Global Information Assurance Certification Paper

Continuously Anticipating the Network Attack
Mark Georgas
Version 1.2f
February 20, 2002

Introduction

Information and network security professionals are tasked with ensuring the confidentiality, availability, and integrity of their network environments from those unauthorized to access it. In maintaining the peace of mind of trying to secure networks within an organization, one must recognize how an attacker might coordinate their efforts before initiating an attack. Below are the potential processes an attacker may take to gain access to a network:

- Information Gathering – Conducting social engineering or scanning the targeted network to learn what services are running and vulnerabilities the target may be exposed to if attacked.
- Attacking – Using the information gathered, the attacker can implement their malicious code to gain access on the target.

Being aware of the various methods an attacker may choose in trying to penetrate a given network will allow the responsible party to better anticipate and defend against the attack. Presented in the following discussion, information gathering and techniques, attacking, and defensive measures will be explored. The information presented is to provide the reader with a heightened awareness for observations regarding methods an attacker may use when implementing their attack and seek to make recommendations to alleviate the risk of a network compromise.

Information Gathering and Techniques

Social engineering is the aim to trick people into revealing passwords or other information that compromises a target system's security. It usually involves some form of impersonation, of either a particular individual or a role and can exist as a computer or human based medium [1]. For example:

- Authority Attack - Perceiving the position of authority, the attacker will intimidate the help desk into giving him/her a new password by stressing that they have only a limited amount of time to retrieve some information for an executive meeting.
- Popup Windows – A pop-up window will appear prompting the user to re-enter their username and password due to losing a network connection. A program previously installed by the intruder will then email the information back to a remote site.
- Help Desk Attack – Impersonating a current or new end-user needing help with access to a network or server.
- Fake Survey/Questionnaire Attack – Offering to reward an unsuspecting individual the potential for a free vacation trip by answering a few simple questions about their network. In conjunction, the user must also enter an email address and password. Many

employees will enter the same password that they use at work. This gives the attacker a valid username and password to enter an organization's network.

- Dumpster Diving – Going through the target's trash bin and collecting valuable information. The Supreme Court ruled in 1988 that once an item is left for trash pickup, there is no expectation of privacy or continued ownership [2].

These methods are probably the attackers easiest entry method into a trusted computer system. Minimizing the threat of social engineering is a user education problem. Therefore emphasizing training and awareness of such attacks will greatly decrease the chances of unauthorized access.

Another method of gathering information an attacker will utilize is scanning networks and hosts before mounting an attack of the target. Such methods include but certainly are not limited to:

- Port Scanning – This is a popular reconnaissance technique used to discover what services can be broken into. The objective is to get root on a remote system by port scanning the target system and getting a list of open ports. An attacker must know what software is using that port. There are various port scanner techniques employed by attackers [3]. For example, Nmap is a port scanner that supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, pings sweeps, and more. Some of the more commonly used techniques from the tool support the following according to Fyodor [4]:
  - TCP SYN (half open) scanning
  - TCP FIN (stealth) scanning
  - SYN/FIN scanning using IP fragments (bypass packet filters)

  Another port scanner to look at is Nessus.
- IP Address Scanning – The first thing an attacker needs to know is the IP Address to connect to the target. An easy method of obtaining information in regards to knowing whether or not the targeted box is connected to a network is using the command prompt to do a ping –a. Ping commands to the target IP stack which sends out an ICMP Echo Request packet, and waits for an ICMP Echo Reply. If the destination of the ICMP packet is up, has an IP stack, and is not behind a device blocking ICMP echoes (a firewall), the ICMP Echo Reply will be received by the target IP stack, and presented to the attackers Ping program so they can see that the reply was received, and that the target is up and reachable [5]. Another method is going to the Verisign website to find IP Addresses and domain names. The information found here is usually important contact names, addresses, and phone numbers. Attackers use that information to their advantage when applying social engineering techniques.
- Man-in-the-Middle – A method used commonly by an attacker to take over a session between two points on a network. Since most authentication takes place at the beginning of the TCP session, where the handshake occurs; this allows the party to gain access to a given machine. And with that, valuable or confidential data can be within reach.

These tools and techniques help the attacker to determine what ports of a host are listening for connections, which represent potential communication channels. Mapping their existence facilitates the exchange of information with the host, and thus it is quite useful for anyone

wishing to explore the victim's networked environment. By employing the same tools and methods used by an attacker, an administrator will see what their site looks like to the would-be intruder, and expectantly take the necessary steps to help secure their systems.

