Global Information Assurance Certification Paper

WATCHING YOUR SECURITY WALK OUT THE DOOR

Abstract:

Security in the work environment is a critical issue; particularly security of a company's network. Companies invest abundant financial, employee, and material resources to ensure the security of critical and confidential data. Current software allows employees to transfer data from office networked computers to outside computers, thus providing flexibility to work on projects. However, the same software that allows this flexibility can create breeches in security. One thing that seems to be overlooked is the confidential files that employees take home to work on and utilizing programs like Briefcase makes it easier for them to copy the information to their hard drive and keep it up to date. Unfortunately, with programs like Subseven and godswill, social engineering is brought to a whole new level. Employees should be an asset to security; not a liability. As one CEO stated "An asset to me is a piece of land, a building or my car. This is the first situation I have been where the assets walk out the door every night at 5:00".

Ensuring company security needs to be a comprehensive solution that can be easily managed by all employees. Security policies can be implemented and products made available that safeguard data files, but with the growing number of people now being serviced with fast Internet service it can make any employee an easy and unsuspecting target. Our job will get much harder based on the fact that people can now be accessed outside our protective cloak. These trustworthy employees can easily take the company assets, you are paid to safeguard, home with them at 5:00 pm, and when they walk out the door they may control your fate WHEN they are compromised.

Scenario:

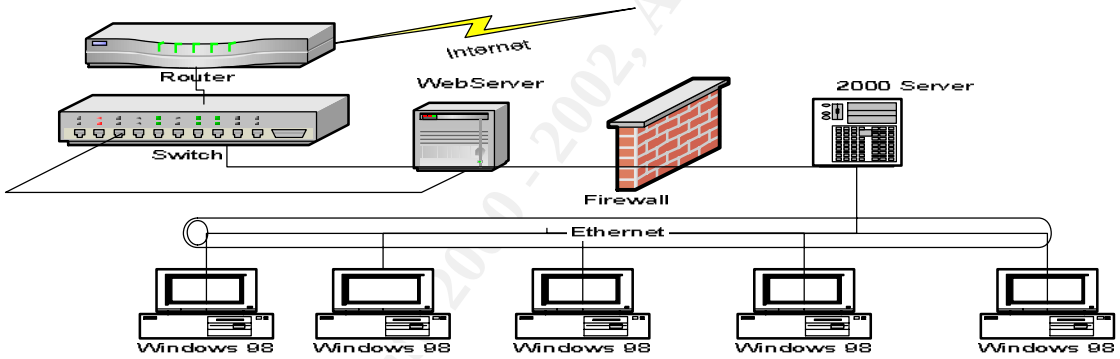
I was recently contracted to repeat a basic analysis on a corporate network to include external probes, port scanning, and determining what computers could be accessed from the Internet. I had previously worked with the company, configuring the firewall and setting up the Win2000 Advanced Server. The company was on a tight budget and so the tools I initially used were inexpensive or freeware. When the company requested a new analysis of the same system, only one month after my previous analysis, I was concerned about the solidity of my work. I later learned my work had been checked by another consultant one week prior; and the need for the repeat analysis was due to compromised information within the system.

The outline of the network is a simplistic one. The router is used as the border guard and connects to the Internet using a T1 connection provided by the local Internet Service Provider (ISP). The Access Control List (ACL) on the router is setup to limit access of the Web Server which is sitting on its' own virtual local area network (VLAN) controlled through the router and switch configuration. The web Server sits outside the corporate firewall as a honey pot, of sorts. The company website is located on this server and there is no other corporate information placed on it. I setup Tripwire http://www.tripwire.com to watch for potential attacks. The Web server has to be accessible to the Internet, so I am using the fruit on the lowest branch analogy hoping that if they do get past the router and switch they will find the Web server (named Wserver). The server will only be running a web site so without much on the server the attacker may not have much interest in it. If someone gets into the network my hope is that they hit the web server first, that Tripwire gives us a heads up that someone is poking around. If the

1.http://www.commodon.com/threat

attacker alters the website it can quickly be restored from backup, so it does sit external to the software firewall configured for the internal network. The internal network is configured for Internet access through the NAT server. The internal network is also on its own VLAN. It sits behind a software firewall called Sygate. Sygate is a software firewall used to protect the internal network. I used Sygate http://www.sygate.com/swat/default.htm because I like the self testing software they had setup on their site to do an external port scan, the log file information and the fact that I can use a tool called "Back Trace" which can backtrack any logged event recorded and do a whois query on them. .

