Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2f

Basic Self-assessment: Go Hack Yourself
Barry Dowell
September 11, 2001

Introduction

Hacker n. 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. A malicious meddler who tries to discover sensitive information by poking around. Hence 'password hacker', 'network hacker', or 'cracker'.[1]

One of the greatest fears of the system administrator is the thought of their network being compromised. There are many threats, constantly bombarding the defenses of computer networks. If an intruder has physical access to a machine, they will be able to remove or damage parts of the system. If a hacker already has a low-privilege user account on the system, and the latest security patches have not been applied, there is a good chance he will be able to use known exploits in order to gain additional privileges. Finally, remote intrusion involves a hacker who attempts to penetrate a system across a network. He starts with no privileges and must gain entry by bypassing the network's defenses.[2] In order to combat these threats, one must put oneself in the mind of the attacker, and assess their own vulnerabilities from that point of view. System administrators must not only be aware of the potential vulnerabilities inherent in their operating system and applications software, but they must know how to protect the network from these dangers, and they must be able to assess their defenses before a successful attack is carried out.

Security Policy

Probably the single most important tool for network security is the Security Policy. This is a well written and signed document that has been approved by management and is mandatory reading for everyone who has access to the network. The Security Policy will dictate exactly what the security parameters will be for the given network: What kind of hardware protection will the network require, such as firewalls, intrusion detection, proxy servers, etc.? Will the server be in a locked room, and who will have access to it? Will dial-up modems be allowed? What type of auditing will be done, by whom, and when? What constitutes a good password? When will backups be performed and by whom? What is the disaster recovery plan?[3] Self-assessment is a very important part of this plan. The procedures that are put in place must be tested regularly to ensure that they are being followed and are effective.
These are just a few of the subjects that the policy should touch on. The scope of this document will vary widely, depending on the depth of security that the individual

network requires. The Security Policy is a living document, and will need to be updated regularly to meet the needs of the ever-changing environment of the office and the Internet.

Operating System

Operating Systems Installation – Put CDROM into CD drive and click <Install>. You are now up and running on your new secure network. *WRONG!* For all hosts, whether they are servers or clients, the first step toward security is hardening the operating system. The numerous holes and security exploits on Windows and UNIX systems are widely publicized on hacker websites and on the sites of those trying to improve network security. One of the most common types of these exploits is the buffer overflow. In a buffer overflow attack, the hacker would typically send more logon characters than the operating systems is prepared to handle. These extra characters may be treated like executable code. When run, this code allows the hacker to gain access to the network. This is just one of the many methods used by attackers. By limiting the number of open ports and services on your system, it follows that you would be limiting the number of available exploits. So, one of the first things to do after your installation, is turn off or disable every network service that is not essential to your operation and disable any unnecessary open ports that are running.[4] Nmap is a free utility, downloadable from http://www.insecure.org/nmap/index.html that you can use to scan your entire network for open ports. Keep in mind that Nmap may also be used by attackers to scan your network. You should also keep patches updated on your system. For Microsoft, visit http://www.microsoft.com/security/ at least once a month to download patches and keep abreast of the latest security news and alerts.

Know the enemy. One of the most common hacker profiles is a 13 year old "script kiddie".

> ***Script kiddie***
>
> *1. The lowest form of cracker; script kiddies do mischief with scripts and programs written by others, often without understanding the exploit they are using. Used by people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems. Since most of these tools are fairly well known by the security community, the adverse impact of such actions is usually minimal.*[5]

The script kiddie hunts for vulnerabilities with no specific target in mind. They simply download a malicious script from the Internet and fire it off, in hopes of finding a victim. By keeping your patches up to date and knowing the inherent problems with your operating system and your application software, problems caused by script kiddies can usually be avoided. To test your network against script kiddies, after obtaining written permission to do so, download a recent script from any number of hacker web sites, and run it against your system. Note: This is a very dangerous thing to do. Results are unpredictable, and your system could be damaged. Always have a good backup,

and know how to use it.

