

ATME COLLEGE OF ENGINEERING

13th KM Stone, Bannur Road, Mysore - 560 028



A T M E

College of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
- CYBER SECURITY



LECTURE NOTES

COURSE: Hackers Technique, Tools and Incident Handling

COURSE CODE: BCY515C

SEMESTER: V

COURSE COORDINATOR: Ms. Darshini Y

(ACADEMIC YEAR 2026)

INSTITUTIONAL MISSION AND VISION

Objectives

- To provide quality education and groom top-notch professionals, entrepreneurs and leaders for different fields of engineering, technology and management.
- To open a Training-R & D-Design-Consultancy cell in each department, gradually introduce doctoral and postdoctoral programs, encourage basic & applied research in areas of social relevance, and develop the institute as a center of excellence.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To cultivate strong community relationships and involve the students and the staff in local community service.
- To constantly enhance the value of the educational inputs with the participation of students, faculty, parents and industry.

Vision

Development of academically excellent, culturally vibrant, socially responsible and globally competent human resources.

Mission

- To keep pace with advancements in knowledge and make the students competitive and capable at the global level.
- To create an environment for the students to acquire the right physical, intellectual, emotional and moral foundations and shine as torch bearers of tomorrow's society.
- To strive to attain ever-higher benchmarks of educational excellence

Chapter 1 :Windows Basics

The Windows operating system can be used as both a standalone and a networked operating system, but for the purposes of this chapter you will consider mostly the networked aspects of the operating system (OS). It is important to consider what needs to be secured and how to secure the operating system in the networked environment. One of the big issues of securing Windows in the networked environment is the sheer number of features that must be considered and locked down to prevent exploitation. However, before we can determine what to secure, we need to know how Windows works.

Controlling Access

One of the first things that must be understood prior to securing Windows is how access to resources such as file shares and other items is managed. Windows uses a model that can be best summed up as defining who gets access to what resources. For example, a user gets access to a file share or printer.

NOTE

Always consider what a user account will be used for, because that will dictate what privileges it needs and what ones it doesn't. For example, if a user will never be performing administrative tasks, don't give the user administrative access.

Users

In the Windows OS, the fundamental object that is used to determine access is the user account. User accounts are used in Windows to access everything from files shares to run services that keep the system functioning. In fact, most of the services and processes that run on the Windows operating system run with the help of a user account, but the question is, which one. Processes in Windows are run under one of four user contexts:

- **Local Service**—A user account with greater access to the local system, but limited access to the network
- **Network Service**—A user account with greater access to the network, but limited access to the local system
- **SYSTEM**—A super-user style account that gets nearly unlimited access to the local system and can perform actions on the local system with little or no restriction
- **Current User**—The currently logged-in user who can run applications and tasks, but still is subject to restrictions that other users are not subject to. The restrictions on this account hold true even if the user account being used is an Administrator account.

Each of these user accounts is used for different specific reasons, and in a typical Windows session each is running different processes behind the scenes to keep the system performing.

FYI

Prior to the introduction of Windows XP, all system services ran under the SYSTEM account, which allowed all the services to run as designed, but also gave each service more access than it needed. With each service running with what was essentially no restrictions, the potential for widespread harm if a service was compromised was unacceptable. Starting in Windows XP on up to the current version of Windows system, services run under an account with the appropriate level of access to perform their tasks and none of the extra access that could be a hazard. As will be seen later, this setup limits the amount of damage an attacker could cause if a service were compromised.

Table 7-1. SAM changes in Windows.

NAME	EARLIEST VERSION	WINDOWS SUPPORTED	DESCRIPTION
LAN Manager (LM)		Windows for Workgroups	Considered weak due to the way hashes are created and stored
NT Manager (NTLM)		Windows NT	Stronger than LM, but somewhat similar
Kerberos		Windows 2000	Available with Active Directory

User account information can be physically stored in two locations on a Windows system: in the SAM or in Active Directory. The **Security Account Manager (SAM)** is a database on the local system that is used to store user account information. By default, the SAM resides within the Windows folder %WINNT%\system32\config\sam. This is true of all versions of Windows clients or servers. The other method of storing user information is in Active Directory, which is used in larger network environments such as those present in mid- to enterprise-level businesses. For simplicity, this chapter will not discuss Active Directory. Inside the SAM are a few items that should be covered prior to moving forward with other features; namely, some of the storage details that occur here. The SAM stores within it hashed versions of users' passwords used to authenticate user accounts; these hashes are stored in a number of different ways depending on the version of Windows. The hash details are listed in [Table 7-1](#).

NOTE

Remember that the SAM is a file that physically resides on the hard drive and is actively accessed while Windows is running.

Groups

Groups are used by Windows to grant access to resources and to simplify management. Groups are effective administration tools that enable management of multiple users because a group can contain a large number of users that can then be managed as a unit. By using groups, you can assign access to a resource such as a shared folder to a group instead of each user individually, saving substantial time and effort. You can configure your own groups as you see fit on your network and systems, but most vendors such as Microsoft include a number of predefined groups that you can use as well or modify as needed. There are several default groups in Windows, discussed in the following list:

- **Anonymous logon**—Designed to allow anonymous access to resources; typically used when accessing the Web server or Web applications
- **Batch**—Used to allow batch jobs to run schedule tasks, such as a nightly cleanup job that deletes temporary files
- **Creator Group**—Windows 2000 uses this group to automatically grant access permissions to users who are members of the same group(s) as the creator of a file or a directory.
- **Creator Owner**—The person who created the file or the directory is a member of this group. Windows 2000 uses this group to automatically grant access permissions to the creator of a file or directory.
- **Everyone**—All interactive, network, dial-up, and authenticated users are members of this group. This group is used to give wide access to a system resource.
- **Interactive**—Any user logged on to the local system has the Interactive identity, which allows only local users to access a resource.
- **Network**—Any user accessing the system through a network has the Network identity, which allows only remote users to access a resource.
- **Restricted**—Users and computers with restricted capabilities have the Restricted identity. On a member server or workstation, a local user who is a member of the Users group (rather than the Power Users group) has this identity.
- **Self**—Refers to the object itself and allows the object to modify itself
- **Service**—Any service accessing the system has the Service identity, which grants access to processes being run by Windows 2000 services.
- **System**—The Windows 2000 operating system has the System identity, which is used when the operating system needs to perform a system-level function.
- **Terminal Server User**—Allows terminal server users to access terminal server applications and to perform other necessary tasks with terminal services

Source: <http://technet.microsoft.com/en-us/library/bb726982.aspx>

Security Identifiers

Each user account in Windows has a unique ID assigned to it commonly known as a security identifier (SID) that is used to identify the account or group. The SID is a combination of characters that looks like the following:

S-1-5-32-1045337234-12924708993-5683276719-19000

WHY ALL THE CODES?

SIDs may not sound like a good idea, but you need to look at why they are being used instead of the actual usernames. For a moment, consider usernames and SIDs to be like a person and his or her phone number. If you were to go to any city in the world, you would find multiple people with the same first name, but it is unlikely that those people would share the same phone number. In Windows, once a SID is used it is never reused, meaning that even if the username is the same, Windows doesn't treat it as the same. By using this setup, an attacker cannot gain access to your files or resources simply by naming their account the same as yours.

Even though you may use a username to access the system, Windows identifies each user, group, or object by the SID. For example, Windows uses the SID to look up a user account and see whether a password matches. Also, SIDs are used in every situation in which permissions need to be checked; for example, when a user attempts to access folder or shared resource to determine whether that user is allowed to access it.

Commonly Attacked and Exploited Services

The Windows OS exposes a tremendous number of services, each of which can be exploited in some way by an attacker. Each service that runs on a system is designed to offer extra features and capabilities to a system and, as such, Windows has a lot of basic services running by default, which are supplemented by the ones applications themselves install.

Although there are a number of services running in Windows, one of the most commonly targeted ones is the NetBIOS service, which uses User Datagram Protocol (UDP) ports 137 and 138 and Transmission Control Protocol (TCP) port 139.

NetBIOS has long been a target for attackers due to its ease of exploitation and the fact that it is commonly enabled on Windows systems even when it is not needed. NetBIOS was designed to facilitate communications between applications in local area networks, but is now considered to be a legacy service and usually can be disabled.

