot from Ostinato.

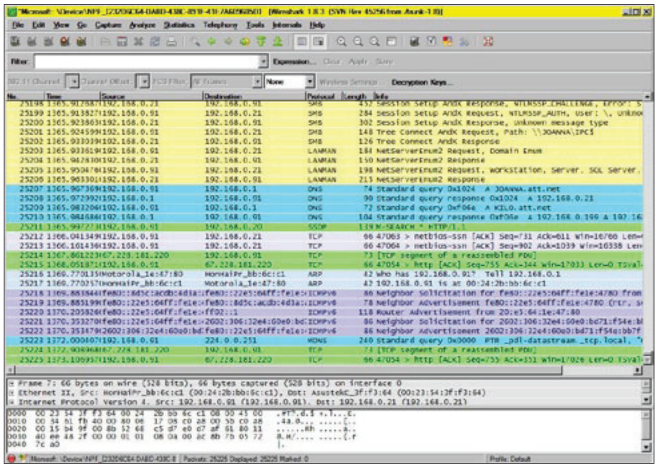


Figure 5. *Wireshark Opening Screenshot after a Network Interface Has Been Selected for Packet Capture*

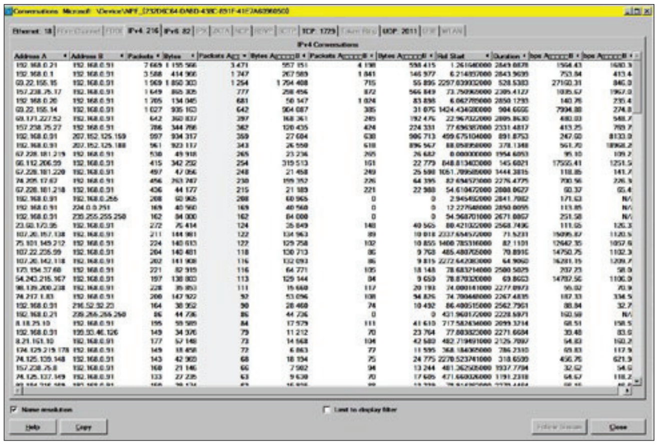


Figure 6. *Wireshark Conversation Analysis Screen*

Ostinato will run on Windows-based platforms and several other platforms. This is the website location where you can find Ostinato: *http://code.google.com/p/ostinato/* (Figure 9).

TCPView

TCPView is an excellent analysis program that shows what is happening on your computer at layer four of the OSI networking model. If you remember, this is where TCP and UDP activities take place. TCPView allows the user to view and sort data by process, PID, protocol (TCP or UDP), local address, remote address, port number, TCP state, sent packets, sent bytes, received packets, and received bytes. The data can also be saved for later analysis.

TCPView was originally written by Mark Russinovich and Bryce Cogswell and was published and distributed for free by their company, Sysinternals. In 2006, Microsoft acquired Sysinternals and TCPView and many other tools that were created by Sysinternals continue to be updated and distributed