Once your operating system has been hardened, patches have been installed, and application software has been installed and updated accordingly, you should make a backup of your entire system and lock it away in a safe place. If something catastrophic should happen to your network, you will always be able to restore to your original baseline. Backup and Restore procedures must define when a backup must be performed, who will perform it, and what method will be used. The disaster recovery plan should define who is responsible for the restore, and the step-by-step procedure for completing a thorough recovery. The disaster recovery plan should be tested periodically to ensure success.

Choosing good passwords

A good Password is one that is kept secret and is difficult for someone to guess or crack through traditional brute force methods.
So the first rule is “Keep it a secret”! Do not disclose your password to anyone. Many people routinely write down their passwords on a sticky note and put it on their monitor or under their keyboard. This makes it extremely easy for any passerby to obtain access and use their account. If a person must write down a password, it should be kept in a secure, locked place. This should be spelled out in your security policy and can be audited by randomly making a quick sweep of a person’s office or cubicle, looking for written passwords.

The second rule is to choose a good password. Passwords should not be comprised of a person’s name, their pets name, their birthday, social security number, or anything else that could be easily discovered and used to gain access. There are many parameters that can be set to ensure good passwords. Free applications, such as npasswd or yppapasswd, or commercial applications such as PowerPassword by Symark, (http://www.symark.com/) can do automatic password checking every time a password is changed. Microsoft Windows NT and most flavors of UNIX have password rule sets that can be configured to do this, although they typically do not have the number of options that a third party offers. A good password should have at least 6 characters. More characters increase the difficulty of cracking or guessing the password. A good password will also contain a combination of upper and lower case characters, numbers, and special characters like *, &, $, #, etc. A good method to create your own good password is to think of an easy to remember phrase, and use the first letter of each word, adding a number and a special character, somewhere in the middle. For example if you like Coca Cola you might say:

Have a Coke and a Smile 2 times a day

The password would be **HaC*aaS2tad**

This looks like garbage, but is an excellent password. Even an excellent password is not foolproof, so they should be forcibly changed on a regular time schedule and there

should be rules determining how often a password can be reused.[6]

To audit the passwords that your users have chosen, you can use cracking tools like L0phtCrack or Crack. These tools attempt to guess passwords using dictionary attacks and brute force attacks. A dictionary attack simply uses all of the words in a dictionary to guess a password, including hybrid attacks that check for backwards spelling and using numbers to replace certain letters, such as using 1's for l's in the word "hello" (i.e. "he11o"). The brute force attack is a guaranteed method of cracking a password, but it may take more time than is practical for the hacker. The brute force attack tries every character in every position of a password, until it gets the correct combination. The longer and more complicated passwords may take years for a single pc to crack. Before running any of these tools on your network, get written permission from anyone in management that may be concerned with this, and give your users at least a weeks notice before your test.

Social Engineering: How may I help you?

Social Engineering is hacker-speak for tricking a person into revealing their password. This is the most common and easiest way for an attacker to gain access to a network. There are several ways to do this. A hacker may send a bogus email message claiming to be the system administrator needing your password for some administrative task. Another method is "shoulder surfing", simply looking over someone's shoulder as they type in their password. Another problem is sharing accounts. This should never happen. If a person needs to be on the system, they should have their own account.[7] A bold hacker may even use the telephone to impersonate someone in the upper management of your company claiming that he forgot his password and is under pressure to sign on to the network immediately to get information for an impending meeting or deadline. He may ask the administrator to reset his password, so he can log on and "save the world". These types of attacks are surprisingly successful due to the naiveté of users and human nature (i.e. we want to be helpful).

It only takes one of these mistakes to bypass all of the password policies, firewalls, and whatever else you have implemented for your perimeter security. To fight social engineering, you must educate your users and frequently test them to ensure awareness. Send your own emails and make your own phone calls asking for passwords. If someone makes a mistake, let him or her know how serious it is, and, chances are, it will not happen again.