The internal network is configured as a Windows 2000 domain with the NAT server on the Windows 2000 server acting as the domain Controller and also functions as the Sygate firewall. The overall configuration of the internal network includes 16 workstations running Windows 98 and one domain controller running Windows 2000 Advanced Server. The Windows 98 machines have been edited with the System Policy editor to create policies for the local computer to restrict the access at a computer level and the domain controller has been setup with group policies and user profiles to make the environment as secure as possible when looking at the scenario from the user accounts, point of view. I chose to strengthen the perimeter with hardware and audit the interior using software.



I used nmap and Fping to run the external scans against the network and they turned up as expected. I ran the port scanning utility that is available with Sygate and that came back as expected. The router denied my initial scans from the Internet as I expected; I scanned passed the router and was able to find the Web Server. The web server event viewer, security logs, and Tripwire recorded my presence and my attacks were stopped, where I expected them too be, SyGate picked up my scans and I was able to BackTrace to my system. I used a somewhat advanced mentality trying to pretend I didn't know the limitations of the network were and found that, based on that mind set, I was not able to see passed the Web server. I was satisfied that the auditing system and log files were able to detect intrusions and satisfied with the integrity of the hardware configurations, so I moved to examining the log files.

I used the Event Viewer to examine the security and application logs on the Windows 2000 Server. The Windows 2000 server does not give source addresses for events, so I had installed the NukeNabber tool (http://www.dynamsol.com/puppet/nukenabber.html) when I set up the server. The server returned the scans of my IP address, but there were no other logged scans that I observed. I

1.http://www.commodon.com/threat

do understand that there are better tools than NukeNabber, but for the price and company budget it was the best choice. There was nothing that struck me as out of place or suspicious in any of the log files. The Web server, running IIS 5.0, and the Windows 2000server logs showed several scans, but no suspicious activity beyond the initial scan; Sygate logs came up clean as well. I checked the possibility of Event Viewer log being altered, by looking at the version number on the Microsoft_ Authentication_Package and it was still Version 1.0. I was satisfied that the attack did not originate from outside the network. I submitted these findings and recommended that barring the expense of updating some system hardware and software components, which we had previously discussed; my recommendations came back with no substantial findings.

I discussed with the senior management the need for the new analysis and discovered that someone obtained quarterly financial reports and posted them in the break room. The company asked me to give them four answers. The questions were: 1. How they were compromised? 2.How seriously had they been compromised? 3. How to prevent it in the future? Their forth question was "Could we have been attacked from the Internet?" I was not able to honestly rule that out based on their system design, however, if the incident was not done internally how did it get in the break room? I still let them know that yes the attack could have been generated outside the network, but would have been VERY impressed with the skill set this attacker had. I learned that the copy of the financial report posted in the break room was not the final one submitted to the CEO for the quarter. I asked the CFO to try and nail down exactly when that report would have looked like the one in the break room. The information shared with me was that the report could have only been copied a day or two prior to the one given to the CEO. This significantly closed the time frame I needed to focus on. Now, I could focus on log files and examine the system for a specific time frame. I explained that I believed this incident had only three possible areas the event could have come from; an internal employee attack, external attack, or social engineering. These were the areas I would focus on for them.

External Attack:

Although there was strong evidence for an internal attack, I double checked the external connections and studied the external log files and configuration. The dates given by management focused my assessment. I spoke with the network administrator in more detail about the site configuration and any recent updates or upgrades to the hardware or software including the network anti-virus program. The router configuration and the firewall logs were showing no peculiar events, there were no curious port scans found, except my own. The ports that were supposed to be closed were closed and the network virus protector was up to date. I questioned the administrator about the audit system next because I was satisfied with my findings on the possibility of it being an external attack and ruled it out.

Internal Attack:

I concluded the attack came from inside. I started a preliminary assessment talking to the administrator about the auditing files and by looking at the permissions setup on there Win2000 Advanced Server. I asked the network admin to bring up the audit files for the fail password attempts in the security log and the audit files on the successful access of resource folders set up when the server was installed. The reports in question are on an

1.http://www.commodon.com/threat

NTFS partition and stored on the Windows 2000 server. The only two users who had access to it were the CFO and the CEO, the owner of the file was still the CFO. The log files showed no failed password attempts at on the folder, so I asked the CFO to look at the dates and times of access on this folder and file to see if anything looked unusual. He was able to account for every entry in the log and they were all made from the computer in his office, so the results of my findings started to confuse me.
I wanted to see if we could catch the culprit, as did the CEO. I asked the CFO and the CEO to keep the same passwords for two days. I then ran an audit on the successful password attempts, the failure attempts would do us no good at this point (since I suspected someone was using the password to get into the files). They also volunteered to not change the file, so now we had a honey pot (of sorts) in place. I did ask them to change one item in the file, so that if it showed up in the break room again we would know it was accessed after the change and we should be able to track it.