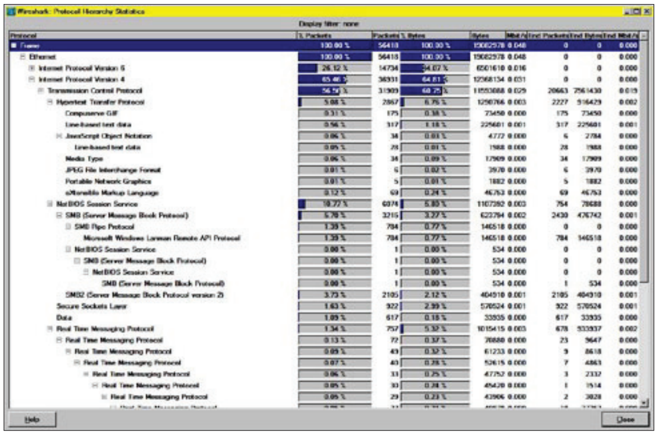


Figure 7. *Wireshark Protocol Analysis Screen*

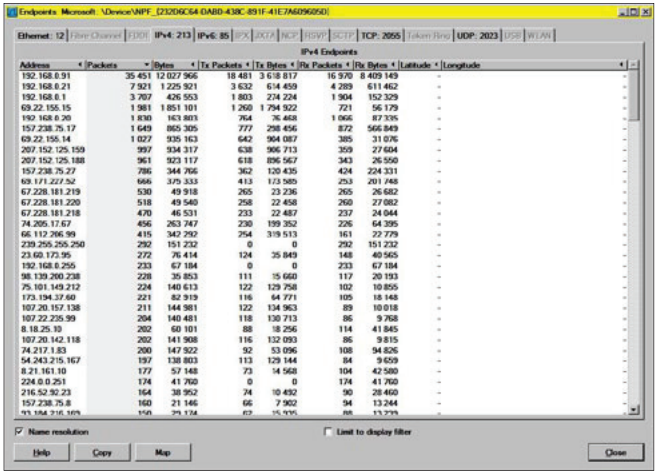


Figure 8. *Wireshark Endpoint Analysis Screen*

by Microsoft for free. TCPView will only run on Windows-based platforms and this is the website location where you can find TCPView and many other great Sysinternals tools: *http://technet.microsoft.com/en-us/sysinternals* (Figure 10).

Traffic to Watch

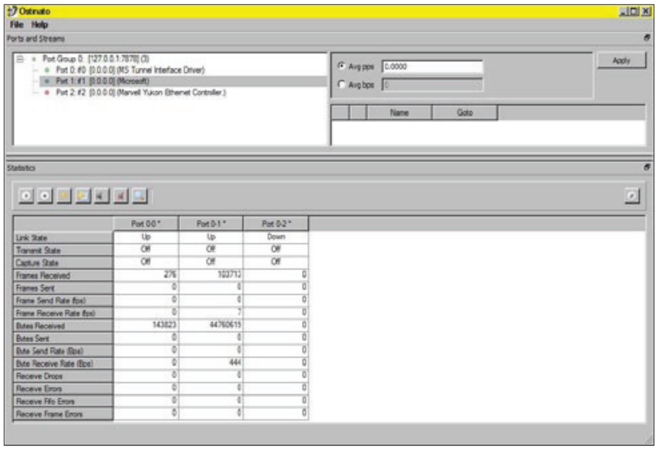
By far the most interesting and dangerous external traffic to watch on most networks is ICMP traffic. ICMP is the Internet Control Messaging Protocol, and there are eight types of ICMP messages. Hackers can easily use ICMP (PING) messages to create DDOS attacked. A tool like Simple Nomad's "icmpenum" can issue ICMP messages such as ICMP_TIMESTAMP_REQUEST and ICMP_INFO and make it possible to map a network inside of a firewall (K, 2011).

Outbound traffic is just as important as inbound traffic if not more so (Geers, 2011). It is not uncommon for programs like botnets to take up residence and open up secure channels to transmit data to remote servers in places like China, Russia, Eastern Europe and even North Korea.

Programs that are unrecognizable should be suspected as possible malware and should be quickly researched to determine if they are hostile. If they cannot be easily identified, that is a bad sign and they should probably be uninstalled.

A Caution to those Who Understand Network Attacks

Title 10 of the U.S. Code forbids U.S. Citizens from taking offensive action against network attackers. Nevertheless, monitoring the evidence and results of unwanted traffic could help you understand it and also help you decide how to improve upon your network defenses (firewall settings for inbound traffic, desktop firewalls, etc.) and even provide evidence to law enforcement authorities.



- Port Group 0: [127.0.0.1:7878] (3)
  - Port 0: #0 [0.0.0.0] (MS Tunnel Interface Driver)
  - Port 1: #1 [0.0.0.0] (Microsoft)
  - Port 2: #2 [0.0.0.0] (Marvell Yukon Ethernet Controller.)