NOTE

In reality, any service can be a potential target; it all depends on the knowledge and skill of the attacker. However, some services are much more likely to be attacked than others, and NetBIOS fits the profile of a service that is commonly selected for attack.

In the Windows OS, the NetBIOS service can be used by an attacker to discover information about a system. Information that can be obtained via the service is very diverse and includes usernames, share names, service information, among other things. In the enumeration phase, we will see how to obtain this information using something known as a NULL session.

Enumeration

Once port scanning has been performed, it is time to dig deeper into the target system itself to determine what specifically is available. Enumeration represents a more aggressive step in the hacking and penetration testing process because the attacker has now started to access the system to see specifically what is available. All the steps leading up to this point have been aimed at gaining information about the target to discover the vulnerabilities that exist and how the network is configured. When enumeration is performed, the process is now attempting to discover what is offered by these services for later usage in actual system hacking.

When performing enumeration, the attacker has the goal of uncovering specific information about the system itself. During a typical enumeration process an attacker will make active connections to the target system to discover items such as user accounts, share names, groups, and other information that may be available via the services discovered previously. It is not uncommon during this phase of the attack to confirm information that was discovered earlier, information that the intended target may have even made publicly available such as Domain Name System (DNS) settings. During this process, however, new details will emerge that the victim did not make available; otherwise, details that tend to appear at this point include the following:

- User accounts
- Group settings
- Group membership
- Application settings
- Service banners
- Audit settings
- Other service settings

IS IT LEGAL?

A case can be made that enumeration represents the point at which hacking really starts, because the target is now being actively accessed. The steps leading up to enumeration have different levels of interaction with the target, but none of them seeks to actively extract information from the target as enumeration does. Enumeration has gone beyond actively probing a target to see what operating system it may be running to determining specific configuration details.

Enumeration can be said to be the point where the line has been crossed, with the activities from this point on becoming illegal.

In addition to determining what services and settings are present, the enumeration phase also can employ techniques used to determine the placement and capabilities of countermeasures. An attacker can use enumeration methods to get a picture of whether or how a target can respond to

system hacking activities. By uncovering information on whether or how a defender can respond will allow the attacker to modify their attack accordingly to make their activity more productive.

NOTE

The more information an attacker can gather, the more accurate the attack can be. With enough information about a target, an attacker can move from a "shotgun"-style attack to an attack similar to what a sniper would carry out.

NULL Session

The **NULL session** is a feature in the Windows operating system that is used to give access to certain types of information across the network. NULL sessions are a feature that has been a part of Windows for some time—one that is used to gain access to parts of the system in ways which are both useful and insecure.

A NULL session occurs when a user attempts a connection to a Windows system without the standard username and password being provided. This connection type cannot be made to any Windows share, but it can be made to a feature known as the Interprocess Communication (IPC) administrative share. In normal practice, NULL sessions are designed to facilitate connection between systems on a network to allow one system to enumerate the process and shares on another. Using a NULL session it is possible to obtain information such as the following:

- List of users and groups
- List of machines
- List of shares
- Users and host SIDs

The NULL session allows access to a system using a special account known as a NULL user that can be used to reveal information about system shares or user accounts while not requiring a username or password to do so.

Exploiting a NULL session is a simple task that requires only a short list of commands. For example, assume that a computer has the name "ninja" as the host name, which would mean that the system could be attached to using the following, where host is the Internet Protocol (IP) address or name of the system being targeted:

NOTE

NULL sessions may sound like a bad idea, but they are very handy when used properly. In practice, the Windows operating system has given broad powers to this account that are not needed to use the account for its intended function. As a security professional, being vigilant about how the sessions are used will help in securing them.

```
net use \\ninja\ipc$ "" /user:""
```

To view the shared folders on the system the following command can be used:

```
Net view \\ninja
```

If shared resources are available, they will be displayed as a list, at which point the attacker can attach to a shared resource as follows:

```
Net use s:\\ninja\\(shared folder name)
```

At this point, the attacker can browse the contents of the shared folder and see what data is present.

OVERSHARING?

Remember that on the Windows operating system shared folders give access to the Everyone group by default. If the Everyone group is given default access to a folder and this is not changed, it creates a situation in which attackers can easily browse the contents of the folder because they will be part of the Everyone group by default. Prior to Windows 2003, the Everyone group was granted full controls of a folder. From Windows 2003 on, the Everyone group is given read-only access. In either situation, it is possible for an attacker to at least view the contents of a folder, and in the case of full control, do much worse.

Table 7-2. Partial list of nbtstat switches.

SWITCH	NAME	FUNCTION
-a	Adapter Status	Returns the NetBIOS name table and mandatory access control (MAC) address of the address card for the computer name specified
-A	Adapter Status	Lists the same information as -a when given the target's IP address
-c	Cache	Lists the contents of the NetBIOS name cache
-n	Names	Displays the names registered locally by NetBIOS applications such as the server and redirector
-r	Resolved	Displays a count of all names resolved by broadcast or Windows Internet Name Service (WINS) server

SWITCH	NAME	FUNCTION
-s	Sessions	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names
-S	Sessions	Lists the current NetBIOS sessions and their status, with the IP address

Working with Nbtstat

An additional tool that can be used in the enumeration process is a tool known as nbtstat. Included with every version of the Windows operating system, nbtstat is a utility intended to assist in network troubleshooting and maintenance. The utility is specifically designed to troubleshoot name resolution issues that are a result of the NetBIOS service. During normal operation, a service in Windows known as NetBIOS over TCP/IP will resolve names known as NetBIOS names to IP addresses. Nbtstat is a command line utility designed to locate problems with this service.

Nbtstat has a number of switches that can be used to perform different functions; some of the more useful functions for the ethical hacker are listed in [Table 7-2](#).

The -A switch can be used to return a list of addresses and NetBIOS names the system has resolved. The command line that uses this option would look like the following if the targeted system had an IP address of 192.168.1.1:

```
nbtstat -A 192.168.1.1
```

SuperScan

SuperScan is a tool that was used back in [Chapter 6](#) to perform port scanning, but can also perform enumeration. On top of SuperScan's previously mentioned abilities to scan TCP and UDP ports, perform ping scans, run whois and tracert, it also has a formidable suite of features designed to query a system and return useful information.

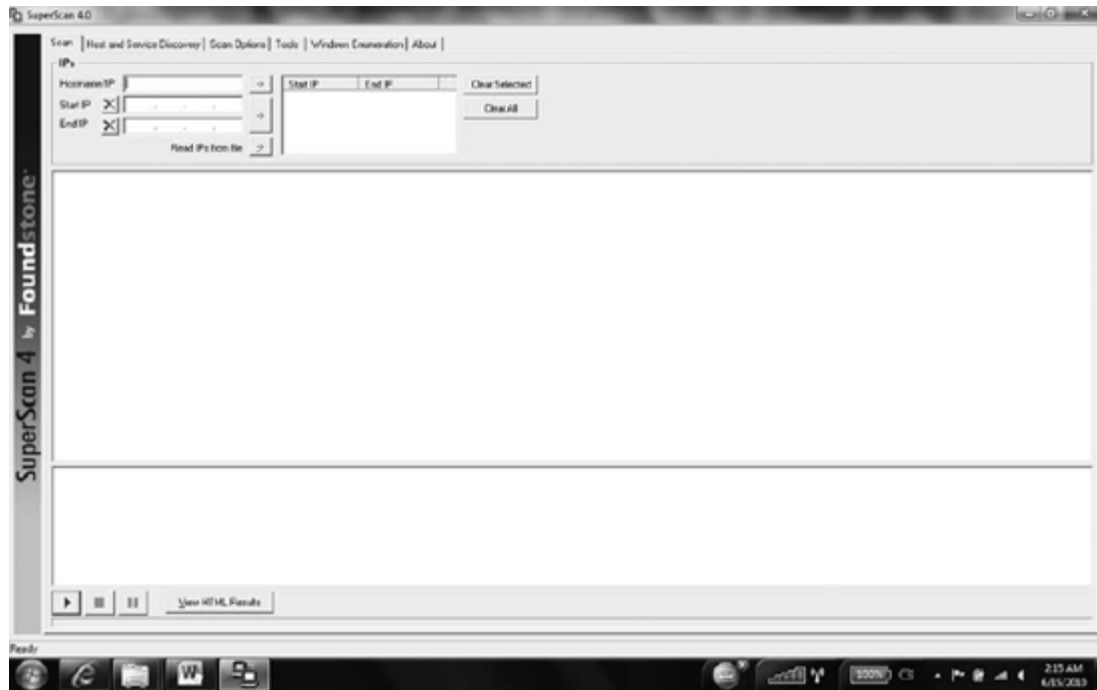


Figure 7-1. SuperScan.