The CEO then announced, to all the employees, that the financial statement placed in the break room was months old and the real one looks nothing like it. My hope was to have someone access it from the network and then at least be able to isolate it to the internal network and that the incident would have occurred on the premises, focusing my assessment. We watched for two days, nothing came up out of the ordinary and the file on the server was never successfully or unsuccessfully accessed, the event never occurred. I then asked the CEO and CFO change their user name and password and increased the audits to both success and failure on the file and on logins. I also asked the network administrator to strengthen the password policy of the network…..Needless to say I was taken off of his Christmas card list.

My brain started thinking about external incidents again, were the log files doctored? Did I overlook something? Were all the ports closed? Is there a back door I missed? I had to put these questions in the back of my mind and turn my full attention to the next element, social engineering.

Social Engineering:

The office layout is not the most secure. The offices are accessed at night by cleaning crews and the last person to turn off the lights at night is not always a member of senior management. This was a huge hole and one that I could have thrown speculations at for days, instead I decided to turn my attention back to the root of the problem and that was the individuals who are ultimately responsible for the confidentiality of this information. The CEO and CFO are the only two people who have full access to the information.. I had reviewed three days worth of log files prior to the break room incident, but when I really hammered them about the date and time the records were compromised I was able to find out that the changes that were made to the financial report were changes that were made the night before. This meant that the report in the break room was accessed by someone the day before it was put in the break room. The CFO knew this by a line item he had changed that night, he could tell because of a particular line item that he had not yet adjusted.
The network did not support a remote access line into the corporate network or use VPN's. The CFO carried everything on a floppy disk when he took work home. I asked him if this disk with the financial information was the floppy disk sticking out of his floppy drive behind him that was in plain view to everyone (I didn't ask it in that manner, but you get the idea). He said it was, so I was putting a scenario in my head as you are probably doing

1.http://www.commodon.com/threat

now, BUT WAIT……getting ready to talk to them about physical security and the importance of keeping valuable data secure and tying that in with the overall security of the office after normal work hours was already forming in my brain stem when the CFO told me he came in the day prior to the incident and copied the file to a disk from the server, on that day (which I verified date and time against the entries in the audit logs), put it in his briefcase and spent the rest of his day in meetings, with his briefcase, outside the office. I asked to examine the disk for viruses or other files and I came up empty. I was right back to square one and my physical security speech went out the window along with my scenario. I was looking for an easy way out and looked back to blaming it on the lack of physical security of the office at night.

Reviewing what I knew:

There are days when we just need to walk away and clear our heads to try and gain a little perspective. I prefer to go back through what I know and this is what I knew. I knew the event occurred one day prior to the incident, that the log files and network security appeared to be intact, that the network appeared to be free of both internal or external attacks, and that the only time the information appeared to be at risk was when it was in a locked brief case traveling from meeting to meeting OR at night when it was being worked on from the CFO's home computer.

I ruled out the disk growing legs and wandering around the halls during a meeting. I focused on the CFO's home computer. The questions I began asking the CFO made me grimace with every response.

The CFO's computer was hooked up to a DSL connection at his house, he was running Windows 98, he had an ancient copy of McAfee antivirus software in place, and there was no personal firewall because "the service provider takes care of it". He looked very bewildered when I asked him to bring his home computer to work the following day.

What scenario is running through your head? I was thinking that the file was stored on his home PC and that someone got access to it the night prior, the information was accessed while he was at home, or it was the CFO who posted the information in the break room (Why do you think I verified his story with the log files?).

The next day, I plugged his computer in (I kept it off the network) and started by running the Antivirus eXpert suite on the computer. BINGO!! I found the Subseven server running on the system. Nasty little Trojan this was my first run in with it, so I was impressed by all it was able to do.

