Global Information Assurance Certification Paper

ATTACKS AND TOOLS THAT PROVIDE ANSWERS

Scott Baker
March 5, 2004
GSEC Practical Assignment, version 1.4b, Option 1

ATTACKS AND TOOLS THAT PROVIDE ANSWERS

Abstract:

Like a lot of us new to the Computer Security world, one is placed in a role with very little “hands-on” or mentored training. With this paper I hope to assist someone with gaining a basic knowledge of different attacks and the utilization of certain tools thereby equipping any security professional with the answers to many questions including, who, how, when and for how long.

Introduction:

This paper will describe a variety of attacks, their method of deployment, ways of detecting them, utilizing several tools, and briefly explain log keeping and analyzing. Next, it will introduce ways to try and eliminate the threat of an attack from happening again.

With the growing fear of terrorism in our society, we are faced with paranoia of “am I going to be next?” We are looking for answers to questions that we never had to ask before. These questions of course are:

- am I being attacked
- by whom
- how I am being attacked
- when have these attacks taken place and
- how long have they been going on

Attacks:

I would like to start off by telling you about different types of attacks. Attacks occur in a variety of different approaches. Some arrive via Email, Web and straight on vulnerability attacks; and, yes, even physical attacks.

Email is a common deployment strategy which usually attaches a file that, when opened or executed, will deploy its payload of a virus, worm or Trojan horse. There are more than 81,000 threats today[1]. Viruses come in many different forms. One type is to cause damage to your computer system itself, just like the JDBGMGR.EXE Hoax[2]. This was an example of a mass mailing email that would have you delete this executable program from your system causing it not to operate properly. Another form of attack is known as a “Trojan horse.“ According to legend, the Greeks won the Trojan War by hiding in an oversized, hollow wooden horse to sneak into the fortified city of Troy. In today's computer world, a Trojan horse is defined as a malicious, security-breaking program that is disguised as something benign. Installing a program onto your system of this

[1] Network Associates Inc.
[2] Network Associates Inc., JDBGMGR.EXE Hoax

nature could perform a denial of service attack against other's systems, open ports to allow other activities like these attacks: Back Orifice, IniKiller, NetBus, NetSpy, Priority, Ripper, Senna Spy, Striker. Descriptions are best noted from Sonicwall's[3] web site at http://www.sonicwall.com/products/demo/attack.html.
Or, just delete files on your hard drive or collect your personal information by allowing the ability to collect credit card or bank account information or just let the hacker take control of (hijack) your system for their own needs.

Sometimes an email will just have a link to a site that looks like it provides a reasonable offer. Normally these reasonable offers are carefully structured web sites that will take advantage of an unsuspecting user who has an unprotected computer system. Not only are links to web sites sent via email, hackers will utilize many tactics to spread their infections. One worth mentioning is the use of web page redirection. Web page redirection is a process of having links or embedded code on a site that will direct one to another site. Commonly pages like this will also cause what are known as pop-ups or pop-unders. These additional web browser windows are now running the carefully crafted code of a hacker's choice. Another way to lure an unsuspecting user is the use of manipulation of the users own knowledge by having a domain name that uses misspelling to attract unsuspecting victims. All it takes is to have the wrong spelling of a site and the user goes to a web site that appears to be legitimate, like the notorious whitehouse.com, but in fact the misdirection will cause you to be taken to an undesirable site.

Vulnerability attacks are generally caused by flaws found in the code of a device. These vulnerabilities are found by hackers who actually discover the flaw or by searching the web for known vulnerabilities, found by others or posted by the device manufacturer. One would take these vulnerabilities and use them to exploit a system that is subject to the flaw. Once a vulnerable system is compromised, a hacker would search for other devices that may be subject to similar attacks, or worse, may have already gained access to your systems.

Physical attacks are in my option the worst that could happen to an organization. Not always will this type of attack be obvious. Allowing someone unescorted access to any part of you company could be very detrimental to your network. Attackers have the know how to persuade their way past security guards, cleaning personnel and even your co-workers.

Tools:
To evaluate your network a security professional must rely on some tools. A security professional's tool bag should never be limited to a few programs that will do scanning and packet analyzing. Instead, that tool bag should include virus scanning, patch management, router information tools, firewall logs, configuration knowledge and basic DOS utilities.