SuperScan offers a number of useful enumeration utilities designed for extracting information from a Windows-based host:

- NetBIOS Name Table
- NULL session
- MAC addresses
- Workstation type
- Users
- Groups
- Remote procedure call (RPC) endpoint dump
- Account policies
- Shares
- Domains
- Logon sessions
- Trusted domains
- Services

Each of these features can extract information from a system that can be useful in later stages of the hacking process.

SNScan

SNScan is a utility designed to detect **Simple Network Management Protocol (SNMP)**- enabled devices on a network. The utility is designed to locate and identify devices that are vulnerable to

SNMP attacks. SNScan scans specific ports (for example, UDP 161, 193, 391, and 1993) and looks for the use of standard (public and private) and user-defined SNMP community names. User-defined community names may be used to more effectively evaluate the presence of SNMP-enabled devices in more complex networks.

Enumeration is designed to gather useful information about a system; specifically what can be accessed through a discovered service. By using the process of enumeration, an attacker can obtain information that may not otherwise be available such as usernames, share names, and other details. Enumeration represents the point at which the attack crosses the legal line to being an illegal activity in some areas.

System Hacking

After an attacker has performed enumeration, he or she can begin attacking the system. Enumeration has provided details that are actionable for the next phase of system hacking, including details of user accounts and groups. The information on usernames and groups provides points on the target system on which to concentrate the system hacking activities. Up to this point, progressively more detailed information has been gathered and what those services are offering has been determined; now the process of exploiting what has been uncovered can begin.

During the enumeration phase, among the detailed information that was acquired was usernames. The information on user accounts provides the system hacking process a point to focus on using a technique known as **password cracking**. Password cracking is used to obtain the credentials of an account with the intent of using the information to gain access to the system as an authorized user.

To understand why password cracking is successful, think of how and why passwords are used. Passwords are designed to be something that an individual can easily remember and at the same time not be something easily guessed. Herein lies the problem. In practice, individuals will tend to use passwords that are easy to guess or susceptible to cracking methods such as those introduced in this section. Some examples of passwords that lend themselves to cracking include the following:

- Passwords that use only numbers
- Passwords that use only letters
- Passwords that are only upper- or lowercase
- Passwords that use proper names
- Passwords that use dictionary words
- Short passwords (fewer than eight characters)

Passwords that adhere closely to any of the points on this list lend themselves to quick and easy password cracking methods. Passwords that avoid any of these points tend to be less easy to crack, but not impossible, as the techniques discussed in this section will demonstrate.

Types of Password Cracking

Despite what is seen in movies, TV shows, and other media, password cracking isn't as simple as a hacker sitting in front of a computer running some software and breaking the password. It is much more involved. Password cracking can take one of four forms, all designed to obtain a password that the attacker is not authorized to possess. The following are the four password cracking methods that can be utilized by an attacker:

- Passive online attacks
- Active online attacks
- Offline attacks
- Nontechnical attacks

Each one of these attacks offers a way of obtaining a password from an unsuspecting party in a different but effective way.

Passive Online Attacks

In passive online attacks, an attacker obtains a password simply by listening for it. This attack can be carried out using two methods; packet sniffing, or man-in-the-middle and replay attacks. These types of attacks are successful if the attacker is willing to be patient and employ the right technique in the correct environment.

Using a packet sniffer is effective, but it can be thwarted by technology that prevents the observation of network traffic. Specifically, packet sniffing will work only if the hosts are on the same collision domain. This is a condition that exists if a hub is used to join the network hosts together; if a switch, bridge, or other type of device is used, the attack will fail.

Other types of passive online attacks utilize a man-in-the-middle or replay attack to capture the password of the target. If a man-in-the-middle attack is used, the attacker must capture traffic from both ends of the communication between two hosts with the intention of capturing and altering the traffic in transit. In a replay attack, the process consists of an attacker capturing traffic using a sniffer, using some process to extract the desired information (in this case, the password), and then using or replaying it later to gain access to a resource.

FYI

While a packet sniffer may have limited success when trying to capture passwords on most networks, companies do tend to frown upon their use by unauthorized individuals. An individual that runs a packet sniffer on a corporate network has a possibility of capturing a password, not to mention other confidential information. It is for these reasons that companies tend to take a very tough stance on their usage, and in some cases have terminated employment of individuals caught using them on the network without permission.

FYI

Dictionary attacks are successful when users are allowed to choose passwords without any restrictions being placed upon them. Evidence has shown that individuals will choose passwords that are common names or words if allowed to do so, and it is in these cases that dictionary attacks thrive. The enforcement of complex passwords that introduce upper- and lowercase letters as well as numbers and special characters tends to limit the success of dictionary attacks.

Active Online Attacks

The next form of attack is known as an active online attack, which consists of more aggressive methods such as brute-force and dictionary attacks. Active online attacks are effective in situations in which the target system has weak or poorly chosen passwords in use. In such cases, active online attacks can crack passwords very quickly.

NOTE

Brute-force attacks, although effective, are thwarted by preventive techniques such as policies that lock user accounts when a password is entered incorrectly a preset number of times. When policies are in effect that limit unsuccessful logon attempts before locking an account, the effectiveness of a brute-force attack is diminished.

The first type of active online attack is the brute-force attack, which is unsophisticated but can be very effective in the right situation. In this type of attack, all possible combinations of characters are tried until the correct combination is discovered. Given enough time, this type of attack will be successful 100 percent of the time; however, that is also part of the problem—having enough time.

A dictionary attack shares some traits with the brute-force attack. Whereas a brute-force attack attempts all combinations of characters, the dictionary attack tries passwords that are pulled from a predefined list of words. Dictionary attacks are particularly successful in situations in which the passwords in use on a system have been chosen or can be chosen from common words. This type of attack is successful even if the password is a reversed form of a dictionary word, changes certain characters, or even uses tactics such as appending digits to the end of the word. These types of attacks are easy to carry out by an attacker largely due to the availability of the components to perform them, such as password crackers and predefined word lists that can be downloaded and used immediately.

Offline Attacks

Offline attacks are a form of password attack that relies on weaknesses in how passwords are stored on a system. The previous attack types attempted to gain access to a password by capturing it or trying to break it directly; offline attacks go after passwords where they happen to be stored on a system. On most systems, a list of usernames and passwords is stored in some location; if these lists are stored in a plaintext or unencrypted format, an attacker can read the file and gain the credentials. If the list is encrypted or protected, the question becomes "How is it protected?" If the list is using weak encryption methods, it can still be vulnerable.

A LOOK AT PASSWORD HASHING

Passwords used to grant access to a system are generally stored in a database on a system in which they can be accessed to validate the identity of a user. Due to its very nature, a database can store quite a number of passwords, each providing the ability to grant some sort of access to the system, so the confidentiality and integrity of these items must be preserved. Two ways to protect these valuable credentials are encryption and hashing. Encryption provides a barrier against unauthorized disclosure, while hashing ensures the integrity of these credentials. When users attempt to log on to the system, they provide their credentials in the form of username and password, but the password is hashed. Because the database on the system already has a hashed form of the user's password on file, a comparison is made. If the comparison between what the user provides and what is on file matches, the use is authenticated; if not, they are denied access.

While the hashing method is known to both parties and can be discovered with some work by an attacker, it does not tell them what a password is because they would still have to reverse the hash (which is designed to be infeasible). However, the attacker can apply the same hashing function to different character combinations in an attempt to reveal an identical hash. The rate at which this can be performed varies depending largely on the hashing function used, but in some cases this process can be performed quite rapidly—which can allow the plaintext password to be recovered easily.

The process discussed in this section relies on this process to recover passwords.

Four types of offline attacks are available to the attacker, each offering a method that can be used to obtain passwords from a target system. The types of offline attacks available include the two mentioned previously (dictionary and brute-force attacks), and also hybrid and precomputed attacks.