Subseven:

I would recommend that if you have not used it to experiment with its' capabilities it might be worth your time. That whole saying about keeping your enemies closer is true in this case. I have included a brief overview of this nasty little Trojan for those of you who know little about it. During the time it has taken me to write this paper I have had to change the link to find this software twice, however, Subseven could be downloaded for free at http://62.146.74.11/?layout=11&pid=hgr-11656 if you hurry. SubSeven (aka Sub7 or Backdoor_G) currently affects Windows 95/98/ME machines. The beauty of the program is that once it is downloaded to a machine it can alert the client (attacker) that it is on-line and ready to take control of the computer. Once the client knows this it has the ability to do several scary things. It can start an FTP server at the root of the system drive,

1.http://www.commodon.com/threat

edit the registry remotely, restart the remote system, log the keystrokes punched on the keyboard, and even hijack the mouse. It has the ability to spy on Instant messenger conversations and even change them if so desired. This particular attacker knew enough to place the EditServer application in the Win.ini file and "melt" the executable once it was run. This gave the attacker almost unlimited access to the files and settings on the victim's computer, but more importantly it would be harder to back trace.
I knew of Subseven, but needed to research its' capabilities. I found great information about this Trojan at http://trojanports.tlsecurity.net/ and www.tlsecurity.net/tlfaq.htm . I also reviewed the information in several books. The Following information can be retrieved in greater detail from http://www.commodon.com/threat/threat-sub7.htm . The information I provided here is courtesy of http://www.commodon.com/threat and just hits the highlights of the Trojan and how to remove it.

[1]"The server portion of the Subseven can be configured to rerun itself automatically from any of four places each time the system has been rebooted. The Trojan also has two files that can be configured with any name and although the server portion can have any name, it is found in the WINDOWS directory, with one of the following:
"server.exe" (328kb)
"rundll16.exe" (328kb)
"systray.dl" (328kb)
"Task_bar.exe" (328kb)
The second file is found in the WINDOWS\SYSTEM directory, with one of the following:
"FAVPNMCFEE.dll" (35kb)
"MVOKH_32.dll" (35kb)
"nodll.exe" (35kb)
"watching.dll" (35kb)
TCP Ports 6711 and 6776 are used by default, but there's a third TCP port which is the port used in the establishment of the connection between the "client" and "server". This third TCP port can be configured to be anything, although it's commonly seen as TCP port 1243 or TCP port 1999 . As mentioned above, the server portion of the Trojan can be configured by the hacker to rerun itself every time the system is rebooted due to an entry in one of the four locations. Provided below, are the four locations.
The first, is an entry on the "shell=" line in the SYSTEM.INI file.
The second, is an entry on the "load=" or "run=" line in the WIN.INI file.
The third, is under
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
The fourth, is under
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"
NOTE: Of the systems compromised with SubSeven, it's often found to be the first location.

How to Remove SubSeven

1.http://www.commodon.com/threat

The SubSeven Trojan can be configured to be loaded automatically from one of four locations, you'll need to look at all of the locations first. Although the steps are relatively easy, I cannot be held responsible if a mistake is made. Please use caution.
The first and second locations - The WIN.INI and SYSTEM.INI files
Step 1.
Click START | RUN
Type SYSEDIT and press ENTER
Step 2.
Click on the SYSTEM.INI file and look at the "shell=Explorere.exe" line under the [boot] section. There shouldn't be anything to the right of it. However, if yours looks like "shell=Explorer.exe Task_Bar.exe", then Task_Bar.exe is the server portion of the Trojan.
Delete Task_Bar.exe from the line, save the change. Skip to the END.
Step 3.
Click on the WIN.INI file and look at the run= and load= lines under the [windows] section. Because it is common to have legitimate programs on either of these lines. You should look at the name of the file that appears on the line and compare it to those above.
If you find one, delete it from the line, save the change. Skip to the END
The third and fourth locations - The Registry
Step 1.
Click START | RUN
Type REGEDIT and press ENTER
Step 2.
In the left window, click the "+" (plus sign) to the left of the following:
HKEY_LOCAL_MACHINE
Software
Microsoft
Windows
CurrentVersion
Run
Step 3.
In the right window, look for a key that has a Value that loads one of the files listed above. If you don't find a file as listed above, it might mean that the server portion was renamed to something else. Note the names of any suspicious files.
What you will need to do, is open Windows Explorer and go to the WINDOWS directory. Locate each of the suspicious files that were referenced within the right window of regedit. When you find the file that's 328Kb in size. You've probably found the renamed server portion of SubSeven.
Step 4.
Return to the registry and in the right window, highlight the key that loads the file and hit the DELETE key. Answer YES to delete the entry.
Step 5.
Exit the Registry and reboot your computer.
Step 6.
After the computer has restarted, open Windows Explorer

1.http://www.commodon.com/threat

Step 7.
Go to the WINDOWS directory and look for the suspicious file. Once you've found the file, DELETE it.
Step 8.
Exit Windows Explorer."

http://www.commodon.com/threat is the site I used to gather this information. They have screen shots and additional info about this and other Trojan attacks if you are interested.