[3] Sonicwall, Alerts and Attacks, March 2004

Port scanners like SuperScan 4[4] and AngryIP[5], provide an administrator the ability to evaluate a network for mis-configured workstations and servers. "SuperScan 4 provides a powerful TCP port scanner, pinger, resolver, superior scanning speed, support for unlimited IP ranges, host detection using multiple ICMP methods, TCP SYN scanning, UDP scanning (two methods), IP address import supporting ranges and CIDR formats, simple HTML report generation, source port scanning, fast hostname resolving, Extensive banner grabbing, massive built-in port list description database, IP and port scan order randomization, a selection of useful tools (ping, traceroute, Whois etc), extensive Windows host enumeration capability."

"AngryIP scanner is a very fast IP scanner for Windows. It can scan IPs in any range. Its binary file size is very small compared to other IP scanners. AngryIP scanner simply pings each IP address to check if it's alive, then optionally it is resolving hostname, scans ports, etc." Finding open ports on a system could indicate serious vulnerabilities, like having ports 25-mail or 23-ftp open on your internal SQL server, although some may desire this configuration. To speed up network scanning some utilities have included a port list option, where they provide you with a list of known vulnerable ports to scan for. This approach is very helpful in speeding up your task of open port network scanning but, a word of wisdom---false positives are sometimes a norm. Take for example port 6667. This port is known for Internet Relay Chat servers and it is also the port that American Power Conversion[6] (APC) uses for their PowerChute battery backup management software.

Using a virus scanner like Symantec's Norton Antivirus[7] program will protect your email, instant messenger and files by automatically scanning those processes and files in real time and if found to be infected, will remove such things as viruses, worms and Trojan horses.

Patch management should be an ongoing task. To make that task simpler you need to use good products. Products like Shavlik's HFNetChkPro[8] will allow you to deploy system patches remotely. By setting up groups within HFNetChkPro, it provides ways to test your patches before you deploy them to the masses. This product gives detailed reports and links to the appropriate patch resources. After a scan of your systems, HFNetChkPro will provide you with a breakdown on each machine that was scanned furnishing a detailed report of installed and missing patches and levels, not to mention the criticality of the patch and much more.

[4] Foundstone, SuperScan4
[5] Angryziber Software, AngryIP
[6] American Power Conversion Corp., APC
[7] Symantec's Norton Antivirus
[8] Shavlik, HFNetChkPro

How does one gather information about routers? Like most of us, we do it the old-fashioned way: we telnet to the device and copy and paste our configuration and run a few router IOS commands. Believe it or not, there are products out there that were developed to do just that type of information gathering for you. One product is Kiwi's Cat Tools[9] which will automate your network device configuration management. Not only does Cat Tools perform configuration backups but it will also provide you with IOS versions, Mac addresses and an ARP table, and even tracks changes for you. One should utilize the scheduling feature imbedded in this product to perform scheduled tasks, like report generation and configuration backups.

A firewall is typically one's first line of defense to the outside world. You should know how this device works and learn the rules for *creating* rules. There's not a lot of people who can say they have never accidentally disabled there access to the firewall by implementing a rule change that was wrong. Be careful in your configuring of this device, make backups of your firewall often. Let me also inform you that just because your firewall comes, for the most part pre-configured out of the box, don't rely on it. At minimum, configure your firewall to block all unnecessary ports. Next, make sure any service that is not going to be used is turned off. Some firewalls include DHCP and VPN features, if not in use, disable them. Most people assume the firewall will protect them from all the hacker's attempts at hacking them. This is far from the truth; although a firewall will protect you from a majority of attempts, we need to create rules that only allow appropriate traffic to flow. This thought process should also pertain to all of your outbound (egress) traffic as well. As security professionals we need to ensure that the integrity of our traffic is intact and of an appropriate use.

Other basic tools come from old, reliable DOS. With these commands at our finger tips we need to use them. Some to include are ping, tracert, and Nbtstat.

The ping tool created by Mike Muuss,[10] was named after the sound that a sonar makes, inspired by the whole principle of echo-location. According to Microsoft Corporation[11], "Ping verifies connections to remote computers. It sends Internet Control Message Protocol (ICMP) echo packets to a computer and listens for echo reply packets. Ping waits for up to 1 second for each packet sent, and prints the number of packets transmitted and received to the console. This tool is available only if you install TCP/IP." One option I like to use with the ping command is the –a. This option allows you to resolve the IP address to the host name, providing you with the host name an IP address together.