● Avg pps 0.0000

○ Avg bps 0

	Port 0-0 *	Port 0-1 *	Port 0-2 *
Link State	Up	Up	Down
Transmit State	Off	Off	Off
Capture State	Off	Off	Off
Frames Received	276	103713	0
Frames Sent	0	0	0
Frame Send Rate (fps)	0	0	0
Frame Receive Rate (fps)	0	7	0
Bytes Received	143823	44760615	0
Bytes Sent	0	0	0
Byte Send Rate (Bps)	0	0	0
Byte Receive Rate (Bps)	0	444	0
Receive Drops	0	0	0
Receive Errors	0	0	0
Receive Fifo Errors	0	0	0
Receive Frame Errors	0	0	0

Figure 9. *Ostinato Packet Generator Screen*

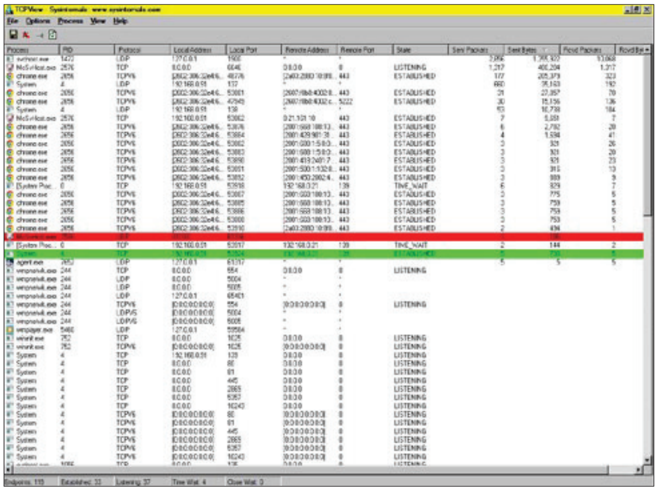
The Future

Without trying to present a gloomy picture of the cyberspace environment that is composed of the Internet and all the computers, smart phones and other devices attached to it, it appears that for the time being, the bad guys far outnumber the good guys and it appears that they are winning. But it is also apparent that that now more free information and free tools are available than ever before. For the foreseeable future, every person who uses the Internet should seek to educate themselves about the dangers in cyberspace and the ways to protect themselves from these dangers.

Conclusion

This article has briefly reviewed the topic of cyberwarfare and presented some information about free network analysis tools that can help you better understand your network traffic.

The good news is that President Obama and his Administration have an acute awareness of the importance of the cyberspace to the American economy and the American military. The bad news is that because we are already in some form of cyberwarfare that appears to be rapidly escalating, it remains to be seen what effects these cyberattacks and the expected forthcoming Executive Orders that address cybersecurity will have on the American people and our way of life. I believe it will be necessary to act prudently, carefully balancing our freedoms with our need for security, and also considering the importance of enabling and protecting the prosperity of the now electronically connected, free enterprise economy that makes the U.S. the envy of and the model for the rest of the world.