Now, I knew how the company's file was compromised. The CFO put this file on his computer (used Briefcase to synchronize the files) and someone had loaded the Subseven on the computer to take the file. I asked the CFO if he ever got emails from people at the office or if he emailed people from his computer at home to people at the office. The CFO is a likable guy and said yes that he sent and received jokes and the like to and from several people at the office. I asked to look at his email and did a little investigating. I found nothing in the inbox that would help me out, then I looked in the deleted items sorting the information by date and looked for the day prior to the incident. This is where I caught my first break because fortunately the CFO doesn't ever empty his trash. I still found nothing suspicious, so I went back a week prior to the incident and still no rogue emails. I got frustrated and checked the sent items, which were much fewer; I sorted them again by date and went back even further. I found a reply labeled "this didn't work" almost three weeks prior to the incident. It was from Bob (not really his name this is just the standard name everyone seems to use to protect the guilty) I did not see his name in the scores of e-mails I rummaged through earlier, but I went back into the trash can and alphabetized the discarded mail by name this time and there they were. There were only two pieces sent from Bob, one with the subject of "Your gonna love this one" and the other labeled "Try this one". The first email was the Subseven server but the attachment was called "Joke". The second email also had an attachment called "Joke" and it was actually a joke.

It turns out that Bob had sent an email with the Subseven as an attachment. The CFO unwittingly opened it and now his computer was owned by Bob. I mentioned catching a break and this was it if the CFO had deleted his mail or left the default in place to automatically delete it every 5 days there may have been no way to trace it back to its' source.

Bob was indeed an employee who was on probation for insubordination, taking long lunches, and always being late. The funny thing was that when the CFO went back to check payroll and time cards for the day of the incident to see if he worked that day…….It was the only day he clocked in early…….not 10 or 15 minutes early, but he clocked in 45 minutes early that day. The really interesting thing was that Bob had access to the CFO's computer for almost three weeks and did nothing, he waited for the right time. Bob somehow got wind of our findings and quit before he was confronted by management. The company is deciding how they want to proceed.

Creating a procedure:

I offered the CEO a written procedure for anyone who is going to work from home on confidential material. I have added my set of guidelines to this article. These are

1.http://www.commodon.com/threat

guidelines, not a formal policy. A formal policy in a company like this would have been a waste of time and money, they would have stuck it in a drawer somewhere and never looked at it, so I developed the following guidelines. If you want a formal policy outline, there is great information all over the web. I have gathered a lot of information about policies from http://www.secinf.net/ipolicye.html . In this environment ,however, I wanted to find a way to make this a viable procedure not something that would be ignored. My goals were two-fold;
1. I wanted to idiot proof the resulting security, but make it easy for an employee to understand and follow the instructions.
2. If they did not follow all of the procedures then they are still protected in some way when working on the company's information. The guidelines to the procedure are as follows

Procedure:

Company information, ABC Inc, is not to be worked on or discussed outside the company location at 123 Main St. Sandy, Utah. This would include files, electronic and hard copy. Company documents are not to be taken off the premises on floppy disc, sent through the e-mail system, or copied in any way without the expressed written consent of one of the principles of this company listed in the section labeled PEOPLE.
This was the blanket "policy" statement. It is not allowed to happen unless the company knows about it. The principles accepted this responsibility knowing that there was going to be more paperwork for the requests, but that it was important to have it in the document as a standard.

Plans

Information that must leave the premises or be put on a computer which is not directly linked to the corporate network must meet the following guidelines at a minimum.

1- The network administrator will supply you with CD-ROM(s) which you will need to install on the computer system prior to editing corporate documents. This CD will come with a detailed set of instructions on how to load the necessary software.
2- Once all the software is loaded the computer must be rebooted.
3- The off site computer must be disconnected from the Internet for the entire time the company information is being utilized
4- The computer must have the software listed in the section labeled "Products" installed on the computer. This software can be checked out through the systems administrator with the instructions to load the products.
5- Corporate documents must NOT be saved to the computers hard drive. All files are to be saved to the floppy or Zip disk.