"Tracert determines the route taken to a destination by sending ICMP echo packets with varying time-to-live (TTL) values to the destination. Before forwarding a packet, each router along the path is required to decrement the TTL

[9] Kiwi Enterprices, Kiwi Cat Tools
[10] Muuss, Mike, The Ping Story
[11] Microsoft Coporation, Ping and Tracert utilities

value on a packet by at least 1, so the TTL value is effectively a hop count. When the TTL value on a packet reaches 0, the router sends back an ICMP "Time Exceeded" message to the source computer. Tracert determines the route by sending the first echo packet with a TTL value of 1 and incrementing the TTL value by 1 on each subsequent transmission until the target responds, or the maximum TTL value is reached. The route is determined by examining the ICMP "Time Exceeded" messages sent back by intermediate routers. Some routers silently drop packets with expired TTL values and are invisible to Tracert." With the usage of these two commands one is able to determine, at times, the computer name and routes that they took to get to your network. "

Nbtstat[12] displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS names tables for both the local computer and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS)."
Don't count on this tool all the time, as it will not provide much unless the remote system provides you with NetBios information and the remote networks are not blocking any NetBios traffic from getting back to you. In using these three commands, one is able to obtain detailed routing paths, along with host names and IP addresses.

One way to bring all three and more of these commands together would be to use a handy application called SamSpade.[13] SamSpade combines a vast amount of handy tools together, providing you with ping, DNS information, whois, IP block information (what's their range of addresses). DIG will request all DNS records for a host or domain, tracert, finger; it will even retrieve the home page's raw data and search the abuse.net site. Samspade allows you to log your findings to four different log files per session and persistent archive of results copied to log, per session and persistent archive of all results. This product has many options to set and if you still don't like its logging features, you can still copy and paste to your favorite editing tool. I use the logging feature then save them to names like IPAddress_Date.txt for future reviewing.

ARIN – RIPE – APNIC: these are regional internet registries. They will provide you with a whois and rwhois search of the internet numbering resource.

"The American Registry for Internet Numbers (ARIN)[14] is a nonprofit organization responsible for managing the Internet numbering resources for North America, a portion of the Caribbean, and sub-equatorial Africa."

"The RIPE Network Coordination Centre (RIPE NCC)[15] is one of four Regional Internet Registries (RIR) that exist in the world today, providing allocation and

[12] Microsoft Corporation, Nbtstat utility
[13] Atkins, Steve, SamSpade 1.14
[14] American Registry for Internet Numbers
[15] RIPE Network Coordination Centre

registration services that support the operation of the Internet globally. The RIPE NCC performs activities primarily for the benefit of the membership in Europe, the Middle East, Central Asia and African countries located north of the equator."

"APNIC[16] is one of four Regional Internet Registries currently operating in the world. It provides allocation and registration services which support the operation of the Internet globally. It is a not-for-profit, membership-based organization whose members include Internet Service Providers, National Internet Registries, and similar organizations. APNIC represents the Asia Pacific region, comprising 62 economies."

Detection:
Detecting intrusions should be performed with persistence and consistency. Utilizing some of these solutions will help verify the integrity of your systems and data. Detection will include the use of log servers, virus scanning, intrusion diction systems (IDS), network scanners and file integrity checking.

Some may feel "is this all necessary just to detect if someone is hacking me?" My own objection is that security should be "Intrusion Detection In-Depth"[17].

Log servers are an essential part of detection. One such product is Kiwi Syslog daemon.[18] Kiwi Syslog is a centralized collection point for all of your network devices that are able to send syslog and snmp traps. It will receive logs and display the results on screen. Kiwi Syslog can be configured to forward Syslog messages or send a heart beat to any other syslog enabled device.

Virus scanning. Enough said already, just do It! Making sure in a corporate environment that you use a server/client based configuration. Letting the server handle all of the updating will make your life a whole lot easier. The clients contact the server on a scheduled basis, keeping up with the virus definitions. This should be a daily task. Some virus protection vendors post their new virus definitions weekly. There's always a change of that zero day virus update. You will also want to subscribe yourself to a virus alert mailing list provided by your virus protection vendor.

Intrusion Detection Systems (IDS) are very successful in detecting attacks. Sometimes to the point that you will not get any sleep. One great tool to mention is SNORT[19] "Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and

[16] Asia Pacific Network Information Centre
[17] Sans, Track 3
[18] Kiwi Enterprises, Kiwi Syslog Daemon
[19] Sourcefire, Inc., Snort

much more." Snort is a rule based intrusion detection system that is leading the way in the IDS world. Think of Snort as a virus scanner on steroids, analyzing packets of data and comparing them against its vast array of customizable rule sets. An intrusion detection system should be an integral part of every network, inside and out.