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes ▼	Rcvd Packets	Rcvd Byt
svchost.exe	1472	UDP	127.0.0.1	1900	*	*		2,096	1,295,327	11,068	
McSvHost.exe	2576	TCP	0.0.0.0	6646	0.0.0.0	0	LISTENING	1,217	400,204	1,217	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	48776	[2a03:2880:10:8f8...	443	ESTABLISHED	177	205,379	323	
System	4	UDP	192.168.0.51	137	*	*		660	35,163	192	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53001	[2607:f8b0:4002:8...	443	ESTABLISHED	31	27,357	70	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	47949	[2607:f8b0:4002:c...	5222	ESTABLISHED	30	15,156	136	
System	4	UDP	192.168.0.51	138	*	*		53	10,738	184	
McSvHost.exe	2576	TCP	192.168.0.51	53062	8.21.101.10	443	ESTABLISHED	7	5,081	7	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53076	[2001:668:100:13...	443	ESTABLISHED	6	2,792	20	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53064	[2001:428:901:3f...	443	ESTABLISHED	4	1,594	41	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53082	[2001:500:1:5:0:0...	443	ESTABLISHED	3	921	26	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53083	[2001:500:1:5:0:0...	443	ESTABLISHED	3	921	20	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53090	[2001:418:2401:7...	443	ESTABLISHED	3	921	23	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53051	[2001:500:1:132:8...	443	ESTABLISHED	3	915	13	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53052	[2001:450:2002:4...	443	ESTABLISHED	3	889	9	
[System Proc...	0	TCP	192.168.0.51	53918	192.168.0.21	139	TIME_WAIT	6	829	7	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53087	[2001:668:100:13...	443	ESTABLISHED	3	775	5	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53085	[2001:668:100:13...	443	ESTABLISHED	3	759	5	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53086	[2001:668:100:13...	443	ESTABLISHED	3	759	5	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53080	[2001:668:100:13...	443	ESTABLISHED	3	753	5	
chrome.exe	2856	TCPV6	[2602:306:32e4:6...	53910	[2a03:2880:10:8f8...	443	ESTABLISHED	2	494	1	
McSvHost.exe	2576	UDP	0.0.0.0	[illegible]	[illegible]			[illegible]	[illegible]		
[System Proc...	0	TCP	192.168.0.51	53017	192.168.0.21	139	TIME_WAIT	2	144	2	
System	4	TCP	192.168.0.51	52524	192.168.0.21	139	ESTABLISHED	5	730	5	
agent.exe	7652	UDP	127.0.0.1	61317	*	*		5	5	5	
wmpnetwk.exe	244	TCP	0.0.0.0	554	0.0.0.0	0	LISTENING				
wmpnetwk.exe	244	UDP	0.0.0.0	5004	*	*					
wmpnetwk.exe	244	UDP	0.0.0.0	5005	*	*					
wmpnetwk.exe	244	UDP	127.0.0.1	65401	*	*					
wmpnetwk.exe	244	TCPV6	[0:0:0:0:0:0:0:0]	554	[0:0:0:0:0:0:0:0]	0	LISTENING				
wmpnetwk.exe	244	UDPV6	[0:0:0:0:0:0:0:0]	5004	*	*					
wmpnetwk.exe	244	UDPV6	[0:0:0:0:0:0:0:0]	5005	*	*					
wmplayer.exe	5460	UDP	127.0.0.1	59584	*	*					
wininit.exe	752	TCP	0.0.0.0	1025	0.0.0.0	0	LISTENING				
wininit.exe	752	TCPV6	[0:0:0:0:0:0:0:0]	1025	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCP	192.168.0.51	139	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	80	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	81	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	2869	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	5357	0.0.0.0	0	LISTENING				
System	4	TCP	0.0.0.0	10243	0.0.0.0	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	80	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	81	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	445	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	2869	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	5357	[0:0:0:0:0:0:0:0]	0	LISTENING				
System	4	TCPV6	[0:0:0:0:0:0:0:0]	10243	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1056	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING				

Endpoints: 115 Established: 33 Listening: 37 Time Wait: 4 Close Wait: 0

Figure 10. *TCPView in operation, with records sorted by sent packets, in descending order*