Examples of password crackers in this category include:

- **Cain and Abel**—Has the ability to crack password hashes offline. Works with Windows, Cisco, VNS, and other similar passwords.
- **John the Ripper**—Cracks UNIX and Windows passwords
- **Pandora**—Designed to crack Novell passwords
- **Pwdump3**—Extracts passwords from the SAM database

Dictionary Attacks

Dictionary attacks are similar to active online attacks in that all possible combinations are tried until the correct combination is discovered. The difference between this type of attack and the active online version is how the correct combination is uncovered. In this method, an attacker reads the list of passwords looking for hashes that match the hashed values of words in the dictionary. If the attacker finds a match between the hashed values on the system and the hashed values from a dictionary or wordlist, he or she has found the correct password.

FYI

A method of thwarting hashes that is used by many systems such as UNIX is a technique known as salting. When you use salting, you add extra characters to a password prior to hashing. This has the effect of changing the hash, but not the password. Attackers who recover the list of hashes from the system will have a much harder time recovering the passwords because they would have to determine the password by reversing the hash or determining the text used to generate it.

Hybrid Attacks

Hybrid attacks are another form of offline attack that functions much like dictionary attacks, but with an extra level of sophistication. Hybrid attacks start out like a dictionary attack, in which different combinations of words from the dictionary are attempted; if this is unsuccessful at uncovering the password, the process changes. In the next phase of the attack, characters and symbols are added to the combinations of characters to attempt to reveal the password. The attack is designed to be fast and thwart the incorrect or improper use of salting.

Brute-Force Attacks

Brute-force attacks function like online attacks because they attempt all possible combinations or a suspected subset of possible passwords. Brute force has the benefit of always working, but the downside is that it takes a long time. Typically, this method starts using simple combinations of characters and then increases complexity until the password is revealed.

Examples of brute-force password crackers include:

- Opcrack
- Proactive Password Auditor

FYI

Given enough time (possibly years!), brute-force attacks will succeed, but the issue becomes whether the attackers have enough time before they are detected. Brute-force methods of any type can take substantial periods of time depending on the complexity of the password, password length, and processor power of the system attempting the break in. Attackers run the risk that if they take too long to break a password, they will be detected by the system owner, at which point the attack will have failed.

Precomputed Hashes

Precomputed hashes are used in an attack type known as a **rainbow table**. Rainbow tables compute every possible combination of characters prior to capturing a password. Once all the passwords have been generated, the attacker can then capture the password hash from the network and compare it with the hashes that have already been generated. With all the hashes generated ahead of time, it becomes a simple matter to compare the captured hash to the ones generated, typically revealing the password within a few moments.

Of course, there's no getting something for nothing, and the case of rainbow tables is no exception. The downside of rainbow tables is that they take time. It takes a substantial period of time, sometimes days, to compute all the hash combinations ahead of time. Another downside of rainbow tables is the lack of ability to crack passwords of unlimited length because generating passwords of increasing length takes increasing amounts of time.

NOTE

Rainbow tables are an effective method of revealing passwords, but the effectiveness of the method can be diminished through salting. Salting is used in Linux, UNIX, and BSD, but is not used in some of the older Windows authentication mechanisms such as LM and NTLM.

Examples of password crackers that use rainbow tables include:

- Opcrack
- RainbowCrack

Nontechnical Attacks

The last of the password cracking methods is a family of techniques that obtain passwords using nontechnical methods. In some cases, an attacker may choose to use nontechnical methods due to the conditions in the environment or just because it is easier. The nontechnical methods represent a change over previous attacks; where previous attacks relied on attacking the technology, nontechnical methods go after the human who uses the system. In the right hands, nontechnical methods can be as effective as technical methods at obtaining passwords.

Shoulder Surfing

Shoulder surfing is a method of obtaining a password by observing people entering their password. In this attack, the individual wanting to gain access to the password takes a position to see what a user is typing or what is appearing onscreen. Additionally, the attacker may also look for clues in the user's movements that suggest they are looking up a password such as on a Post-It note or other location. To deter this attack, use the privacy screen that can be put onscreen and always pay attention to your surroundings to see whether anyone is watching.

Keyboard Sniffing

Keyboard sniffing intercepts the password as a user is entering it. This attack can be carried out when users are the victims of keylogging software or if they regularly log onto systems remotely without using any protection.

Social Engineering

Social engineering methods can be used to obtain a password based on trust or ignorance on the user's end. For example, a password may be obtained by an attacker calling an individual,

pretending to be the system administrator, and asking for the password. Social engineering is effective because users tend to be trusting; if an individual sounds or acts legitimate, the feeling is that he or she probably is.

Using Password Cracking

Using any of the methods discussed here with any type of password cracking software may sound easy, but there is one item to consider: whose password to crack? Going back to the enumeration phase, it was discussed that usernames could be extracted from the system using any one of a number of software packages or methods. Using these software tools, usernames were uncovered and at this point the attacker could target a specific account without the password cracking tool of choice.

So which password to crack? Accounts such as the administrator account are targets of opportunity, but so are lower-level accounts such as guest that may not be as heavily defended nor even considered in security planning.

Privilege Escalation

If a password is cracked, the probability of the account being one that has high level access is somewhat low because these types of accounts tend to be well defended. If a lower-level account is cracked, the next step is **privilege escalation**: to escalate the privileges to a level at which increased access and fewer restrictions are in place such as with the administrator account.

OUT OF SIGHT, OUT OF MIND

Every operating system ships with a number of user accounts and groups already present. In Windows, users who are already configured include the administrator and guest accounts. Because it is easy for an attacker to find information on the accounts that are included with an operating system, care should be taken to ensure that such accounts are secured properly, even if they will never be used. An attacker who knows that these accounts exist on a system is more than likely to try to obtain the passwords of each.

STOPPING PRIVILEGE ESCALATION

A number of methods can be used to blunt the impact of privilege escalation such as the concept known as least privilege. The thinking behind this concept is to limit the amount of access an account has to just what is needed to perform its assigned duties. For example, a user account given to someone in sales would be able to only perform the tasks required by a salesperson to do the job. It is in this way that the actions that an account can perform are limited, preventing inadvertent or accidental damage or access to resources.

One way to escalate privileges is to identify an account that has the access desired and then change the password. There are several tools that offer this ability, including the following:

- Active@ Password Changer
- Trinity Rescue Kit
- ERD Commander
- Recovery Console

These utilities function by altering the SAM with the goal of resetting passwords and accounts to settings desired by the attacker.

Active@ Password Changer

The Active@ Password Changer is a utility that is used to perform multiple functions on user accounts including password resets. The utility can be used to change a password of a targeted user account to a password that the attacker chooses to set. To use this utility requires the attacker to gain physical access to a system, at which point the system can be rebooted from a universal serial bus (USB), floppy, or CD.

NOTE

The designers of Active@ designed it to prevent the lengthy process of reinstalling operating systems when a password reset could be performed instead. However, as is the case with any tool, it can be used for good or bad. It all depends on the user's intent.

Active@ has the advantage of being able not only to reset passwords, but also to:

- Re-enable accounts
- Unlock an account
- Reset expiration on an account
- Display all local users on a system
- Reset administrator account credentials

To change a password using Active@, select a specific user account to view the account information, as seen in [Figure 7-2](#).

To view and change permitted logon days and hours, press the [PgDn] key, as seen in [Figure 7-3](#).

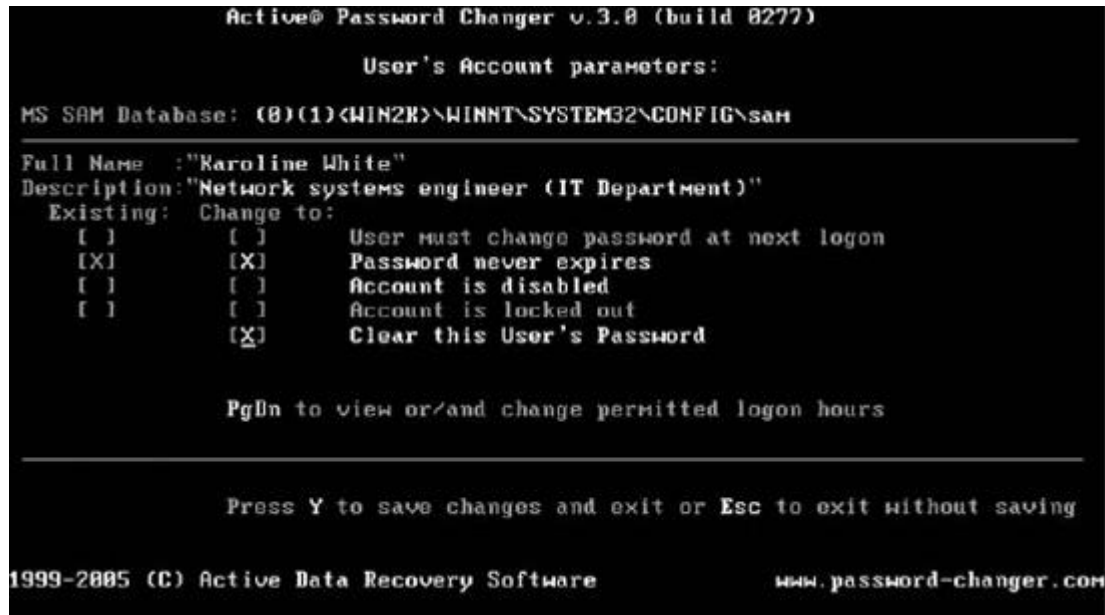


Figure 7-2. Viewing account information.