Products

The products that must be installed on your personal computer while working on corporate documents will be reviewed and updated by the systems administrator, John Jones, every three months starting Feb. 2000. The products currently approved are

1. Zone Alarm or Sygate
2. F Protect, Bit Defender, or Norton Anti-Virus

1.http://www.commodon.com/threat

The systems administrator will provide you with a CD version of this software which is compatible with your operating system. Once the network administrator has verified that the employee has written permission to work on corporate information off-site the employee will sign out the products and install instructions.

Note: I know that if the plan is strictly adhered to that the Zone Alarm is not a needed precaution; however, knowing that some users still do not understand basic concepts to interacting with the interface, they will not know how to "unplug" from the Internet. This may look like overkill; however, I consider it trying to idiot proof a potential event from occurring. The antivirus serves two functions. One if they load a corporate document at home and the personal system has a virus there is a chance that they will bring it back to the office. The other reason is that the products I picked have an auto update feature and can update the signatures in case they have recently downloaded something that will morph into a virus. These anti-virus programs also will monitor ports that are opened and alert you to this fact.

Processes

These processes are mandated by the principles of the company. Failure to comply with them will hold the individual liable for any information that is stolen or copied from them while they have the corporate files in their possession. These processes are as follows:

1. Unplug anything on the back of your computer that looks like a telephone cable
2. Reboot your computer (the detailed instructions will guarantee the anti-virus and the firewall program starts at boot-up)
3. Copy corporate files only to the Floppy drive or a Zip drive (the anti-virus program is set up to run when the floppy is accessed).

People

The principles that have the authority to give written permission on behalf of the Board of Directors are as follows:
John Jones CEO
Bill Smith CFO
Mary Jones Dir of Personnel

Outside of these guidelines I have advised the company to look into encryption of e-mail in the near future and restrict the ability to send company files without encryption in place. The problem in this scenario was promptly solved as soon as I discovered the way the attacker gained access to my clients system. All the books, case studies and research I have seen give us information about ways to protect the assets of the company; however, technically speaking this scenario was outside the scope of my responsibility and yet it is exactly my responsibility. There is an interesting article at http://zdnet.com.com/2100-1105-889542.html that talks about this issue and shows that this is becoming a real concern for companies all around the world.

The guidelines put in place for this scenario are there to avoid this issue in the future and it will take additional time on the part of the system administrator to initialize. The employees may view this as an inconvenience, but beyond that it did not add substantially to anyone's workload or to network resources. There are vulnerabilities in this plan and the largest one I think is ignorance. If everyone is trained properly and

1.http://www.commodon.com/threat

follows the steps this type of event would be eliminated. If the employees are just thrown a CD and a piece of paper with abstract steps on it, then it will end up on sitting on the corner of their personal computer and the issue will arise again.
The SANS Security Essentials course reaffirmed the steps that I took and the processes that I followed using the tools and skills I had acquired. There was information in the courseware that I used during my analysis of this incident, which helped to reaffirm the steps I took when isolating the events that took place in this scenario week's earlier.

I once worked for a gentleman who was big into real estate. One day, in a board meeting, he made the comment "An asset to me is a piece of land, a building, or my car. This is the first situation I have been in where the assets walk out the door every night at 5:00 ". This comment never rang more true than in this scenario.

List of References:

1. McClure, Stewart; Scambray Joel; Kurtz George, Hacking Exposed. New York: Osborne/McCraw-Hill, 2001. Pages 125-127

2. Schultz,E.,Shumway,Russell. Incident Response. Boston: New Rider, 2002.

3. Schneier, Bruce. Secrets & Lies. New York: Wiler Computer Publishing, 2000. Pages 256-269

4. Rubin,Aviel. White-Hat Security Arsenal, Boston: Addison-Wesley, 2001

5. http://www.sygate.com/swat/default.htm

6. http://www.dynamsol.com/puppet/nukenabber.html

7. http://62.146.74.11/?layout=11&pid=hgr-11656

8. http://trojanports.tlsecurity.net/

9. www.tlsecurity.net/tlfaq.htm

10.http://www.commodon.com/threat/threat-sub7.htm

11. Loney, Matt Your worst security threat: Employees? ZDNet (UK) April 23, 2002, http://zdnet.com.com/2100-1105-889542.html

12. http://www.secinf.net/ipolicye.html

13. http://www.tripwire.com/download

1.http://www.commodon.com/threat

Last Updated: September 20th, 2017

Upcoming Training

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event