Network scanning is a procedure that maps out your network for active hosts, IP addresses and open ports. Another procedure to mapping a network is to use inverse mapping. Inverse mapping is a stealth-approach method that gathers information about inactive IP addresses on a network. Attackers will use this information to try to determine which IP addresses are associated with active hosts, in turn mapping out your network. The use of scanners like SuperScan4, AngryIP, Nmap[20], Ethereal[21] and similar ones, should only be used with direct permission from your organization.

A word of caution when performing a network scan---some mis-configured scans could cause excessive amounts of traffic on your network, bringing your network to a crawl. Try to limit your network scanning to only visible networks and never venture outside of your controlled network.

Another approach in using network scanning is to find out what type of information your systems are giving out. Some interesting facts about your systems can be acquired just by querying a system. Some useful information would be IP and Mac addresses, null sessions, type of operating system, Net bios name, domain or workgroup name, type of services, open shares, user and group accounts and account policy information.

Take heed and know every bit of information that your systems are giving out, sometimes willingly. Perform network scans regularly to find out this information before someone else does. Stop unneeded services and ports, close the gaps.

File integrity checking is a way of ensuring that critical system files have not been tampered with. Files like your registry, startup, kernel files and main program files including dlls and exes. Tripwire[22] is one product that supplies an administrator with the functionality of checking file integrity. "Tripwire software establishes a "digital inventory" of known good files and their attributes and uses it as a baseline for monitoring changes."

Incident Handling:
After we have collected and centralized all of our logs, now we need to decipher them. There are several approaches to doing this. There's the automated and the manual way; be prepared to do more of the latter. First, the automated way, hopefully everyone has set up at least their firewalls and routers to inform them

[20] Fyodor, NMap
[21] Ethereal
[22] Tripwire, Tripwire

of updates and alerts. Next, using a tool like Kiwi Syslog, you may setup email notification based on filtered messages. Snort will perform similar functions and can be configured to have an audible alert. Kiwi can be configured to provide you with daily activity reports. These are very useful and will provide you with a quick view of items such as the amount of messages received, total, last 24 hours, last hour, this hour, average and since midnight. It will even give you a breakdown of syslog messages by severity.

Manual deciphering of logs will be a necessity. Using a parsing tool like WinGrep[23] will enhance your ability in searching through log files. You will find yourself searching for items such as source and destination IP addresses and ports, key words, command strings, times, dates and even message levels.

Reports from your virus scanner will prove to be valuable. Have you ever been asked the question "are all our machines up to date with virus definitions?" Having virus scanning logs at your fingertips will not only help to answer these types of questions, but will give any security professional a sense of knowing that their systems are safe from at least the last virus, Trojan horse or worm that came out.

Did you ever want to know if someone has been trying to logon to your systems? Well, you won't know without the event logs and auditing turned on. Centralizing your event logs will enable you to parse through them easily. Another way would to have your event logs sent to your syslog centralized server. Using a tool like the Event to Syslog utility,[24] one gains the benefits of the Kiwi Syslog features in monitoring the event logs in near real time. Other items to consider before an attack occurs and its aftermath are:

- The default event log configuration supplied by Windows is not useful for auditing and attack detection and needs to be modified. Turn it on and increase your maximum log size.
- Be sure to move log data out to a different log server - an attacker can otherwise easily modify it.
- The log host should be hardened.
- Event log data is probably not enough information to track an attacker, just another source of information.
- Also, be sure to check several text log files, like IIS logs, DHCP logs, becoming familiar with what is normal.
- Turn on auditing for important system files and check for unauthorized processes accessing them.

What about your server and workstation operating system patch levels? Are they up to date? Some may believe HFNetCheckPro to be a tool for just that, keeping

[23] Huw Millington, Windows Grep
[24] Smith, Curtis, Purdue University, Event to Syslog

their operating systems up to date. What if you find out that one of your systems has been compromised? Depending on the attack used, one could use the patch level report to check for other systems with the same patch level deficiency. Using this information you can check other systems for evidence of attacks.

Eliminating the Threat:
This is the big question we all have. One may believe that the threats can be eliminated. I believe that we will always have a level of vulnerability, as long as software and hardware vendors continue to make products with flaws. Our job as security professionals is to minimize those threats to a point where it doesn't happen to us. So how do we do that?

We need to limit and control the access to our networks and systems with the use of firewalls and routers that are configured most restrictively. Configuring access control lists will assist in stopping attackers from known sources from even reaching your network. Creating a deny everything rule in your firewall and then create an allow rule for only what you need.