Select and choose days and hours to allow logons. Account logon hours are displayed in GMT (Greenwich Mean Time). The time will have to be adjusted for the local time zone where the system resides or for the time zone set on the system.

Press [Y] to save changes or press [Esc] to leave the previous account information unchanged and return to previous window (List of accounts). See [Figure 7-4](#).

Resetting a user's password results in the following:

- The user's password is set to blank.
- The account is enabled.
- The password will be set never to expire.

```
Active@ Password Changer v.3.0 (build 0277)

User's Account parameters:

MS SAM Database: (0)(1)<WIN2K>\WINNT\SYSTEM32\CONFIG\sam

-----
      0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Su [X][X][X][X][X][ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [X][X][X][X][X][X][X][X][X]
Mo [X][X][ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [X]
Tu [X][X][X][X][ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [X]
We [X][X][X][X][ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [X]
Th [X][X][X][X][ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [X]
Fr [X][X][X][X][ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [X]
Sa [X][X][X][X][ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [X][X][X][X][X][X][X]

PgUp to view or/and change account parameters

-----

Press Y to save changes and exit or Esc to exit without saving

1999-2005 (C) Active Data Recovery Software      www.password-changer.com
```

Figure 7-3. Changing logon days and times.

```
Active@ Password Changer v.3.0 (build 0277)

User's Account parameters:

MS SAM Database: (0)(1)<WIN2K>\WINNT\SYSTEM32\CONFIG\sam

-----
Full Name      : "Karoline White"
Description: "Network systems engineer (IT Department)"
Existing:      Change to:
[ ]           [ ]      User must change password at next logon
[X]           [X]      Password never expires
[ ]           [ ]      Account is disabled
[ ]           [ ]      Account is locked out
[ ]           [X]      Clear this User's Password

PgDn to view or/and change permitted logon hours

-----

Press Y to save changes and exit or Esc to exit without saving
User's attributes has been succesfully changed. (Press any key...)

1999-2005 (C) Active Data Recovery Software      www.password-changer.com
```

Figure 7-4. List of accounts.

Trinity Rescue Kit

Trinity Rescue Kit (TRK) is a Linux distribution that is specifically designed to be run from a CD or flash drive. TRK was designed to recover and repair both Windows and Linux systems that were otherwise unbootable or unrecoverable. While TRK was designed for benevolent purposes,

it can easily be used to escalate privileges by resetting passwords of accounts that you would not otherwise have access to.

NOTE

The TRK can be used as a follow-on tool to the enumeration techniques discussed earlier. It works best when you know the name of the account to be changed. The enumeration techniques shown previously allow you to browse the accounts on a system and select a target account.

TRK can be used to change a password by booting the target system off of a CD or flash drive and entering the TRK environment. Once in the environment, a simple sequence of commands can be executed to reset the password of an account.

The following steps change the password of the Administrator account on a Windows system using the TRK:

1. At the command line enter the following command:

```
winpass -u Administrator
```

2. The winpass command will then display a message similar to the following:
3. Searching and mounting all file system on local machine
4. Windows NT/2K/XP installation(s) found in:
5. 1: /hda1/Windows
Make your choice or 'q' to quit [1]:
6. Type 1 or the number of the location of the Windows folder if more than one install exists.
7. Press Enter.
8. Enter the new password or accept TRK's suggestion to set the password to a blank.
9. You will see this message: "Do you really wish to change it?" Enter Y and press Enter.
10. Type init 0 to shut down the TRK Linux system.
11. Reboot.

As you can see, it is possible to change the password of a specific account using TRK in a few steps.

Escalating privileges gives the attacker the ability to perform actions on the system with fewer restrictions and perform tasks that are potentially more damaging. If an attacker gains higher privileges than he or she would have otherwise, it is possible to run applications, perform certain operations, and engage in other actions that have a bigger impact on the system.

Planting Backdoors

The next step after escalating privileges is to place **backdoors** on the system so you can come back later and take control of the system repeatedly. An attacker who places a backdoor on a system

can use it for all sorts of reasons, depending on specific goals. Some of the reasons for planting backdoors include the following:

- Placing a rootkit
- Executing a Trojan

Of course, the question is how to get a backdoor on a system. With the escalated privileges obtained earlier, you have the power to run an application on a system and do so more freely than you would without such privileges. If the privileges obtained previously were administrator (or equivalent), you now have few if any limitations, which means that you can install a backdoor quite easily.

To start the process, you must first run an application remotely. Several tools are available, but for this discussion you will use some of the components of a suite of tools known as PsTools.

FYI

PsTools is a suite of tools designed by Mark Russinovich of Microsoft. The PsTools suite was originally designed for Windows NT systems, but has continued to serve a useful purpose in later versions. PsTools contains applications designed to do everything from running commands remotely to terminating processes, as well as a number of other functions. All the applications that make up the PsTools suite are command line-based and offer the ability to be customized by the use of switches.

Using PsTools

The PsTools suite includes a mixed bag of utilities designed to ease system administration. Among these tools is PsExec, which is designed to run commands interactively or noninteractively on a remote system. Initially, the tool may seem similar to Telnet or remote desktop, but does not require installation on the local or remote system in order to work. PsExec need only be copied to a folder on the local system and run with the appropriate switches to work.

Let's take a look at some of the commands that can be used with PsExec:

- The following command launches an interactive command prompt on a system named \\zelda:

```
psexec \\zelda cmd
```

- This command executes IpConfig on the remote system with the /all switch, and displays the resulting output locally:

```
psexec \\zelda ipconfig /all
```

- This command copies the program rootkit.exe to the remote system and executes it interactively:

```
psexec \\zelda -c rootkit.exe
```

- This command copies the program rootkit.exe to the remote system and executes it interactively using the administrator account on the remote system:

```
psexec \\zelda -u administrator -c rootkit.exe
```

As these commands illustrate, it is possible for an attacker to run an application on a remote system quite easily. The next step is for the attacker to decide just what to do or what to run on the remote system. Some of the common choices are Trojans, rootkits, or backdoors.

Rootkits

A **rootkit** is piece of software designed to perform some very powerful and unique tasks to a target system. This software is designed to alter system files and utilities on a victim's system with the intention of changing the way a system behaves. Additionally, a rootkit quite commonly has the capability to hide itself from detection, which makes the device quite dangerous.

A rootkit is beneficial to an attacker for a number of reasons, but the biggest benefit is the scope of access the attacker can gain. With a rootkit installed on a system, attackers gain root access to a system, which means that they now have the highest level of access possible on the target system. Once attackers have a rootkit installed, they effectively own the system and can get it to do whatever they want. In fact, a rootkit can be embedded into a system so deeply and with such high levels of access that even the system administrator will be unable to detect its presence. Having root access to a system allows an attacker to do any of the following:

SONY'S ROOTKIT PROBLEM

One of the more famous rootkits was produced by Sony BMG in 2005 as a way to enforce Digital Rights Management (DRM) on its music. The software was shipped on the CDs of some of Sony's popular artists. When the CD was placed into a computer using Microsoft Windows, the software would install on the system and prevent copying of music. The biggest downside to this software was that it had no protection, so an attacker who knew the software was present or knew how to scan for it could connect to and take control of a victim's system.