References

- Andreasson, K. (Ed.). (2012). Cybersecurity: Public Sector Threats and Responses. Boca Raton, FL: CRC Press.
- Andress, J. and Winterfeld, S. (2011). Cyber Warfare: Techniques and Tools for Security Practitioners. Boston, MA: Syngress.
- Arndreasson, K. (ed.). (2012). Cybersecurity: Public Sector Threats and Responses. Boca Raton, FL: CRC Press.
- Barnett, M. B. and Finnemore, M. (2004). Rules for the World: International Organizations in Global Politics. Ithaca, NY: Cornell University Press.
- Bayles, A., et al. (2007). Penetration Tester's Open Source Toolkit, Volume 2. Burlington, MA: Syngress.
- Blitz, A. (2011). Lab Manual for Guide to Computer Forensics and Investigations, fourth edition. Boston, MA: Course Technology, Cengage Learning.
- Bousquet, A. (2009). The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York, NY: Columbia University Press.
- Brancik, K. (2008). Insider Computer Fraud: An In-Depth Framework for Detecting and Defending Against Insider IT Attacks. Boca Raton, FL: Auerbach Publications.
- Britz, M. T. (2009). Computer Forensics and Cyber Crime: An Introduction, second edition. Upper Saddle River, NJ: Prentice-Hall.
- Bush, G. W. (2008). Comprehensive National Cybersecurity Initiative (CNCI). Published by the White House January 2008. Retrieved from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative on January 5, 2012.
- Calder, A. and Watkins, S. (2010). IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002, 4th edition. London, UK: Kogan Page.
- Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.
- Carrier, B. (2005). File System Forensic Analysis. Upper Saddle River, NJ: Addison-Wesley.
- Carvey, H. (2009). Windows Forensic Analysis DVD Toolkit, second edition. Burlington, MA:
- Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, third edition. New York, NY: Elsevier.
- Chappell, L. (2010). Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide, first edition. San Jose, CA: Chappell University.
- Cialdini, R. B. (2009). Influence: Science and Practice, fifth edition. Boston, MA: Pearson Education.
- Clarke, R. A. and Knake, R. K. (2010). Cyberwar: the Next Threat to National Security and What to Do About It. New York, NY: HarperCollins Publishers.
- CNBC. (2012) Cyber Espionage: The Chinese Threat. A collection of articles about the cyber threats posed by Chinese hackers. Retrieved from http://www.cnbc.com/id/47962207/ on July 10, 2012.
- Cole, E. and Ring, S. (2006). Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Present Employees and Contractors from Stealing Corporate Data. Rockland, MA: Syngress Publishing, Inc.
- Cole, E., et al. (2009). Network Security Bible, second edition. Indianapolis, IN: Wiley Publishing, Inc.
- Czosseck, C. and Geers, K. (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.
- Davidoff, S. and Ham, J. (2012). Network Forensics: Tracking Hackers Through Cyberspace. Upper Saddle River, NJ: Prentice-Hall.
- Dhanjani, N. (2009). Hacking: The Next Generation. Sebastopol, CA: O'Reilly.
- Edwards, M. and Stauffer, T. (2008). Control System Security Assessments. A technical paper presented at the 2008 Automation Summit – A Users Conference, in Chicago. Retreived from the web at http://www.infracritical.com/papers/nstb-2481.pdf on December 20, 2011.
- Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf on September 30, 2012.
- Freedman, L. (2003). The Evolution of Nuclear Strategy. New York, NY: Palgrave Macmillan.
- Friedman, G. (2004). America's Secret War: Inside the Hidden Worldwide Struggle Between America and Its Enemies. New York, NY: Broadway Books.
- Geers, K. (2011). Strategic Cyber Security. A Cybersecurity technical paper published at DEFCON 20.
- Georgetown University. (2012). International Engagement in Cyberspace part 1. A YouTube video. Retrieved from http://www.youtube.com/watch?v=R1lFNgTui00&feature=related on September 21, 2012.
- Gerwitz, D. (2011). The Obama Cyberdoctrine: tweet softly, but carry a big stick. An article published at Zdnet.com on May 17, 2011. Retrieved from http://www.zdnet.com/blog/government/the-obama-cyberdoctrine-tweet-softly-but-carry-a-big-stick/10400 on September 25, 2012.
- Gjelten, T. (2010). Are 'Stuxnet' Worm Attacks Cyberwarfare? An article published at NPR.org on October 1, 2011. Retrieved from the web at http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet on December 20, 2011.
- Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from the web at http://www.npr.org/templates/story/story.php?storyId=130260413 on December 20, 2011.
- Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from the web at http://www.npr.org/templates/story/story.php?storyId=130260413 on December 20, 2011.
- Gjelten, T. (2011). Security Expert: U.S. 'Leading Force' Behind Stuxnet. An article published at NPR.org on September 26, 2011. Retrieved from the web at http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet on December 20, 2011.
- Gjelten, T. (2011). Stuxnet Raises 'Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011. Retrieved from the web at http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar on December 20, 2011.
- Gjelten, T. (2011). Stuxnet Raises 'Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011. Retrieved from the web at http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar on December 20, 2011.
- Glenny, M. (2011). Dark Market: Cyberthieves, Cybercops and You. New York, NY: Alfred A. Knopf.
- Grabo, C. M. (2004). Anticipating Surprise: Analysis for Strategic Warning. Lanham, MD: University Press of America, Inc.
- Guerin, J. (2010). The Essential Guide to Workplace Investigations: How to Handle Employee Complaints & Problems. Berkeley, CA: Nolo.
- Guerin, J. (2010). The Essential Guide to Workplace Investigations: How to Handle Employee Complaints & Problems. Berkeley, CA: Nolo.