Installing an IDS system on the outside of your firewall will not only provide you with information about who is trying to attack you, but will also act as a deterrent.

We need to ensure that we stay current with all software patch levels and virus definitions. The use of an outlining network virus scanner, scanning network traffic before it hits your network, will prove to be invaluable. This will help in the never ending job of keeping our users from damaging their workstations and/or our network.

Physical security starts with you, the administrator. We may want to ensure that we have lockable cabinets and doors. Keeping your data center secure will ensure that no one enters without proper authorization. Clean up after yourself! Administrators are notorious for leaving sensitive information laying around. Control the use of hubs and or switches out on the floor, don't let them be obviously visible. Spot check your facility, making sure that there aren't any additional or unneeded pieces of equipment plugged into your network. Don't be afraid to ask a stranger if you may help them. Sometimes this tactic will deter probing attackers. Lastly, provide escorted travel while in your company; this proves to be the most secure means.

Another successful solution in preventing attacks is to inform your users by having annual security training. Training them in hacking trends, ramifications of an intrusion, users' role in security, hacker types/motivation, threats to your information, hacking 101, malicious code (Viruses, Worms, Trojans, etc…) and key policies, will provide well-informed users who are less likely to harm you in your efforts in securing your network. Remember, your network is only secure as the weakest link.

Conclusion:

After all is said and done, attacks are inevitable. We need to learn how to limit our own exposure to them and put a stop to it. Security is not solved by a "silver bullet." It takes layers of fortification to become secure. Then and only then are we able to feel like we are secure. We can harden our systems and block anyone from accessing them. We can scan our networks for anomalies but making our weakest links to security disappear will not happen. By informing them, this will ensure that we become more secure. Tools allow us to find out the who, how, when and for how long, but the proactive security professionals are the ones who stay ahead of the security threat.

References:

McAfee AVERT Virus Information Library, March 2004
http://vil.nai.com/vil/

McAfee AVERT Labs, Jdbgmgr.exe hoax, 01/22/2003 8:54 AM (PT)
http://vil.nai.com/vil/content/v_99436.htm

SonicWALL, Alerts and Attacks, March 2004
http://www.sonicwall.com/products/demo/attack.html

Foundstone, SuperScan 4, March 2004
http://www.foundstone.com/resources/proddesc/superscan4.htm

Angryziber Software, AngryIP Scanner, version 2.20, March 2004
http://www.angryziber.com/ipscan

American Power Conversion Corp., PowerChute version 5.21
http://www.apc.com/index.cfm?isoCountryCode=us

Symantec's Norton AntiVirus™ 2004,
http://www.symantec.com/nav/nav_9xnt/

Shavlik Technologies, Hot Fix Net Check, March 2004
http://www.shavlik.com/pHFNetChkPro.aspx

Kiwi Enterprises, Kiwi CatTools 2.0.6 Beta 2- Released 21st February 2004
http://www.kiwisyslog.com/cattools2.htm

Muuss, Mike, The Story of the PING Program, prior November 20, 2000
http://ftp.arl.mil/~mike/ping.html

Microsoft Corporation, Description of the Ping and Tracert Tools, 10/9/2002 (1.0)
http://support.microsoft.com/default.aspx?scid=kb;en-us;217014

Microsoft Corporation, nbtstat, March 2004
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/nbtstat.mspx

Atkins, Steve, SamSpade, version 1.14
http://www.samspade.org

American Registry for Internet Numbers, March 2004
http://www.arin.net/about_us/about.html

RIPE Network Coordination Centre (RIPE NCC), March 2004

http://www.ripe.net/ripencc/about/

Asia Pacific Network Information Centre, March 2004
http://www.apnic.org/info/about.html

SANS, Intrusion Detection In-Depth, Track 3, March 2004
http://www.sans.org

Kiwi Syslog Daemon, 7.1.0 Beta 6 - Released 11th February 2004
http://www.kiwisyslog.com/info_syslog.htm

Sourcefire, Inc., Snort, Thu Mar 4 03:15:27 2004 GMT
http://www.snort.org/about.html

Fyodor, NMap, version 1.30 for windows, March 2004
http://www.insecure.org/nmap

Ethereal version 0.10.2, March 2004
http://www.ethereal.com

Tripwire, Tripwire for Servers, 2004
http://www.tripwire.com/products/servers/index.cfm

Huw Millington, Windows Grep, version 2.3, March 2004
http://www.wingrep.com

Smith, Curtis, Purdue University, Event to Syslog version 3.4, June 12, 2003
https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys)