

Covers all Exam Objectives for CEHv6



Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEH™

Certified Ethical Hacker

STUDY GUIDE


Exam 312-50
Exam EC0-350

Kimberly Graves



SERIOUS SKILLS.

Chapter 4. System Hacking: Password Cracking, Escalating Privileges, and Hiding Files.....	1
Section 4.1. The Simplest Way to Get a Password.....	2
Section 4.2. Types of Passwords.....	2
Section 4.3. Cracking a Password.....	8
Section 4.4. Understanding Keyloggers and Other Spyware Technologies.....	15
Section 4.5. Escalating Privileges.....	16
Section 4.6. Understanding Rootkits.....	18
Section 4.7. Hiding Files.....	19
Section 4.8. Understanding Steganography Technologies.....	21
Section 4.9. Covering Your Tracks and Erasing Evidence.....	22
Section 4.10. Summary.....	23
Section 4.11. Exam Essentials.....	24
Section 4.12. Review Questions.....	25
Section 4.13. Answers to Review Questions.....	29



Chapter 4

System Hacking: Password Cracking, Escalating Privileges, and Hiding Files

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Understand password-cracking techniques
- ✓ Understand different types of passwords
- ✓ Identify various password-cracking tools
- ✓ Understand escalating privileges
- ✓ Understand keyloggers and other spyware technologies
- ✓ Understand how to hide files
- ✓ Understand rootkits
- ✓ Understand steganography technologies
- ✓ Understand how to cover your tracks and erase evidence



In this chapter, we'll look at the various aspects of system hacking. As you recall from Chapter 3, "Gathering Network and Host Information: Scanning and Enumeration," the system hacking cycle consists of six steps. The first step—enumeration—was discussed in the previous chapter. This chapter covers the five remaining steps:

- Cracking passwords
- Escalating privileges
- Executing applications
- Hiding files
- Covering tracks

The Simplest Way to Get a Password

Many hacking attempts start with getting a password to a target system. Passwords are the key piece of information needed to access a system, and users often select passwords that are easy to guess. Many reuse passwords or choose one that's simple—such as a pet's name—to help them remember it. Because of this human factor, most password guessing is successful if some information is known about the target. Information gathering and reconnaissance can help give away information that will help a hacker guess a user's password.

Once a password is guessed or cracked, it can be the launching point for escalating privileges, executing applications, hiding files, and covering tracks. If guessing a password fails, then passwords may be cracked manually or with automated tools such as a dictionary or brute-force method, each of which are covered later in this chapter.

Types of Passwords

Several types of passwords are used to provide access to systems. The characters that form a password can fall into any of these categories:

- Only letters
- Only numbers
- Only special characters

- Letters and numbers
- Only letters and special characters
- Only numbers and special characters
- Letters, numbers, and special characters

A strong password is less susceptible to attack by a hacker. The following rules, proposed by the EC-Council, should be applied when you're creating a password, to protect it against attacks:

- Must not contain any part of the user's account name
- Must have a minimum of eight characters
- Must contain characters from at least three of the following categories:
 - Nonalphanumeric symbols (\$,:”%#@!#)
 - Numbers
 - Uppercase letters
 - Lowercase letters

A hacker may use different types of attacks in order to identify a password and gain further access to a system. The types of password attacks are as follows:

Passive Online Eavesdropping on network password exchanges. Passive online attacks include sniffing, man-in-the-middle, and replay attacks.

Active Online Guessing the Administrator password. Active online attacks include automated password guessing.

Offline Dictionary, hybrid, and brute-force attacks.

Nonelectronic Shoulder surfing, keyboard sniffing, and social engineering.

We'll look at each of these attacks in more detail in the following sections.

Passive Online Attacks

A passive online attack is also known as *sniffing* the password on a wired or wireless network. A passive attack is not detectable to the end user. The password is captured during the authentication process and can then be compared against a dictionary file or word list. User account passwords are commonly *hashed* or encrypted when sent on the network to prevent unauthorized access and use. If the password is protected by encryption or hashing, special tools in the hacker's toolkit can be used to break the algorithm.



Cracking the password-hashing will be discussed later in this chapter in the "Attacks" section.

Another passive online attack is known as *man-in-the-middle* (MITM). In a MITM attack, the hacker intercepts the authentication request and forwards it to the server. By inserting a sniffer between the client and the server, the hacker is able to sniff both connections and capture passwords in the process.

A *replay attack* is also a passive online attack; it occurs when the hacker intercepts the password en route to the authentication server and then captures and resends the authentication packets for later authentication. In this manner, the hacker doesn't have to break the password or learn the password through MITM but rather captures the password and reuses the password-authentication packets later to authenticate as the client.

Active Online Attacks

The easiest way to gain administrator-level access to a system is to guess a simple password assuming the administrator used a simple password. Password guessing is an active online attack. It relies on the human factor involved in password creation and only works on weak passwords.

In Chapter 3, when we discussed the Enumeration phase of system hacking, you learned the vulnerability of NetBIOS enumeration and null sessions. Assuming that the NetBIOS TCP 139 port is open, the most effective method of breaking into a Windows NT or Windows 2000 system is password guessing. This is done by attempting to connect to an enumerated share (IPC\$ or C\$) and trying a username and password combination. The most commonly used Administrator account and password combinations are words like Admin, Administrator, Sysadmin, or Password, or a null password.

A hacker may first try to connect to a default Admin\$, C\$, or C:\Windows share. To connect to the hidden C: drive share, for example, type the following command in the Run field (Start ⇨ Run):

```
\\ip_address\c$
```

Automated programs can quickly generate dictionary files, word lists, or every possible combination of letters, numbers, and special characters and then attempt to log on using those credentials. Most systems prevent this type of attack by setting a maximum number of login attempts on a system before the account is locked.