- Harper, A., et al. (2011). Gray Hat Hacking: The Ethical Hacker's Handbook, third edition. New York, NY: McGraw Hill.
- Hintzbergen, J., el al. (2010). Foundations of Information Security Based on ISO27001 and ISO27002, second edition. Amersfoort, NL: Van Haren Publishing.
- Honker's Union of China. (2012). Honker's Union of China website. Retrieved from http://www.huc.me/ on September 21, 2012.
- Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.
- Jones, K. J., et al. (2006). Real Digital Forensics: Computer Security and Incident Response. Upper Saddle River, NJ: Addison-Wesley.
- Jones, R. (2006). Internet Forensics: Using Digital Evidence to Solve Computer Crime. Cambridge, MA, CA: OReilly.
- K., Dr. (2011). Hacker's Handbook, fourth edition. London, U.K.: Carlton.
- Kaplan, F. (1983), The Wizards of Armagedden: The Untold Story of a Small Group of Men Who Have Devised the Plans and Shaped the Policies on How to Use the Bomb. Stanford, CA: Stanford University Press.
- Kerr, D. (2012). Senator urges Obama to issue 'cybersecurity' executive order. An article published at Cnet.com on September 24, 2012 Retrieved from http://news.cnet.com/8301-1009_3-57519484-83/senator-urges-obama-to-issue-cybersecurity-executive-order/ on September 26, 2012.
- Knapp, E D. (2011). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Waltham, MA: Syngress, MA.
- Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.
- Landy, G. K. (2008). The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media, and IP Law. Burlington, MA: Syngress.
- Langer, R. (2010). Retrieved from the web at http://www.langner.com/en/blog/page/6/ on December 20, 2011.
- Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.
- Lockhart, A. (2007). Network Security Hacks: Tips & Tools for Protecting Your Privacy, second edition. Sebastopol, CA: O'Reilly.
- Logicalis. (2011). Seven Ways to Identify a Secure IT Environment. Published at IT Business Edge in 2011. Retrieved from http://www.itbusinessedge.com/slideshows/show.aspx?c=92732&placement=bodycopy in May 5, 2011.
- Long, J., et al. (2008). Google Hacking for Penetration testers, Volume 2. Burlington, MA: Syngress Publishing, Inc.
- Long, J., et al. (2008). No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Burlington, MA: Syngress Publishing, Inc.
- Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all on June 28, 2009.
- Mayday, M. (2012). Iran Attacks US Banks in Cyber War: Attacks target three major banks, using Muslim outrage as cover. An article published on September 22, 2012 at Poltix.Topix.com. Retrieved from http://politix.topix.com/homepage/2214-iran-attacks-us-banks-in-cyber-war on September 22, 2012.
- McBrie, J. M. (2007). THE BUSH DOCTRINE: SHIFTING POSITION AND CLOSING THE STANCE. A scholarly paper published by the USAWC STRATEGY RESEARCH PROJECT. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA423774 on September 30, 2012.