Attacking

To reiterate, information gathering enables an attacker to obtain a blueprint of operating systems and version numbers of programs running on a target. To exploit the vulnerabilities of an attacker's target, there are many toolkits with recipes for attacking at their disposal. "As malicious code authors implement new propagation methods, hacker tools become more readily available and easier to use, and the number and potency of worms and viruses grow, information security threats and vulnerabilities will continue to increase dramatically," according to Jim Jones, director of Information Security Analysis, at Predictive Systems [6]. These toolkits are programmed with the information of the vulnerabilities and instructions on how to exploit them. These are simply a point and click type application in which an attacker enters the target IP address and clicks on a button, which initiates the attack. Attackers that frequently use this method are known as script-kiddies. These are individuals with little skill in code development and their motivation for attacking is intellectual curiosity.

The attacking phase is distinctive in that it has a malicious payload, which causes the damage and a delivery of the malicious payload focused on the target. In regards to the malicious payload, there is virtually no limit to the damage it can cause to its targeted host.
To touch upon, BackOrifice 2000 (B02K) created by Cult of the Dead Cow, is without a doubt considered one of the most malicious payloads because it can give complete control of the attacker's targeted system. Its capabilities include [7]:

- Keystroke logging – Enables the attacker to gather any information typed into the system.
- List detailed system information – The program can tell the attacker the operating system version, CPU type, hard drive size, and the amount of RAM of the victim computer.
- Multimedia control – Control of the keyboard and mouse of the victim computer is possible as well as viewing real-time streaming video of the victim screen.
- Altering of the system registry – This is the bread and butter of complete control over the victim computer. An attacker can reconfigure the system through the registry with ease.

These capabilities allow BO2K to look like a legitimate remote control program similar to the commercial tool pcAnywhere. However the main differences are BO2K is available in full source code form and it can run in stealth mode. When in stealth mode, the application will not show up on the task or process list of Windows NT/2000 thus making the victim totally unaware the application exist [7].

Delivery of such a malicious payload onto its target without the victim being aware is quite stealthy. One method in particular is through the use of wrappers, which are batch files that enclose executable programs to allow for separate programs to join together [8]. In this case, wrappers attach a given EXE application (such as an electronic greeting card) to the BO2K server application giving it the characteristics of being a Trojan horse. The attacker will deliver

the malicious payload via email although making the application in appearance look unthreatening by the file name extension. The unsuspecting user will open the file thus installing BO2K, and run the wrapped application. The victim sees only the latter action. There are several wrapper programs released, which include SaranWrap, SilkRope, and EliteWrap [9]. These wrapping programs are easily created Trojan horses without having to do any programming that can create havoc for the unlucky party. The figure below displays the simplicity of the program, thus being a point and click.

Figure 1 Silk Rope 2000 by netninja.com [9]

The moral here is to be cautious in downloading software to your computer from unknown or untrustworthy sources. Some other common methods of attacks regarding exploited Internet security flaws used presently, taken directly from the recently published SANS document "The Twenty Most Critical Internet Security Vulnerabilities" include [10]:

- *Exploitation of cgi-bin vulnerabilities - Most web servers support Common Gateway Interface (CGI) programs to provide interactivity in web pages, such as data collection and verification. Many web servers come with sample CGI programs installed by default. The fix is to is to remove any unnecessary files and users who have access to the server. In addition, establish a limited root for the web server and review the directory permissions to limit access. Regularly audit and test the web server with tools available on the Internet that are designed to identify vulnerabilities. One tool developed specifically for identifying vulnerable CGI scripts is WHISKER, which is freely available over the Internet* [11].

- *User accounts, especially root or administrator with weak passwords or no passwords at all - Some systems come with "demo" or "guest" accounts with no passwords or with widely known default passwords. Service workers often leave maintenance accounts with no passwords, and some database management systems install administration accounts with default passwords. Compromised user accounts get the attackers inside the firewall and inside the target machine. Once inside, most attackers can use widely accessible exploits to gain root or administrator access. The most common fix is to create an acceptable password policy stating user responsibility and verification of password quality. In addition, implement password-cracking programs such as l0pthcrack for*

Windows NT and Crack for UNIX to ensure passwords are difficult to break.

- *Global file sharing and inappropriate information sharing via netBIOS and operating systems - Windows NT ports 135->139 (445 in Windows2000), or UNIX NFS exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548. These services allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access to any hostile party connected to the network. Many computer owners and administrators use these services to make their file systems readable and writeable in an effort to improve the convenience of data access.*

- *IMAP and POP buffer overflow vulnerabilities or incorrect configuration - IMAP and POP are popular remote access mail protocols, allowing users to access their e-mail accounts from internal and external networks. The "open access" nature of these services makes them especially vulnerable to exploitation because openings are frequently left in firewalls to allow for external e-mail access. Attackers who exploit flaws in IMAP or POP often gain instant root-level control. The advice given is to disable these services on machines that are not e-mail servers to implement the latest patches.*

These are just a few of the threats mentioned from the SANS Institute resources. A full list is available from their website.