Inside, Outside, Upside-down

It seems that the main focus of computer security is protection from the malicious outside hacker, but, in reality, your network is more likely to be compromised by people inside your organization. Even the best security policy is no match for an unhappy employee. According to the Computer Security Institute/FBI and Ernst & Young, nearly 50% of all network attacks come from the inside. In a NetVersant survey, 82%

reported spotty or no compliance with their company's security policies. 85% say a properly implemented firewall would still be vulnerable to a disgruntled employee. And 75% say the firewall is at risk because of employee incompetence.[8] It is far beyond the scope of the system administrator's responsibilities to keep employees happy, but there are several things one can do to prevent these inside hackers from causing network problems. You can start with the physical location of your servers. They should be located in a locked, air-conditioned room. Access to this room should be limited to those who actually need physical access to the servers. The main console may also be locked away in this room. The rules that you setup for your users can limit such things as which files they can access, what they can do with those files, the time window in which they can log onto the system, and which workstations they can use to logon. A system administrator must have auditing turned on, and must review these logs on a regular schedule that has been spelled out in the security policy. Log filters can be put in place to weed-out unusual or suspect traffic, and can alert an administrator via email, pager, etc.. Employees must be taught to lock their workstations before walking away from a terminal session. A partial fix to this problem is to set password protected screen savers to be invoked at a maximum of 15 minutes of idle time. This will still leave a window of opportunity for the would-be hacker, but it is better than the alternative. Essentially the system administrator must take on the role of security guard, periodically "rattling doorknobs", and watching the logs to see who has been where and what they were doing.

Perimeter Security

The surest way to keep hackers from stealing passwords and wreaking havoc on your network is to build a wall that won't allow them to get close enough to touch your system. Typically the first line of defense against outside penetration is the firewall. The firewall acts as a single point of access, where all traffic coming into a network can be audited, authorized and authenticated. Based on the rules used to configure it, a firewall can block any suspicious activity. Common types of firewalls are: **Routers**, which simply look at a packet and decide whether or not its destination is inside the network; **Packet filters**, which examine the source and destination of an IP packet, as well as the source and destination TCP/UDP ports, and accept or reject the packet based on user-defined rules; **Stateful packet systems**, which are similar to packet filters, but they actually examine the contents of a packet to determine if it should accept or reject it, based on the rules defined by the user; and **Application proxies**, which force all network traffic to be examined before they decide which data is to be passed on, and which to drop.[9] When creating the rule sets for firewalls, one must consider the effect certain limitations will have on the performance of the network. The more stringent the rules are, the more processing power is required. There are several methods used to evaluate the effectiveness of your firewall. Auditing tools can log all traffic that hits the firewall, and these logs may be sorted by many variables, such as: what traffic was allowed to pass, what traffic was rejected, where did the traffic originate, and what is its destination. The audit logs can provide important forensic evidence. After an attack, all of the traffic related to the attack can be analyzed to give

the administrator a better understanding of how the attack was carried out, and how to protect the network against future attacks. Intrusion detection is a type of network management tool that gathers information from various places in a network to identify possible security breaches. These breaches include intrusions (attacks from outside the organization) and misuse (attacks from within an organization).

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Tracking user policy violations[10]

One of the most popular Network Intrusion Detection Systems is *Snort*. Snort is an open source application that is capable of performing real-time traffic analysis and packet logging on IP networks.[11]
One gaping hole that is a common problem in many computer networks is the dial-up modem. Many new pc's come with modems installed, and if this modem is connected to an outside line, such as a fax line, and configured to auto-answer, the hacker has a virtual open door to your system. This telephone line bypasses all of the perimeter security that you have meticulously installed and configured to protect your network. (See figure 1) One way to detect this vulnerability is to physically check every pc on the network. This would be nearly an impossible task on a large network. There is a tool called a war dialer that is used by hackers to locate these auto-answering pc's, and it can also be used by system administrators for the same purpose. You can set the war dialer to automatically dial all of the incoming lines to your company, listening for a computer to answer. When a modem does answer, the number is logged, and you can track down the misconfigured pc and solve the problem.