This rootkit case had a lot of fallout for Sony and the computing public at large. Sony was embarrassed by the publicity and ultimately was on the losing side of a class action lawsuit. Additionally, as a result of this problem, the public became aware of the threat of rootkits and learned to be more cautious.

Sony's rootkit episode also attracted hackers to write new worms designed to pounce on the vulnerabilities that the rootkit induced on a system.

- **Installing a virus at any point**—If the **virus** requires root level access to modify system files, or alter and corrupt data or files, a rootkit can provide the means to do so.
- **Placing a Trojan on a system**—Much like viruses, a Trojan may require root level access, so a rootkit will provide the level of access needed to run these types of malware.
- **Installing spyware to track activity**—**Spyware** typically needs to be well placed and well hidden. A rootkit can provide a way to hide spyware such as a **keylogger** so it is undetectable even to those looking for it.
- **Hiding the attack**—A rootkit possesses the ability to alter the behavior of a system any way an attacker wants, so it can be used to hide evidence of an attack. A rootkit can be used to hide files and processes from view by altering system commands to prevent the display or detection of the attack.
- **Maintaining access over the long term**—If a rootkit can stay undetected, it is easy for an attacker to maintain access to the system. For an attacker, the challenge is to construct a rootkit to prevent detection by the owner of the system.
- **Monitoring network traffic**—A rootkit can install a network sniffer on a system to gain inside information about the activities on a network.

NOTE

Rootkits are dangerous because once a system has become the victim of a rootkit, it can no longer be trusted. A rootkit alters the behavior of a system to such a degree that the information being returned by the system itself has to be considered bogus.

- **Blocking the logging of selected events**—To prevent detection, a rootkit can alter the system to prevent the logging of activities related to a rootkit.
- **Redirecting output**—A rootkit can be configured to redirect output of commands and other activities to another system.

Above all, a rootkit is an application and as such can be run with a tool such PsExec and run remotely on a target system. Of course, running a rootkit is one thing; obtaining one is quite another. Currently there exist many ways to get a rootkit—whether it is from a Web site or through a development tool designed to help nonprogrammers create basic rootkits.

NOTE

Rootkits are a form of what is known as malware, which includes software such as viruses, worms, spyware, and other related miscreants.

Covering Tracks

An attack that can be detected is an attack that can be stopped, which is not a good result for an attacker. To stop an attack from being detected, attackers need to cover their tracks as completely and effectively as possible. Covering tracks needs to be a systematic process in which any evidence of the attack is erased to include logons, log files, error messages, files, and any other evidence that may tip off the owner of the system that something has occurred.

Disabling Auditing

One of the best ways to cover your tracks is to not leave any in the first place. In this case, disabling auditing is a way to do just that. Auditing is designed to allow the detection and tracking of events that are occurring on a system. If auditing is disabled, an attacker can deprive the system owner of detecting the activities that have been carried out. When auditing is enabled, all events that the system owner chooses to track to will be placed in the Windows Security Log and can be viewed as needed. An attacker can disable it with the auditpol command included with Windows.

NOTE

A prepared defender of a system will regularly check event logs to note any unusual activity such as a change in audit policy. Additionally a host-based intrusion detection system (IDS) will detect changes in audit policy and in some cases re-enable it.

Using the NULL session technique seen earlier, you can attach to a system remotely and run the command as follows:

```
auditpol \\
```

It is also possible for an attacker to perform what amounts to the surgical removal of entries in the Windows Security Log using tools such as the following:

- Dumpel
- Elsave
- Winzapper

Of course, clearing audit logs isn't the only way to clear tracks because attackers can use rootkits. Using techniques that will be discussed later, you can thwart rootkits to a certain degree, but once rootkits make their way onto a system, sometimes the only reliable way to ensure that a system is free of them is to rebuild that system.

Data Hiding

There are other ways to hide evidence of an attack, such as hiding the files placed on the system. Operating systems provide many methods that can be used to hide files, including file attributes and alternate data streams.

File attributes are a feature of operating systems that allow files to be marked as having certain properties, including read-only and hidden. Files can be flagged as hidden, making for a convenient way of hiding data and preventing detection through simple means such as directory listings or

browsing in Windows Explorer. Hiding files in this way does not provide complete protection, however, because more advanced detective techniques can uncover files hidden in this manner.

Another lesser known way of hiding files in Windows is Alternate Data Streams (ADS), which is a feature of the New Technology File System (NTFS). Originally, this feature was designed to ensure interoperability with the Macintosh Hierarchical File System (HFS), but has since been used by hackers. ADS provides the ability to fork or hide file data within existing files without altering the appearance or behavior of a file in any way. In fact, when ADS is used, a file can be hidden from all traditional detection techniques as well as dir and Windows Explorer.

NOTE

ADS is available only on NTFS volumes, although the version of NTFS does not matter. This feature does not work on other file systems.

In practice, the use of ADS is a major security issue because it is nearly a perfect mechanism for hiding data. Once a piece of data is embedded using ADS and is hidden, it can lie in wait until the attacker decides to run it later on.

The process of creating an ADS is simple:

```
type ninja.exe > smoke.doc:ninja.exe
```

Executing this command will take the file `ninja.exe` and hide it behind the file `smoke.doc`. At this point, the file is streamed. The next step would be to delete the original file that you just hid, specifically `ninja.exe`.

As an attacker, to retrieve the file the process is as simple as the following:

```
start smoke.doc:ninja.exe
```

This command has the effect of opening the hidden file and executing it.

As a defender, this sounds like bad news because files hidden in this way are impossible to detect using most means. But with the use of some advanced methods they can be detected. Some of the tools that can be used to do this include:

- **Sfind**—A forensic tool for finding streamed files
- **LNS**—Used for finding ADS streamed files
- **Tripwire**—Used to detect changes in files, this tool by nature can detect ADS

Depending on the version of Windows and the system settings in place, an attacker can clear events completely from an event log or remove individual events.

CHAPTER SUMMARY

Enumeration is the process of gathering more detailed information from a target system. Whereas previous information has been gathered without disturbing the target, with enumeration the target is being interacted with, and more detailed information is being returned. Information extracted from a target at this point includes usernames, group information, share names, and other details.

Once the attacker has completed enumeration, he or she begins system hacking. In the system hacking phase, the attacker starts to use the information gathered from the enumeration stage by hacking the services. This stage represents the point at which the attacker is compromising the system.

An attacker who wants to perform more aggressive actions or needs greater access can perform a process known as privilege escalation. In this stage, the attacker gains access to a user account or system and attempts to grant it more access than it would otherwise have by resetting passwords of accounts that have more access or installing software that grants this level of access.

Finally, the attackers cover up their tracks to avoid detection and action by possible countermeasures. They can stop auditing, clear event logs, or surgically remove events from the logs to make things look less suspicious. In this last phase, attackers eliminate the traces of their attack as completely as possible leaving few (if any) behind.

KEY CONCEPTS AND TERMS

- Backdoor
- Enumeration
- Keylogger
- NULL session
- Password cracking
- Privilege escalation
- Rainbow table
- Rootkit
- Security Account Manager (SAM)
- Simple Network Management Protocol (SNMP)
- Spyware
- Virus

CHAPTER 1 ASSESSMENT

1. Enumeration discovers which ports are open.
 1. True
 2. False
2. What can enumeration discover?
 1. Services
 2. User accounts
 3. Ports
 4. Shares
3. _____ involves increasing access on a system.
 1. System hacking
 2. Privilege escalation
 3. Enumeration
 4. Backdoor
4. _____ is the process of exploiting services on a system.
 1. System hacking
 2. Privilege escalation
 3. Enumeration
 4. Backdoor
5. How are brute-force attacks performed?
 1. By trying all possible combinations of characters
 2. By trying dictionary words
 3. By capturing hashes
 4. By comparing hashes
6. A _____ is an offline attack.
 1. Cracking attack
 2. Rainbow attack
 3. Birthday attack
 4. Hashing attack
7. An attacker can use a(n) _____ to return to a system.
8. A _____ replaces and alters system files, changing the way a system behaves at a fundamental level.
 1. Rootkit
 2. Virus
 3. Worm
 4. Trojan
9. A NULL session is used to attach to Windows remotely.
 1. True
 2. False
10. A(n) _____ is used to reveal passwords.
11. A _____ is used to store a password.
 1. NULL session

2. Hash
 3. Rainbow table
 4. Rootkit
12. A _____ is a file used to store passwords.
1. Network
 2. SAM
 3. Database
 4. NetBIOS

Chapter 2. Wireless Vulnerabilities

WIRELESS COMMUNICATION and networking technologies have seen rapid growth and adoption over the past few years. Businesses and consumers have adopted wireless technologies for their ability to allow users to be more mobile, unencumbered by wires. Additionally, adopters have taken to the technology because it can allow connections to computers in areas where wires cannot reach or would be expensive to install. Wireless has become one of the most widely used technologies by both consumers and businesses and will most likely continue to be so.