In the following sections, we'll discuss how hackers can perform automated password guessing more closely, as well as countermeasures to such attacks.

Performing Automated Password Guessing

To speed up the guessing of a password, hackers use automated tools. An easy process for automating password guessing is to use the Windows shell commands based on the standard NET USE syntax. To create a simple automated password-guessing script, perform the following steps:

1. Create a simple username and password file using Windows Notepad. Automated tools such as the Dictionary Generator are available to create this word list. Save the file on the C: drive as `credentials.txt`.

2. Pipe this file using the FOR command:

```
C:\> FOR /F "token=1, 2*" %i in (credentials.txt)
```

3. Type **net use \\targetIP\IPC\$ %i /u: %j** to use the credentials.txt file to attempt to log on to the target system's hidden share.



Another example of how the FOR command can be used by an attacker is to wipe the contents of the hard disk with zeros using the command syntax `((i=0; i<11; i++)); do dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done`. The wipe command could also be used to perform the wiping of data from the hard disk using the command `$ wipe -fik /dev/hda1`.

Defending Against Password Guessing

Two options exist to defend against password guessing and password attacks. Both smart cards and biometrics add a layer of security to the insecurity that's inherent when users create their own passwords.

A user can also be authenticated and validated using *biometrics*. Biometrics use physical characteristics such as fingerprints, hand geometry scans, and retinal scans as credentials to validate users.

Both smart cards and biometrics use *two-factor authentication*, which requires two forms of identification (such as the actual smart card and a password) when validating a user. By requiring something the user physically has (a smart card, in this instance) and something the user knows (their password), security is increased, and the authentication process isn't susceptible to password attacks.



RSA Secure ID is a two-factor authentication system that utilizes a token and a password.

Offline Attacks

Offline attacks are performed from a location other than the actual computer where the passwords reside or were used. Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media. The hacker then takes the file to another computer to perform the cracking. Several types of offline password attacks exist, as you can see in Table 4.1.

TABLE 4.1 Offline attacks

Type of attack	Characteristics	Example password
Dictionary attack	Attempts to use passwords from a list of dictionary words	Administrator
Hybrid attack	Substitutes numbers of symbols for password characters	Adm1n1strator
Brute-force attack	Tries all possible combinations of letters, numbers, and special characters	Ms!tr245@F5a

A dictionary attack is the simplest and quickest type of attack. It's used to identify a password that is an actual word, which can be found in a dictionary. Most commonly, the attack uses a dictionary file of possible words, which is hashed using the same algorithm used by the authentication process. Then, the hashed dictionary words are compared with hashed passwords as the user logs on, or with passwords stored in a file on the server. The dictionary attack works only if the password is an actual dictionary word; therefore, this type of attack has some limitations. It can't be used against strong passwords containing numbers or other symbols.

A hybrid attack is the next level of attack a hacker attempts if the password can't be found using a dictionary attack. The hybrid attack starts with a dictionary file and substitutes numbers and symbols for characters in the password. For example, many users add the number 1 to the end of their password to meet strong password requirements. A hybrid attack is designed to find those types of anomalies in passwords.

The most time-consuming type of attack is a brute-force attack, which tries every possible combination of uppercase and lowercase letters, numbers, and symbols. A brute-force attack is the slowest of the three types of attacks because of the many possible combinations of characters in the password. However, brute force is effective; given enough time and processing power, all passwords can eventually be identified.



A *rainbow table* is a list of dictionary words that have already been hashed. Rainbow tables can speed up the discovery and cracking of passwords by pre-computing the hashes for common strings of characters. For example, a rainbow table can include characters from a to z or A to Z. Essentially, rainbow table tools are hash crackers. A traditional brute-force cracker will try all possible plaintext passwords one by one in order. It is time consuming to break complex passwords in this way. The idea of rainbow tables is to do all cracking-time computation in advance.

Nonelectronic Attacks

Nonelectronic—or nontechnical attacks—are attacks that do not employ any technical knowledge. This kind of attack can include social engineering, shoulder surfing, keyboard sniffing, and dumpster diving.

Social engineering is the art of interacting with people either face to face or over the telephone and getting them to give out valuable information such as passwords. Social engineering relies on people's good nature and desire to help others. Many times, a help desk is the target of a social-engineering attack because their job is to help people—and recovering or resetting passwords is a common function of the help desk. The best defense against social-engineering attacks is security-awareness training for all employees and security procedures for resetting passwords.



Social engineering was covered in more detail in Chapter 2, “Gathering Target Information: Reconnaissance, Footprinting, and Social Engineering.”

Shoulder surfing involves looking over someone's shoulder as they type a password. This can be effective when the hacker is in close proximity to the user and the system. Special screens that make it difficult to see the computer screen from an angle can cut down on shoulder surfing. In addition, employee awareness and training can virtually eliminate this type of attack.



Real World Scenario

Shoulder Surfing

Sue is a receptionist at a busy doctor's office. She was working at her computer when a flower delivery man came into the office. He told Sue he had a flower delivery for Dr. Smith. This was the doctor's name he saw on the front door of the office as he entered the waiting room.

Sue was busy that day and Dr. Smith was in with a patient, so she told the flower delivery man that he could leave the flowers on the desk and she would make sure the doctor received them. He said he needed to wait and give them directly to the person who was listed on the delivery ticket. So, Sue asked him to stay in the waiting room until Dr. Smith was available to receive the flower delivery. As Sue turned back to her computer to finish writing an email she had started, she was distracted thinking about the work she had in front of her. She quickly typed the password to unlock her Windows workstation. The flower delivery man paused for just a moment before turning to take a seat in the waiting room. As he paused, he was able to see the five-character password Sue typed to unlock her screen. It was in this manner that he was able to discern her password and continue the hacking process. The password was gathered using shoulder surfing, a form of social engineering.

Dumpster diving hackers look through the trash for information such as passwords, which may be written down on a piece of paper. Again, security awareness training on shredding important documents can prevent a hacker from gathering passwords by dumpster diving.

Cracking a Password

Manual password cracking involves attempting to log on with different passwords. The hacker follows these steps:

1. Find a valid user account (such as Administrator or Guest).
2. Create a list of possible passwords.
3. Rank the passwords from high to low probability.
4. Key in each password.
5. Try again until a successful password is found.

A hacker can also create a script file that tries each password in a list. This is still considered manual cracking, but it's time consuming and not usually effective.

A more efficient way of cracking a password is to gain access to the password file on a system. Most systems *hash* (one-way encrypt) a password for storage on a system. During the logon process, the password entered by the user is hashed using the same algorithm and then compared to the hashed passwords stored in the file. A hacker can attempt to gain access to the hashing algorithm stored on the server instead of trying to guess or otherwise identify the password. If the hacker is successful, they can decrypt the passwords stored on the server.



Passwords are stored in the Security Accounts Manager (SAM) file on a Windows system and in a password shadow file on a Linux system.

Hacking Tools

Legion automates the password guessing in NetBIOS sessions. Legion scans multiple IP address ranges for Windows shares and also offers a manual dictionary attack tool.

NTInfoScan is a security scanner for NT 4.0. This vulnerability scanner produces an HTML-based report of security issues found on the target system and other information.

L0phtCrack is a password auditing and recovery package distributed by @stake software, which is now owned by Symantec. It performs Server Message Block (SMB) packet captures on the local network segment and captures individual login sessions. L0phtCrack contains dictionary, brute-force, and hybrid attack capabilities. Symantec has recently stopped development of the L0phtCrack tool, but it can still be found on the Internet.

LC5 is another good password cracking tool. LC5 is a suitable replacement for L0phtCrack.

John the Ripper is a command-line tool designed to crack both Unix and NT passwords. The cracked passwords are case insensitive and may not represent the real mixed-case password.

KerbCrack consists of two programs: kerbsniff and kerbcrack. The sniffer listens on the network and captures Windows 2000/XP Kerberos logins. The cracker can be used to find the passwords from the capture file using a brute-force attack or a dictionary attack.

Understanding the LAN Manager Hash

Windows 2000 uses NT LAN Manager (NTLM) hashing to secure passwords in transit on the network. Depending on the password, NTLM hashing can be weak and easy to break. For example, let's say that the password is 123456abcdef. When this password is encrypted with the NTLM algorithm, it's first converted to all uppercase: 123456ABCDEF. The password is padded with null (blank) characters to make it 14 characters long: 123456ABCDEF__. Before the password is encrypted, the 14-character string is split in half: 123456A and BCDEF__. Each string is individually encrypted, and the results are concatenated:

123456A = 6BF11E04AFAB197F

BCDEF__ = F1E9FFDCC75575B15

The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15.



The first half of the password contains alphanumeric characters; L0phtCrack will take 24 hours to crack this part. The second half contains only letters and symbols and will take 60 seconds to crack. This is because there are many fewer combinations in the second half of the hashed password. If the password is seven characters or fewer, the second half of the hash will always be AAD3B435B51404EE.

Cracking Windows 2000 Passwords

The SAM file in Windows contains the usernames and hashed passwords. It's located in the Windows\system32\config directory. The file is locked when the operating system is running so that a hacker can't attempt to copy the file while the machine is booted to Windows.

One option for copying the SAM file is to boot to an alternate operating system such as DOS or Linux with a boot CD. Alternately, the file can be copied from the repair directory. If a system administrator uses the RDISK feature of Windows to back up the system,

then a compressed copy of the SAM file called `SAM._` is created in `C:\windows\repair`. To expand this file, use the following command at the command prompt:

```
C:\>expand sam._ sam
```

After the file is uncompressed, a dictionary, hybrid, or brute-force attack can be run against the SAM file using a tool like L0phtCrack. A similar tool to L0phtcrack is Ophcrack. Exercise 4.1 illustrates how to use Ophcrack to crack passwords.

Hacking Tools

Win32CreateLocalAdminUser is a program that creates a new user with the username and password X and adds the user to the local administrator's group. This action is part of the Metasploit Project and can be launched with the Metasploit framework on Windows.

Offline NT Password Resetter is a method of resetting the password to the administrator's account when the system isn't booted to Windows. The most common method is to boot to a Linux boot CD and then access the NTFS partition, which is no longer protected, and change the password.

EXERCISE 4.1

Use Ophcrack to Crack Passwords

1. Download and install ophcrack from <http://ophcrack.sourceforge.net/>.
2. Run the ophcrack program and set the number of threads under the Preferences tab to the number of cores of the computer running ophcrack plus one. If you change this value, you have to exit ophcrack and restart it in order to save the change.

Note: This step is optional but will speed up the cracking process.

3. Click the Load button to add hashes. There are numerous ways to add the hashes:
 - Enter the hash manually (Single Hash option)
 - Import a text file containing hashes you created with pwdump, fgdump, or similar third-party tools (PWDUMP File option)
 - Extract the hashes from the SYSTEM and SAM files (Encrypted SAM option)
 - Dump the SAM from the computer ophcrack is running on (Local SAM option)
 - Dump the SAM from a remote computer (Remote SAM option)

EXERCISE 4.1 (continued)

Note: For the Encrypted SAM option, the SAM is located under the Windows system32/config directory and can only be accessed for a Windows partition that is *not* running. For the Local SAM and Remote SAM options, you must be logged in with the administrator rights on the computer you want to dump the SAM.

4. Click the Tables button.
5. Click the enable (green and yellow) buttons.
6. Using the up and down arrows, sort the rainbow tables you are going to use. Keep in mind that storing the rainbow tables on a fast medium like a hard disk will significantly speed up the cracking process.
7. Click the Crack button to start the cracking process. You'll see the progress of the cracking process in the bottom boxes of the ophcrack window. When a password is found, it will be displayed in the NT Pwd field. You can save the results of a cracking session at any time by clicking the Save button.

Redirecting the SMB Logon to the Attacker

Another way to discover passwords on a network is to redirect the Server Message Block (SMB) logon to an attacker's computer so that the passwords are sent to the hacker. In order to do this, the hacker must sniff the NTLM responses from the authentication server and trick the victim into attempting Windows authentication with the attacker's computer. A common technique is to send the victim an email message with an embedded link to a fraudulent SMB server. When the link is clicked, the user unwittingly sends their credentials over the network.

SMBRelay An SMB server that captures usernames and password hashes from incoming SMB traffic. SMBRelay can also perform man-in-the-middle (MITM) attacks.

SMBRelay2 Similar to SMBRelay but uses NetBIOS names instead of IP addresses to capture usernames and passwords.

pwdump2 A program that extracts the password hashes from a SAM file on a Windows system. The extracted password hashes can then be run through L0phtCrack to break the passwords.

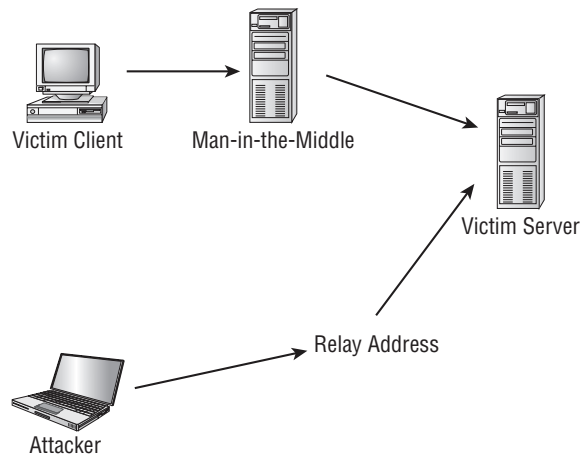
Samdump Another program that extracts NTLM hashed passwords from a SAM file.

C2MYAZZ A spyware program that makes Windows clients send their passwords as cleartext. It displays usernames and their passwords as users attach to server resources.

SMB Relay MITM Attacks and Countermeasures

An SMB relay MITM attack is when the attacker sets up a fraudulent server with a relay address. When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password, and passes the connection to the victim server. Figure 4.1 illustrates such an attack.

FIGURE 4.1 SMB relay MITM attack



SMB relay countermeasures include configuring Windows 2000 to use SMB signing, which causes it to cryptographically sign each block of SMB communications.

Hacking Tools

SMBGrind increases the speed of L0phtCrack sessions on sniffer dumps by removing duplication and providing a way to target specific users without having to edit the dump files manually.

The SMBDie tool crashes computers running Windows 2000, XP, or NT by sending specially crafted SMB requests.

NBTdeputy can register a NetBIOS computer name on a network and respond to NetBIOS over TCP/IP (NetBT) name-query requests. It simplifies the use of SMBRelay. The relay can be referred to by computer name instead of IP address.

NetBIOS DoS Attacks

A NetBIOS denial-of-service (DoS) attack sends a NetBIOS Name Release message to the NetBIOS Name Service on a target Windows systems and forces the system to place its name in conflict so that the name can no longer be used. This essentially blocks the client from participating in the NetBIOS network and creates a network DoS for that system.

Hacking Tool

NBName can disable entire LANs and prevent machines from rejoining them. Nodes on a NetBIOS network infected by the tool think that their names are already in use by other machines.

Another way to create a more secure and memorable password is to follow a repeatable pattern, which will enable to password to be re-created when needed.

1. Start with a memorable phrase, such as
Maryhadalittlelamb
2. Change every other character to uppercase, resulting in
MaRyHaDaLiTtLeLaMb
3. Change a to @ and i to 1 to yield
M@RyH@D@L1TtLeL@Mb
4. Drop every other pair to result in a secure repeatable password or
M@H@L1LeMb

Now you have a password that meets all the requirements, yet can be “remade” if necessary.

Password-Cracking Countermeasures

The strongest passwords possible should be implemented to protect against password cracking. Systems should enforce 8–12-character alphanumeric passwords. The length of time the same password should be used is discussed in the next section.

To protect against cracking of the hashing algorithm for passwords stored on the server, you must take care to physically isolate and protect the server. The system administrator can use the SYSKEY utility in Windows to further protect hashes stored on the server’s hard disk. The server logs should also be monitored for brute-force attacks on user accounts.

A system administrator can implement the following security precautions to decrease the effectiveness of a brute-force password-cracking attempt:

- Never leave a default password.
- Never use a password that can be found in a dictionary.
- Never use a password related to the hostname, domain name, or anything else that can be found with Whois.
- Never use a password related to your hobbies, pets, relatives, or date of birth.
- As a last resort, use a word that has more than 21 characters from a dictionary as a password.



This subject is discussed further in the section “Monitoring Event Viewer Logs,” later in this chapter.

In the following sections, we’ll look at two measures you can take to strengthen passwords and prevent password-cracking.

Password Change Interval

Passwords should expire after a certain amount of time so that users are forced to change them. If the password interval is set too low, users will forget their current passwords; as a result, a system administrator will have to reset users’ passwords frequently. On the other hand, if passwords are allowed to be used for too long, security may be compromised. The recommended password-change interval is every 30 days. In addition, most security professionals recommended that users not be allowed to reuse the last three passwords.



You cannot completely block brute-force password attacks if the hacker switches the proxy server where the source packet is generated. A system administrator can only add security features to decrease the likelihood that brute-force password attacks will be useful.

Monitoring Event Viewer Logs

Administrators should monitor Event Viewer logs to recognize any intrusion attempts either before they take place or while they’re occurring. Generally, several failed attempts are logged in the system logs before a successful intrusion or password attack. The security logs are only as good as the system administrators who monitor them.

Tools such as VisualLast aid a network administrator in deciphering and analyzing the security log files. VisualLast provides greater insight into the NT event logs so the administrator can assess the activity of the network more accurately and efficiently. The program is designed to allow network administrators to view and report individual users’ logon and

logoff times; these events may be searched according to time frame, which is invaluable to security analysts who are looking for intrusion details.

The event log located at `c:\windows\system32\config\Sec.Event.Evt` contains the trace of an attacker's brute-force attempts.

Understanding Keyloggers and Other Spyware Technologies

If all other attempts to gather passwords fail, then a *keystroke logger* is the tool of choice for hackers. Keystroke loggers (keyloggers) can be implemented either using hardware or software. Hardware keyloggers are small hardware devices that connect the keyboard to the PC and save every keystroke into a file or in the memory of the hardware device. In order to install a hardware keylogger, a hacker must have physical access to the system.

Software keyloggers are pieces of stealth software that sit between the keyboard hardware and the operating system so that they can record every keystroke. Software keyloggers can be deployed on a system by Trojans or viruses.



Using Trojans and viruses will be discussed in Chapter 5, "Installing Software on Target Systems: Spyware, Trojans, Backdoors, Viruses, and Worms."

Hacking Tools

Spector is spyware that records everything a system does on the Internet, much like a surveillance camera. Spector automatically takes hundreds of snapshots every hour of whatever is on the computer screen and saves these snapshots in a hidden location on the system's hard drive. Spector can be detected and removed with Anti-spector.

eBlaster is Internet spy software that captures incoming and outgoing emails and immediately forwards them to another email address. eBlaster can also capture both sides of an Instant Messenger conversation, perform keystroke logging, and record websites visited.

SpyAnywhere is a tool that allows you to view system activity and user actions, shut down/restart, lock down/freeze, and even browse the file system of a remote system. SpyAnywhere lets you control open programs and windows on the remote system and view Internet histories and related information.

Invisible KeyLogger Stealth (IKS) Software Logger is a high-performance virtual device driver (VxD) that runs silently at the lowest level of the Windows 95, 98, or ME operating system. All keystrokes are recorded in a binary keystroke file.

Fearless Key Logger is a Trojan that remains resident in memory to capture all user keystrokes. Captured keystrokes are stored in a log file and can be retrieved by a hacker.

E-mail Keylogger logs all emails sent and received on a target system. The emails can be viewed by sender, recipient, subject, and time/date. The email contents and any attachments are also recorded.

Escalating Privileges

Escalating privileges is the third step in the hacking cycle. *Escalating privileges* basically means adding more rights or permissions to a user account. Simply said, escalating privileges makes a regular user account into an administrator account.

Generally, administrator accounts have more stringent password requirements, and their passwords are more closely guarded. If it isn't possible to find a username and password of an account with administrator privileges, a hacker may choose to use an account with lower privileges. In this case, the hacker must then escalate that account's privileges.

This is accomplished by first gaining access using a nonadministrator user account—typically by gathering the username and password through one of the previously discussed methods—and then increasing the privileges on the account to the level of an administrator.

Hacking Tools

GetAdmin.exe is a small program that adds a user to the local administrators group. It uses a low-level NT kernel routine to allowing access to any running process. A logon to the server console is needed to execute the program. GetAdmin.exe is run from the command line or from a browser. It works only with Windows NT 4.0 Service Pack 3.

The Hk.exe utility exposes a local procedure call (LPC) flaw in Windows NT. A nonadministrator user can be escalated to the administrators group using this tool.

Once a hacker has a valid user account and password, the next step is to execute applications. Generally the hacker needs to have an account with administrator-level access in

order to install programs, and that is why escalating privileges is so important. In the following sections, we'll see what hackers can do with your system once they have administrator privileges.

Executing Applications

Once a hacker has been able to access an account with administrator privileges, the next thing they do is execute applications on the target system. The purpose of executing applications may be to install a backdoor on the system, install a keystroke logger to gather confidential information, copy files, or just cause damage to the system—essentially, anything the hacker wants to do on the system.

Once the hacker is able to execute applications, the system is considered *owned* and under the control of the hacker.

Hacking Tools

Psexec is a program that connects to and executes files on remote systems. No software needs to be installed on the remote system.

Remotexec executes a program using RPC (Task Scheduler) or DCOM (Windows Management Instrumentation) services. Administrators with null or weak passwords may be exploited through Task Scheduler (1025/tcp or above) or Distributed Component Object Mode (DCOM; default 135/tcp).

Buffer Overflows

Buffer overflows are hacking attempts that exploit a flaw in an application's code. Essentially, the buffer overflow attack sends too much information to a field variable in an application, which can cause an application error. Most times, the application doesn't know what action to perform next because it's been overwritten with the overflow data. Therefore, it either executes the command in the overflow data or displays a command prompt to allow the user to enter the next command. The command prompt or shell is the key for a hacker and can be used to execute other applications.



Buffer overflows will be discussed in greater detail in Chapter 9, "Attacking Applications: SQL Injection and Buffer Overflows."

Understanding Rootkits

A rootkit is a type of program often used to hide utilities on a compromised system. Rootkits include so-called *backdoors* to help an attacker subsequently access the system more easily. For example, the rootkit may hide an application that spawns a shell when the attacker connects to a particular network port on the system. A backdoor may also allow processes started by a nonprivileged user to execute functions normally reserved for the administrator. A rootkit is frequently used to allow the programmer of the rootkit to see and access usernames and log-in information for sites that require them.

There are several types of rootkits, including the following:

Kernel-Level Rootkits Kernel-level rootkits add code and/or replace a portion of kernel code with modified code to help hide a backdoor on a computer system. This is often accomplished by adding new code to the kernel via a device driver or loadable module, such as loadable kernel modules in Linux or device drivers in Windows. Kernel-level rootkits are especially dangerous because they can be difficult to detect without appropriate software.

Library-Level Rootkits Library-level rootkits commonly patch, hook, or replace system calls with versions that hide information that might allow the hacker to be identified.

Application-Level Rootkits Application-level rootkits may replace regular application binaries with Trojanized fakes, or they may modify the behavior of existing applications using hooks, patches, injected code, or other means.

In the following sections, we'll explore the process of infecting a system with a rootkit.

Planting Rootkits on Windows 2000 and XP Machines

The Windows NT/2000 rootkit is built as a kernel-mode driver, which can be dynamically loaded at runtime. The rootkit runs with system privileges at the core of the NT kernel, so it has access to all the resources of the operating system. The rootkit can also hide processes, hide files, hide Registry entries, intercept keystrokes typed at the system console, issue a debug interrupt to cause a blue screen of death, and redirect EXE files.

The rootkit contains a kernel mode device driver called `_root_.sys` and a launcher program called `DEPLOY.EXE`. After gaining access to the target system, the attacker copies `_root_.sys` and `DEPLOY.EXE` onto the target system and executes `DEPLOY.EXE`. Doing so installs the rootkit device driver and starts it. The attacker later deletes `DEPLOY.EXE` from the target machine. The attacker can then stop and restart the rootkit at will by using the commands `net stop _root_` and `net start _root_`. Once the rootkit is started, the file `_root_.sys` no longer appears in directory listings; the rootkit intercepts system calls for file listings and hides all files beginning with `_root_` from display.

Rootkit Embedded TCP/IP Stack

A new feature of the Windows NT/2000 rootkit is a stateless TCP/IP stack. It works by determining the state of the connection based on the data in the incoming packet. The

rootkit has a hard-coded IP address (10.0.0.166) to which it will respond. The rootkit uses raw Ethernet connections to the system's network card, so it's very powerful. The target port doesn't matter; a hacker can telnet to any port on the system. In addition, multiple people can log into the rootkit at once.

Rootkit Countermeasures

All rootkits require administrator access to the target system, so password security is critical. If you detect a rootkit, you should back up critical data and reinstall the operating system and applications from a trusted source. The administrator should also keep available a well-documented automated installation procedure and trusted restoration media.

Another countermeasure is to use the *MD5 checksum* utility. The MD5 checksum for a file is a 128-bit value, something like the file's fingerprint. (There is a small possibility of getting two identical checksums for two different files.) This algorithm is designed so that changing even one bit in the file data causes a different checksum value. This feature can be useful for comparing files and ensuring their integrity. Another good feature is the checksum's fixed length, regardless of the size of the source file.

The MD5 checksum makes sure a file hasn't changed. This can be useful in checking file integrity if a rootkit has been found on a system. Tools such as Tripwire implement MD5 checksums to identify files affected by the rootkit.

Countermeasure Tools

Tripwire is a file system integrity-checking program for Unix and Linux operating systems. In addition to one or more cryptographic checksums representing the contents of each directory and file, the Tripwire database also contains information that lets you verify access permissions and file mode settings, the username of the file owner, the date and time the file was last accessed, and the last modification made to the item.

Hiding Files

A hacker may want to hide files on a system to prevent their detection. These files may then be used to launch an attack on the system. There are two ways to hide files in Windows. The first is to use the `attrib` command. To hide a file with the `attrib` command, type the following at the command prompt:

```
attrib +h [file/directory]
```

The second way to hide a file in Windows is with NTFS alternate data streaming. NTFS file systems used by Windows NT, 2000, and XP have a feature called *alternate data streams*

that allow data to be stored in hidden files linked to a normal, visible file. Streams aren't limited in size; more than one stream can be linked to a normal file.

NTFS File Streaming

NTFS file streaming allows a hidden file to be created within a legitimate file. The hidden file does not appear in a directory listing but the legitimate file does. A user would usually not suspect the legitimate file, but the hidden file can be used to store or transmit information. In Exercise 4.2, you'll learn how to hide files using NTFS file streaming.

EXERCISE 4.2

Hiding Files Using NTFS File Streaming

Note: This exercise will only work on systems using the NTFS file system.

To create and test an NTFS file stream:

1. At the command line, enter **notepad test.txt**.
2. Put some data in the file, save the file, and close Notepad. Step 1 will open Notepad.
3. At the command line, enter **dir test.txt** and note the file size.
4. At the command line, enter **notepad test.txt:hidden.txt**. Type some text into Notepad, save the file, and close it.
5. Check the file size again (it should be the same as in step 3).
6. Open **test.txt**. You see only the original data.
7. Enter **type test.txt:hidden.txt** at the command line. A syntax error message is displayed.

Hacking Tool

makestrm.exe is a utility that moves the data from a file to an alternate data stream linked to the original file.

NTFS Stream Countermeasures

To delete a stream file, copy the first file to a FAT partition, and then copy it back to an NTFS partition.

Streams are lost when the file is moved to a FAT partition because they're a feature of NTFS and therefore exist only on an NTFS partition.

Countermeasure Tool

You can use `lms.exe` to detect NTFS streams. LMS reports the existence and location of files that contain alternate data streams.

Understanding Steganography Technologies

Steganography is the process of hiding data in other types of data such as images or text files. The most popular method of hiding data in files is to utilize graphic images as hiding places. Attackers can embed any information in a graphic file using steganography. The hacker can hide directions on making a bomb, a secret bank account number, or answers to a test. Any text imaginable can be hidden in an image. In Exercise 4.3 you will use Image Hide to hide text within an image.

Hacking Tools

ImageHide is a steganography program that hides large amounts of text in images. Even after adding bytes of data, there is no increase in the image size. The image looks the same in a normal graphics program. It loads and saves to files and therefore is able to bypass most email sniffers.

Blindside is a steganography application that hides information inside BMP (bitmap) images. It's a command-line utility.

MP3Stego hides information in MP3 files during the compression process. The data is compressed, encrypted, and then hidden in the MP3 bitstream.

Snow is a whitespace steganography program that conceals messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs generally aren't visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message can't be read even if it's detected.

CameraShy works with Windows and Internet Explorer and lets users share censored or sensitive information stored in an ordinary GIF image.

Stealth is a filtering tool for PGP files. It strips off identifying information from the header, after which the file can be used for steganography.

EXERCISE 4.3**Hiding Data in an Image Using ImageHide**

To hide data in an image using ImageHide:

1. Download and install the ImageHide program.
2. Add an image in the Image Hide program.
3. Add text in the field at the bottom of the ImageHide screen.
4. Hide the text within the image using ImageHide.

Steganography can be detected by some programs, although doing so is difficult. The first step in detection is to locate files with hidden text, which can be done by analyzing patterns in the images and changes to the color palette.

Countermeasure Tools

Stegdetect is an automated tool for detecting steganographic content in images. It's capable of detecting different steganographic methods to embed hidden information in JPEG images.

Dskprobe is a tool on the Windows 2000 installation CD. It's a low-level hard-disk scanner that can detect steganography.

Covering Your Tracks and Erasing Evidence

Once intruders have successfully gained administrator access on a system, they try to cover their tracks to prevent detection of their presence (either current or past) on the system. A hacker may also try to remove evidence of their identity or activities on the system to prevent tracing of their identity or location by authorities. To prevent detection, the hacker usually erases any error messages or security events that have been logged. Disabling auditing and clearing the event log are two methods used by a hacker to cover their tracks and avoid detection.

The first thing intruders do after gaining administrator privileges is disable auditing. Windows auditing records certain events in a log file that is stored in the Windows Event Viewer. Events can include logging into the system, an application, or an event log. An administrator can choose the level of logging implemented on a system. Hackers want to

determine the level of logging implemented to see whether they need to clear events that indicate their presence on the system.

Hacking Tool

Auditpol is a tool included in the Windows NT Resource Kit for system administrators. This tool can disable or enable auditing from the Windows command line. It can also be used to determine the level of logging implemented by a system administrator.

Intruders can easily wipe out the security logs in the Windows Event Viewer. An event log that contains one or just a few events is suspicious because it usually indicates that other events have been cleared. It's still necessary to clear the event log after disabling auditing, because using the Auditpol tool places an entry in the event log indicating that auditing has been disabled. Several tools exist to clear the event log, or a hacker can do so manually in the Windows Event Viewer.

Hacking Tools

The `elsave.exe` utility is a simple tool for clearing the event log. It's command line based.

WinZapper is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000. WinZapper also ensures that no security events are logged while the program is running.

Evidence Eliminator is a data-cleansing system for Windows PCs. It prevents unwanted data from becoming permanently hidden in the system. It cleans the Recycle Bin, Internet cache, system files, temp folders, and so on. Evidence Eliminator can also be used by a hacker to remove evidence from a system after an attack.

Summary

The actual hacking of a target system can be broken down into simple steps. Guessing or cracking passwords, escalating privileges, hiding files, and covering tracks are all parts of the hacking process. It is these steps that usually uncover the most valuable information for hackers. However, the information-gathering and scanning steps should not be forgotten as they are critical in getting the most information about a target and its weaknesses. Good information gathering can greatly improve the success and speed of the hacking steps.

Exam Essentials

Understand the importance of password security. Implementing password-change intervals, strong alphanumeric passwords, and other password security measures is critical to network security.

Know the different types of password attacks. Passive online attacks include sniffing, man-in-the-middle, and replay. Active online attacks include passive and automated password guessing. Offline attacks include dictionary, hybrid, and brute force. Nonelectronic attacks include shoulder surfing, keyboard sniffing, and social engineering.

Understand the various types of offline password attacks. Dictionary, hybrid, and brute-force attacks are all offline password attacks.

Know the ways to defend against password guessing. Smart cards and biometrics are two ways to increase security and defend against password guessing.

Understand the differences between the types of nonelectronic attacks. Social engineering, shoulder surfing, and dumpster diving are all types of nonelectronic attacks.

Know how evidence of hacking activity is eliminated by attackers. Clearing event logs and disabling auditing are methods that attackers use to cover their tracks.

Realize that hiding files are means used to sneak out sensitive information. Steganography, NTFS streaming, and the attrib command are all ways hackers can hide and steal files.

Review Questions

1. What is the process of hiding text within an image called?
 - A. Steganography
 - B. Encryption
 - C. Spyware
 - D. Keystroke logging
2. What is a rootkit?
 - A. A simple tool to gain access to the root of the Windows system
 - B. A Trojan that sends information to an SMB relay
 - C. An invasive program that affects the system files, including the kernel and libraries
 - D. A tool to perform a buffer overflow
3. Why would hackers want to cover their tracks?
 - A. To prevent another person from using the programs they have installed on a target system
 - B. To prevent detection or discovery
 - C. To prevent hacking attempts
 - D. To keep other hackers from using their tools
4. What is privilege escalation?
 - A. Creating a user account with higher privileges
 - B. Creating a user account with administrator privileges
 - C. Creating two user accounts: one with high privileges and one with lower privileges
 - D. Increasing privileges on a user account
5. What are two methods used to hide files? (Choose all that apply.)
 - A. NTFS file streaming
 - B. `attrib` command
 - C. Steganography
 - D. Encrypted File System
6. What is the recommended password-change interval?
 - A. 30 days
 - B. 20 days
 - C. 1 day
 - D. 7 days

7. What type of password attack would be most successful against the password T63k#s23A?
 - A. Dictionary
 - B. Hybrid
 - C. Password guessing
 - D. Brute force
8. Which of the following is a passive online attack?
 - A. Password guessing
 - B. Network sniffing
 - C. Brute-force attack
 - D. Dictionary attack
9. Why is it necessary to clear the event log after using the `auditpol` command to turn off logging?
 - A. The `auditpol` command places an entry in the event log.
 - B. The `auditpol` command doesn't stop logging until the event log has been cleared.
 - C. `auditpol` relies on the event log to determine whether logging is taking place.
 - D. The event log doesn't need to be cleared after running the `auditpol` command.
10. What is necessary in order to install a hardware keylogger on a target system?
 - A. The IP address of the system
 - B. The administrator username and password
 - C. Physical access to the system
 - D. Telnet access to the system
11. What is the easiest method to get a password?
 - A. Brute-force cracking
 - B. Guessing
 - C. Dictionary attack
 - D. Hybrid attack
12. Which command is used to cover tracks on a target system?
 - A. `elsave`
 - B. `coverit`
 - C. `legion`
 - D. `nmap`

13. What type of hacking application is Snow?
 - A. Password cracker
 - B. Privilege escalation
 - C. Spyware
 - D. Steganography
14. What is the first thing a hacker should do after gaining administrative access to a system?
 - A. Create a new user account
 - B. Change the administrator password
 - C. Copy important data files
 - D. Disable auditing
15. Which of the following programs is a steganography detection tool?
 - A. Stegdetect
 - B. Stegoalert
 - C. Stegstopper
 - D. Stegorama
16. Which countermeasure tool will detect NTFS streams?
 - A. Windows Security Manager
 - B. LNS
 - C. Auditpol
 - D. RPS
17. Which program is used to create NTFS streams?
 - A. StreamIT
 - B. makestrm.exe
 - C. NLS
 - D. Windows Explorer
18. Why is it important to clear the event log after disabling auditing?
 - A. An entry is created that the administrator has logged on.
 - B. An entry is created that a hacking attempt is underway.
 - C. An entry is created that indicates auditing has been disabled.
 - D. The system will shut down otherwise.

19. What is the most dangerous type of rootkit?
- A. Kernel level
 - B. Library level
 - C. System level
 - D. Application level
20. What is the command to hide a file using the `attrib` command?
- A. `att +h [file/directory]`
 - B. `attrib +h [file/directory]`
 - C. `attrib hide [file/directory]`
 - D. `hide [file/directory]`

Answers to Review Questions

1. A. Steganography is the process of hiding text within an image.
2. C. A rootkit is a program that modifies the core of the operating system: the kernel and libraries.
3. B. Hackers cover their tracks to keep from having their identity or location discovered.
4. D. Privilege escalation is a hacking method to increase privileges on a user account.
5. A, B. NTFS file streaming and the `attrib` command are two hacking techniques used to hide files.
6. A. Passwords should be changed every 30 days for the best balance of security and usability.
7. D. A brute-force attack tries every combination of letters, numbers, and symbols.
8. B. Network sniffing is a passive online attack because it can't be detected.
9. A. The event log must be cleared because the `auditpol` command places an entry in the event log indicating that logging has been disabled.
10. C. A hardware keylogger is an adapter that connects the keyboard to the PC. A hacker needs physical access to the PC in order to plug in the hardware keylogger.
11. B. The easiest way to get a password is to guess the password. For this reason it is important to create strong passwords and to not reuse passwords.
12. A. `elsave` is a command used to clear the event log and cover a hacker's tracks.
13. D. Snow is a steganography program used to hide data within the whitespace of text files.
14. D. The first thing a hacker should do after gaining administrative level access to a system is disable system auditing to prevent detection and attempt to cover tracks.
15. A. Stegdetect is a steganography detection tool.
16. B. LNS is an NTFS countermeasure tool used to detect NTFS streams.
17. B. `makestrm.exe` is a program used to make NTFS streams.
18. C. It is important to clear the event log after disabling auditing because an entry is created indicating that auditing is disabled.
19. A. A kernel-level rootkit is the most dangerous because it infects the core of the system.
20. B. `attrib +h [file/directory]` is the command used to hide a file using the `hide` attribute.