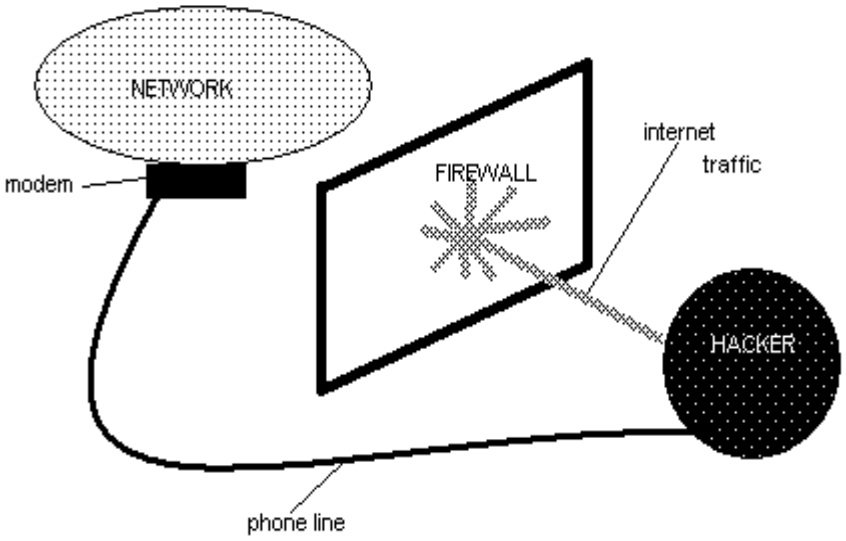

Figure1. How a war dialer can circumvent a firewall.

Malicious Code: Viruses, Trojans, and Worms, Oh My!

There are many dangerous things out there in the Enchanted Forest, but most of them can be avoided easily enough by the installation and continuous updating of anti-virus software. A Virus is a program that reproduces itself, hides in other computer code without permission, and does nasty or undesirable things, not intended by its victim. Viruses travel by email, CD-ROM, diskettes, and in shared files on a network. A Trojan is simply a malicious computer program disguised as something useful. The major difference between a Trojan and a virus is that viruses reproduce, and Trojans are a one time executable program. A Worm is a computer program that can run independently and travel across networks, as opposed to a virus, which requires an operator to transfer files from one system to another.[12] All three of these may make using the Internet seem to be a foolish endeavor, but the majority of these can be stopped in their tracks by a security policy that implements a good anti-virus software routine. Your job as a system administrator would be to make sure this software is updated and enabled on all of the hosts on your system.

Conclusions: Lather, rinse, repeat

No network is 100% secure. A system administrator must determine how secure the network must be, and implement a security policy that conforms to that philosophy. One thing that will play a major role in the security of a network is the monetary cost versus the cost of a security breach. Is the threat from a malicious source dangerous enough to justify the cost of protecting against an intrusion? One must continuously assess the network's vulnerabilities and keep abreast of the latest threats. I believe employee education plays a major role in network security. If your employees don't know what is expected of them, and they are unaware of the consequences of their actions, what motivation could they have to do their part in keeping the network secure? Anti-virus software must be kept up-to-date, operating systems and applications must be patched, passwords must be checked, penetration scans must be performed, and backups must be done. The list goes on and on. When all of this has been done, and no holes have been found, you, as a system administrator, can finally relax…then start from the top and do it all over again.

References:

1. http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html

2. http://www.robertgraham.com/pubs/network-intrusion-detection.html Robert Graham - FAQ: Network Intrusion Detection Systems

3. http://secinf.net/info/policy/policy.htm Information Security Reading Room – What Do I Put in a Security Policy? By William Farnsworth

4. http://networks.depaul.edu/security/winnt.htm DePaul University Network Security - Securing Windows NT

5. http://www.tuxedo.org/~esr/jargon/html/entry/script-kiddies.html

6. http://networks.depaul.edu/security/passwords.htm DePaul University Network Security -- Choosing Good Passwords

7. http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html Del Armstrong -- Social Engineering

8. http://www.zdnet.com/anchordesk/story/story_1959.html Jesse Berst, ZDNet AnchorDesk – The Biggest Threat to Your Network's Secirity. (It Isn't What You Think)

9. http://enterprisesecurity.symantec.com/article.cfm?articleid=743&PID=8104802 - related Symantec, Securing the Perimeter, Part 1

10. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci295031,00.html searchSecurity.com – intrusion detection

11. http://www.snort.org/about.html Snort - What is Snort?

12. http://ksi.cpsc.ucalgary.ca/courses/547-96/cochrane/present/ Computer Viruses, Trojans and Worms

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 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 Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 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
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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event