While wireless offers many benefits, one of the concerns of the technology is security. Wireless technologies have many security issues that must be addressed by the security professional. The technology has traditionally suffered from poor or even ignored security features by those who either adopted the technology too quickly or didn't take the time to understand the issues. Those organizations that did take the initiative in a lot of cases went too far, opting to ban the use of the technology instead of finding out how to secure the technology.

This chapter explores how to use wireless technology in the organization, to reap its benefits but do so securely. Like any technology, wireless can be used safely; it is only a matter of understanding the tools available to make the system secure. For example, we can leverage techniques such as encryption and authentication together with other features designed to make the system stronger and more appealing to the business. With the right know-how and some work, wireless can be secured; the technology needn't be banned.

Chapter 8 Topics

This chapter covers the following topics and concepts:

- Why wireless security is important
- What the history of wireless technologies is
- How to work with and secure Bluetooth
- How to work with wireless local area networks (WLANs)
- What the threats to Wireless LANs are
- What wireless hacking tools are
- How to protect wireless networks

Chapter 8 Goals

When you complete this chapter, you will be able to:

- Explain the significance of wireless security
- Understand the reasons behind wireless security
- Describe the history of wireless
- Understand security issues with cordless phones, satellite TV, and cell phones
- See how Bluetooth works
- Understand security issues with Bluetooth

- Detail wireless LANs and how they work
- Describe threats to Wireless LANs
- List types of wireless hacking tools
- Understand how to defend wireless networks

The Importance of Wireless Security

Wireless technologies have been adopted rapidly over the last decade, but security for those networks has not. As individuals and organizations looked to adopt the technology, security was dealt with in a number of different ways: either by not adopting security measures at all in some cases or by blocking the use of the technology in others. Both cases represent extremes that need not be used because wireless can be secured safely if the security vulnerabilities and issues involved are known.

Wireless networks have a number of vulnerabilities that must be understood before they can be properly dealt with.

Emanations

One of the traits of wireless networks is the way they work through the use of radio frequency (RF) or radio techniques. This is both a strength and a weakness because it allows wireless transmissions to reach out in all directions, enabling connectivity but also allowing anyone in those directions to eavesdrop. As opposed to the transmission of signals in traditional media such as copper or fiber, where someone must be on the "wire" to listen, wireless travels through the air and can easily be picked up by anyone with a device as simple as a notebook with a wireless card. This leads to a huge administrative and security headache and it immediately makes clear the need for additional security measures.

NOTE

Except for fiber optic media, all networks are subject to emanations in the form of electromagnetic radiation. In the case of copper cables this emanation is a result of electrical charges flowing through the media and generating a field.

Emanations of a wireless network can be affected by a number of different factors that make the transmission go farther or shorter distances, including the following:

- **Atmospheric conditions**—Warm or cold weather will affect how far a signal will go due to the changes in air density that changing temperatures cause.
- **Building materials**—Materials surrounding an access point (AP) such as metal, brick, or stone will impede a wireless signal.
- **Nearby devices**—Other devices in the area (for example, microwaves and cell phones) that give off RF signals or generate strong magnetic fields can affect emanations.

NOTE

Anything that generates radio signals on the same or related frequencies can interfere with wireless networks in some form. By extension, anything that affects the atmosphere that the signals are traveling through will cause interference. However it is also of note that interference does not mean that a network will be offline. Interference can manifest itself as low or poor performing networks.

Common Support and Availability

Wireless networks have become more and more common over the last few years, being shipped in all manner of devices and gadgets. From the early 2000s up to the current day, wireless technologies in the form of Bluetooth and **Wi-Fi** have become more common, with both features going from being an option to being standard equipment in notebooks and netbooks. This increased support of wireless technology can be seen even in cell phones, in which Bluetooth support became standard with Wi-Fi support following closely behind on the standard feature list of devices.

FYI

Consider how ubiquitous Bluetooth support is in cell phones alone. A company that wants to eliminate the use of Bluetooth would have a monumental task on its hands because just about all cell phones include this feature. In fact, in some high-security areas, employees have been forced to purchase used cell phones from years ago or go without cell phones while at work.

WHAT IS WI-FI?

Wi-Fi is a trademark introduced in 1999 and owned by the Wi-Fi Alliance that is used to brand wireless technologies that conform to the 802.11 standard. For a product to bear the Wi-Fi logo, it must pass testing procedures to ensure it meets 802.11 standards. The Wi-Fi program was introduced due to the widespread problems of interoperability that plagued early wireless devices. *Wi-Fi* is commonly used to refer to wireless networking much as the name *Coke* is used to refer to any soft drink, but just because a device uses the 802.11 standard does not mean it is Wi-Fi (it may not have undergone testing).

The widespread availability of wireless has made management and security much harder for the network and security administrator. With so many devices implementing wireless, it is now more possible that an employee of a company could bring in a wireless-enabled laptop or other device and attach it to the network without the knowledge of an administrator. In some situations, employees have decided that a company IT department that has said "No wireless" is just being unreasonable and, oblivious to the security risks, have taken it upon themselves to install a wireless AP.

A Brief History of Wireless Technologies

Wireless technologies aren't anything new; in fact, wireless has been around for more than a decade for networks and even longer for devices such as cordless phones. The first wireless networks debuted in the mid-1990s with educational institutions, large businesses, and governments as early

adopters. The early networks did not resemble the networks in use today because they were mainly proprietary and performed poorly compared with today's deployments.

In today's environment, the business or consumer looking to purchase a wireless networking technology will encounter a large selection of options. Among them is the Institute of Electrical and Electronics Engineers (IEEE) **802.11** family of standards, which range from 802.11a to 802.11n. They are known collectively as Wi-Fi in standard jargon. In addition to the 802.11 family of wireless standards, other wireless technologies have emerged (Bluetooth, for example), each purporting to offer something unique.

When looking at wireless networking it is easy to think of it as one standard, but this is not the case. Wireless networks have evolved into a family of standards over time; each includes unique attributes. To understand wireless, it is worth looking at the different standards and their benefits and performance. The following sections discuss the wireless standards that have been or are in use.

802.11

The 802.11 standard was the first wireless standard that saw any major usage outside of proprietary or custom deployments. It was used mainly by large companies and educational institutions that could afford the equipment, training, and implementation costs. One of the biggest problems with 802.11 that led to limited usage was performance. The maximum bandwidth was theoretically 2 megabytes per second (Mbps). In practice, it reached at best only half this speed. The 802.11 standard was introduced in 1997 and saw limited usage, but quickly disappeared.

Its features included:

- Bandwidth—2 Mbps
- Frequency—2.4 Ghz (gigahertz)

802.11b

The first widely adopted wireless technology was 802.11b, introduced two years after the original 802.11 standard. It didn't take too long to be adopted by businesses and consumers alike. The most attractive feature of this standard is performance; 802.11b increased performance up to a theoretical 11 Mbps, which translated to a real-world speed of 6-7 Mbps. Other attractive features of the standard include low cost for the consumer and for the product manufacturer.

NOTE

802.11b is being rapidly replaced in favor of 802.11g and n, but it is still very widely used and supported, with most notebooks still supporting the technology off the shelf and 802.11b APs still available.

Its features include:

- Bandwidth—11 Mbps
- Frequency—2.4 Ghz

One downside of 802.11b is interference. 802.11b has a frequency of 2.4 Ghz, the same frequency as other devices such as cordless phones and game controllers, so these devices can interfere with 802.11b. Additionally, interference can be caused by home appliances such as microwave ovens.

802.11a

When 802.11b was being developed, another standard was created in parallel: 802.11a. It debuted around the same time as 802.11b, but never saw widespread adoption due to its high cost and lesser range. One of the largest stumbling blocks that hampered its adoption was equipment prices, so the alternative 802.11b was implemented much more quickly and is seen in more places than 802.11a. Today 802.11a is rarely seen.