- Middleton, B. (2005). Cyber Crime Investigator's Field Guide, second edition. Boca Raton, FL: Auerbach Publications.
- Mitnick, K. and Simon, W. (2002). The Art of Deception: Controlling the Human Element Security. Indianapolis, IN: Wiley Publishing, Inc.
- Mitnick, K. and Simon, W. (2006). The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. Indianapolis, IN: Wiley Publishing, Inc.
- Nelson, B., Et al. (2010). Guide to Computer Forensics and Investigations, fourth edition. Boston, MA: Course Technology, Cengage Learning.
- Northcutt, S. and Novak, J. (2003). Network Intrusion, third edition. Indianapolis, IN: New Riders.
- Obama, B. H. (2012). Defense Strategic Guidance 2012 – Sustaining Global Leadership: Priorities for 21st Century Defense. Published January 3, 2012. Retrieved from http://www.defense.gov/news/Defense_Strategic_Guidance.pdf on January 5, 2012.
- Obama, B.H. (2011). INTERNATIONAL STRATEGY for Cyberspace. Published by the White House on May 16, 2011. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf on May 16, 2011.
- Osborne, M. (2006). How to Cheat at Managing Information Security. Rockland, MA: Syngress.
- Parker, T., et al. (2004). Cyber Adversary Characterization: Auditing the Hacker Mind. Rockland, MA: Syngress Publishing, Inc.
- Payne, K. B. (2001). The Fallacies of Cold War Deterrence and a New Direction. Lexington, KY: The University of Kentucky Press.
- Philipp, A., et al. (2010). Hacking Exposed Computer Forensics: Secrets and Solutions, second edition. New York, NY: McGraw-Hill.
- Pry, P. V. (1999). War Scare: Russia and America on the Nuclear Brink. Westport, CT: Praeger Publications.
- Radcliff, D. (2012). Cyber Cold War. An article published in the SC Magazine, September 2012 issue.
- Radcliff, D. (2012). Cyber cold war: Espionage and warfare. An article published in SC Magazine, September 4, 2012. Retrieved from http://www.scmagazine.com/cyber-cold-war--espionage-and-warfare/article/254627/ on September 7, 2012.
- Reynolds, G. W. (2012). Ethics in Information Tehnology, 4th edition. Boston, MA: Course Technology.
- Reynolds, G. W. (2012). Ethics in Information Tehnology, 4th edition. Boston, MA: Course Technology.
- Rogers, R., et al. (2008). Nessus Network Auditing, second edition. Burlington, MA: Syngress.
- Rosenbaum, R. (2011). How the End Begins: The Road to a Nuclear World War III. New York, NY: Simon and Schuster.
- RT. (2012). Iran may launch pre-emptive strike on Israel, conflict could grow into WWIII – senior commander. An article published at RT.com on September 23, 2012. Retrieved from http://rt.com/news/iran-strike-israel-world-war-803/ on September 24, 2012.
- Sanger, D. E. (2012). Confront and Coneal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.
- Schell, B. H., et al. (2002). The Hacking of America: Who's Doing It, Why, and How. Westport, CT: Quorum Press.