Conclusion

No single security component will guarantee the security of a given network against the various types of attacks. Although a combination of components will significantly reduce the possibility of an attacker compromising the confidentiality, availability, and integrity of that network. But according to Tom Longstaff, manager of survivability of network technology for the CERT Coordination Center "There's no one thing you can do. Products defeat some misuse, but they don't catch them all" [12]. Methods that can lead to an effective security solution when anticipating a network attack are:

- Avoidance – Placement of firewalls, routers with a good access control list, encryption, etc. are necessary to reduce unauthorized access to your networks. Firewalls provide a security boundary between networks of differing trust or security levels by enforcing a network-level access control policy. Firewalls filter network packets, making decisions to allow and disallow passage of packets according to a specified policy.
- Detection – Obtaining audit logs and have in place an Intrusion Detection System to analyze what activity is hitting the network is crucial.
- Security Investigation – Collecting information to investigate the extent of damage when security breaches do occur. A tool for this I recently saw demonstrated is Niksun's NetDetector. It's a continuous network-recording tool that can reconstruct data from historical periods of time. Data captured by NetDetector is analyzed to inspect traffic flows for improper activities, detect intruders and set alarms while continuously recording and analyzing every packet in the network in real time at full production traffic rates [13].

These methods properly managed will help protect companies from outsider attacks, and help against attacks inside the network. This is a concern equally if not more alarming than the outside threat. Unlike attackers probing from outside the company's networks, insiders have an easier time concealing their activities. They have knowledge of the network architecture and more importantly access to the network. That in essence gives them the ability to insert malicious code and take servers offline. Reasons behind these types of attacks can range from financial gain to revenge due to perhaps being laid off. In addition to the defensive methods discussed above, tools and services have been developed to help prevent insider misuse. Similar to Niksun's NetDetector, Raytheon's Silent Runner can identify risks and spot vulnerabilities, detect network misuse and abuse, and hunt down insider threats [14]. In essence, these tools help enable a company to track all activity on its network. When the software detects unusual activity, it alerts the network administrator. Likewise, startups such as NetSec or Counterpane offer around-the-clock remote network-monitoring services to oversee network operations and detect abnormal usage [15]. In spite of increased awareness of security threats and the new technologies available to battle external and internal threats, businesses are always at a disadvantage in protecting their networks. As attackers get smarter and more sophisticated, it becomes even more difficult to protect networks. However, placing more barriers in their way will surely discourage future attempts, or at least slow them down.

References

[1] Granger, Sarah: "Social Engineering Fundamentals, Part II: Combat Strategies," SecurityFocus; January 9, 2002. URL: http://www.securityfocus.com/infocus/1533

[2] Richards J. Heuer, Jr: "Theft and Dumpster Diving." URL: http://www.mbay.net/~heuer/T3method/Theft.htm

[3] Fadia, Ankit: "Port Scanning Unscanned," 5 October 2001. URL: http://security-protocols.com/article.php?sid=630

[4] Fyoder: "The Art of Port Scanning," Insecure.org; September 6, 1997. URL: http://www.insecure.org/nmap/nmap_doc.html

[5] "ICMP Stands For Trouble," NetworkMagazine.com; September 5, 2000. URL: http://www.networkmagazine.com/article/NMG20000829S0003

[6] "New Worms, Distributed Attack Networks, and Software Vulnerabilities Among Next Wave of Major Information Security Issues," Predictive Systems; January 14, 2002. URL: http://www.predictive.com/company/press_room/releases/ReleaseDetail.cfm?PR_ID=383

[7] "BackOrifice2K.Trojan," Symantec Security Response; July 11, 1999. URL: http://www.symantec.de/avcenter/venc/data/back.orifice.2000.trojan.html

[8] "Trojan Worm Attacks Cloud The Future Of Reactive Anti-virus Software," Info-sec.com; December 7, 1999. URL: http://www.astalavista.com/technologies/library/misc/spending.shtml

[9] "Silk Rope," Netninja.com; URL: http://www.netninja.com/bo

[10] "The Twenty Most Critical Internet Security Vulnerabilities," Version 2.501 November 15, 2001. URL: http://www.sans.org/top20.htm (November 25, 2001)

[11] "Whisker: a next-generation CGI scanner," SecureTeam.com; November 19, 1999. URL: http://www.securiteam.com/tools/3R5QHQAPPY.html

[12] Shafer, T. Scott: "Corporate Espionage The Enemy Within," Red Herring; Pg. 78, January 2002.

[13] "NIKSUN NetDetector: Recording, Analysis and Playback of any Network Activity," Niksun.com; URL: http://www.niksun.com/products/netdetector.html

[14] "Silent Runner," Silentrunner.com; URL: http://www.silentrunner.com

[15] "Counterpane," Counterpane Internet Security; URL: http://www.counterpane.com

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
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