- Schlesinger, J. (2012). Chinese Espionage on the Rise in US, Experts Warn. An article published at CNBC.com on July 9, 2012. Retrieved from http://www.cnbc.com/id/48099539 on July 10, 2012.
- Schmidt, H. S. (2006). Patrolling Cyberspace: Lessons Learned from Lifetime in Data Security. N. Potomoc, MD: Larstan Publishing, Inc.
- Schmitt, E. and Shanker, T. (2011). U.S. Debated Cyberwarfare in Attack Plan on Libya. An article published in the New York Times on October 17, 2011. Retrieved from http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html on October 17, 2011.
- Seagren, E. (2007). Secure Your Network for Free: Using NMAP, Wireshark, SNORT, NESSUS, and MRTG. Rockland, MA: Syngress.
- Seagren, E. (2007). Secure Your Network for Free: Using NMAP, Wireshark, SNORT, NESSUS, and MRTG. Rockland, MA: Syngress.
- SEM. (2011). The Hacker's Underground. Retrieved from http://serpentsembrace.wordpress.com/2011/05/17/the-hackers-underground/ on September 21, 2012.
- Simpson, M. T., et al. (2011). Hands-On Ethical Hacking and Network Defense. Boston, MA: Course Technology.
- Skpudis, E. and Liston, T. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, second edition. Upper Saddle River, NJ: Prentice-Hall.
- Soloman, M. G., et al. (2011). Computer Forensics Jump Start, second edition. Indianapolis, IN: Wiley Publishing, Inc.
- Stallings, W. (2011). Network Security Essentials: Applications and Standards, fourth edition. Boston, MA: Prentice Hall.
- Stiennon, R. (2010). Surviving Cyber War. Lanham, MA: Government Institutes.
- Strohm, C. and Engleman, E. (2012). Cyber Attacks on U.S. Banks Expose Vulnerabilities. An article published at BusinessWeek..com on September 28, 2012 Retrieved from http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability on September 30, 2012.
- Technolytics. (2011). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict. Purchased and downloaded from Amazon.com on April 16, 2011.
- The Hacker's Underground. An article published at the Serpent's Embrace blog. Retrieved from http://serpentsembrace.wordpress.com/tag/honker-union-of-china/ on September 21, 2012.
- Trost, R. (2010). Praaactical Intrusion Analysis: Prevention and Detection for the Twenty-First Century. Boston, MA: Addison-Wesley.
- Vacca, J. R. (2002). Computer Forensics: Computer Crime Scene Investigation. Hingham, MA: Charles River Media.
- van Wyk, K. R. and Forno, R. (2001). Incident Response. Cambridge, MA, CA: OReilly.
- Verizon. (2012). The 2012 Verizon Data Breach Investigations Report. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf on September 17, 2012.
- Version. (2012). The 2012 Verizon Data Breach Investigations Report. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf on September 17, 2012.
- Volonino, L. and Anzaldua, R. (2008). Computer Forensics for Dummies. Hoboken, NJ: Wiley Publishing, Inc.
- Waters, G. (2008). Australia and Cyber-Warfare. Canberra, Australia: ANU E Press.
- Whitman, M. E. and Mattord, H. J. (2007). Principles of Incident Response & Disaster Recovery. Boston, MA: Course Technology – Cengage Learning.
- Wikipedia Commons. (2011). Stuxnet Diagram. Retrieved from the web at http://en.wikipedia.org/wiki/File:Step7_communicating_with_plc.svg on December 20, 2011.
- Wiles, J., et al. (2007). Low Techno Security's Guide to Managing Risks: For IT Managers, Auditors, and Investigators. Burlington, MA: Syngress Publishing, Inc.
- Wiles, J., et al. (2012). Low Tech Hacking: Street Smarts for Security Professionals. Waltham, MA: Syngress Publishing, Inc.
- Wilhelm, T. and Andress, J. (2011). Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques. Burlington, MA: Syngress Publishing, Inc.
- Zalewski, M. (2005). Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. San Francisco, CA: No Starch Press.
- Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. An article published on July 11, 2011 at Wired.com. Retrieved from the web at http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 on December 20, 2011.
- Zittrain, J. (2012). Professor Zittrain Q&A Hacktivism: Anonymous, lulzsec, and Cybercrime in 2012 and Beyond. A YouTube video. Retrieved from http://www.youtube.com/watch?v=CZWjfxY8nmU&feature=related on September 21, 2012.

WILLIAM F. SLATER III

William F. Slater, III, MBA, M.S., PMP, CISSP, SSCP, CISA, ISO 27002, ISO 20000
President, Slater Technologies, Inc.