The 802.11a standard did offer some benefits over 802.11b, notably much greater bandwidth: 54 Mbps over 802.11b's 11 Mbps. Also, 802.11a offers a higher frequency range (5 Ghz), which means less chance for interference because fewer devices operate in this range. Finally, the signaling of 802.11a prevents the signal from penetrating walls or other materials, allowing it to be somewhat easily contained.

FYI

At one point, 802.11a was widely used by businesses due to the performance, cost, and security benefits. The business world adopted wireless primarily because of its better performance and their bigger budgets. Businesses also found a unique benefit in the ability to contain the signal with standard building materials. However, today's world has seen the replacement of 802.11a with 802.11g and 802.11n networks supplemented with appropriate security technologies.

The 802.11a standard is not compatible with 802.11b or any other standard due to the way it is designed. APs that support 802.11a and other standards simply have internals that support both standards.

Its features include:

- Bandwidth—54 Mbps
- Frequency—5 Ghz

802.11g

In response to consumer and business demands for higher performance, wireless networks 802.11g emerged. The 802.11g standard is a technology that combines the best of both worlds (802.11a and 802.11b). The most compelling feature of 802.11g is the higher bandwidth of 54 Mbps combined with the 2.4 Ghz frequency. This allows for greater range and backward compatibility with 802.11b (but not 802.11a). In fact, wireless network adapters that use the 802.11b standard

are compatible with 802.11g APs, which allowed many business and users to migrate more quickly to the new technology.

NOTE

Some networks that identify themselves as 802.11b are actually 802.11g networks and are being identified as otherwise by a wireless card that is not aware of 802.11g.

Its features include:

- Bandwidth—54 Mbps
- Frequency—2.4 Ghz

802.11n

Currently emerging in the marketplace of wireless technologies is 802.11n, which increased the amount of bandwidth that was available in previous technologies up to 600 Mbps in some configurations. The 802.11n standard uses a new method of transmitting signals known as **multiple input and multiple output (MIMO)**, which can transmit multiple signals across multiple antennas. The 802.11n standard offers backward compatibility with 802.11g, so it will encourage adoption of the technology by consumers.

Its features include:

- Bandwidth—Up to 600 Mbps
- Frequency—2.4 Ghz

WHAT'S IN A NAME?

The name *Bluetooth* may seem odd, but it does have reasoning behind it. Bluetooth got its name from a Danish Viking king named Harald Blatland. In the tenth century, Blatland united all of Denmark and Norway under his rule, much as Bluetooth unites different technologies wirelessly. Why the name *Bluetooth*? King Harald apparently liked wild blueberries, which stained his teeth—leading people to call him "Bluetooth."

Other Wireless Technologies

While wireless networking in the form of 802.11 is probably the best known by the average consumer, other wireless technologies are in widespread use, including Bluetooth and WiMax.

Bluetooth

Bluetooth is a technology that emerged for the first time in 1998. From the beginning, Bluetooth was designed to be a short-range networking technology that could connect different devices together. The technology offers neither the performance nor the range of some other technologies,

but its intention wasn't to connect devices over long distances. Bluetooth was intended to be a connectivity technology that could allow devices to talk over a distance of no more than 10 meters with low bandwidth requirements. While the bandwidth may seem low, consider the fact that the technology is used to connect devices that do not need massive bandwidth like headsets and personal digital assistants (PDAs). Bluetooth falls into the category of technologies known as **Personal Area Networking (PAN)**.

NOTE

WiMax is being adopted as a technology to cover some metropolitan areas with wireless access in an effort to offer free Internet access to the masses.

WiMax

Another wireless technology that has emerged over the last few years is WiMax. WiMax is similar in concept to Wi-Fi, but uses different technologies. WiMax is specifically designed to deliver Internet access over the so-called last mile to homes or businesses that may not otherwise be able to get access. In theory, **WiMax can cover distances up to 30 miles**, but in practice ranges of 10 miles are more likely. The technology was not designed for local area networks; it would fall into the category of Metropolitan Area Networking (MAN).

Working with and Securing Bluetooth

Bluetooth emerged as a concept in the mid-1990s as a way to reduce the wires and cables that cluttered offices and other environments. **In 1998, the Bluetooth Special Interest Group (SIG) was created to develop the concept known as Bluetooth and to speed its adoption among the public.** The founders of this group included technology giants such as IBM, Intel, Nokia, Toshiba, and Ericsson. After the standard was implemented, manufacturers rapidly started manufacturing all sorts of Bluetooth devices—everything from mice to keyboards to printers showed up on the market, all Bluetooth enabled.

What makes the technology so attractive is its flexibility. Bluetooth has been used in numerous applications including:

- Connections between cell phones and hands-free headsets and earpieces
- Low bandwidth network applications
- Wireless PC input and output devices such as mice and keyboards
- Data transfer applications
- GPS connections
- Bar code scanners
- A replacement for infrared
- A supplement to universal serial bus (USB) applications
- Wireless bridging
- Video game consoles
- Wireless modems

Bluetooth has worked very well to link together devices wirelessly, but the technology has problems with security. Bluetooth does, however, support techniques that enforce security to make using enabled devices less vulnerable.

Bluetooth Security

Bluetooth technology was designed to include some security measures to make the technology safer. Each mechanism that is employed can be part of a solution to make using the technology acceptable to individuals and businesses.

Trusted Devices

Bluetooth employs security mechanisms called "trusted devices," which have the ability to exchange data without asking any permission because they are already trusted to do so.

BLUETOOTH EVERYWHERE

The victims of Bluetooth attacks aren't just computers, cell phones, and PDAs; they can be any type of Bluetooth-enabled system such as a car stereo. A new piece of software known as the Car Whisperer, for instance, allows an attacker to send and receive audio from a Bluetooth-enabled car stereo. As with any technology, the attacks will come along with every new innovation and upgrade. Device manufacturers try to anticipate every problem, but unfortunately they may be left doing firmware updates and patches later.

With trusted devices in use, any device that is not trusted will automatically prompt the user to decide whether to allow the connection or not.

A device that is trusted in this system should adhere to certain guidelines. It should be:

- A personal device that you own such as a cell phone, PDA, media player, or other similar device
- A device owned by the company and identified as such. These devices could include printers, PDAs, or similar types of devices.

An untrusted device is defined as follows:

- A device that is not under the immediate control of an individual or company is questionable. Devices that fall in this category are any public devices for which you cannot readily identify the owner nor trust the owner.

The idea behind trusted devices is that unknown devices are not allowed to connect without being explicitly approved. If an untrusted device were allowed to connect without being approved, it could mean that a device could accidentally or maliciously connect to a system and gain access to the device.

When working with Bluetooth-enabled devices, take special care to attach only to devices you know. Users should be taught to avoid attaching to devices that they do not know and cannot trust. Impress upon users the difference between trusted and untrusted devices when making connections. Stress that unsolicited connection requests should never be accepted

Discoverable Devices

In an effort to make Bluetooth devices easy to configure and pair with other devices, the discoverability feature was added to the product. When Bluetooth devices are set to be discoverable, they can be seen or discovered by other Bluetooth devices that are in range. The problem with a device being set to be discoverable is that it can be seen by the owners of devices who have both good and bad intentions. In fact, a discoverable device could allow an attacker to attach to a Bluetooth device undetected and swipe data off of it quite easily.

KNOW YOUR DEFAULTS

Device manufacturers such as those who make cell phones are known to set their devices to be discoverable by default. The idea behind having it as the default mode is that the device is easier for the consumer to use right out of the box. The security issue is that a consumer may not be aware of the security risks and leave this feature enabled.

Discoverability should be enabled only to pair devices and then be disabled afterward. This is a technique that newer models of these devices are starting to use.

KEEP YOUR ENEMIES CLOSE

Bluetooth hacking may seem like less of a problem because the range of the technology is only about 10 meters. But with most things in technology and security, there is always a work-around, and Bluetooth's range is no different. A 2004 article published in *Popular Science* (and available on its Web site) titled "Bluetooth a Mile Away," discussed how to extend Bluetooth's range substantially. The article showed how to modify simple, off-the-shelf components to boost the reach of Bluetooth way beyond what is specified, all for a price tag of less than \$70.

A simple exercise like this shows just how an attacker can change the nature of the "game" in creative ways. Attackers used to have to be in close proximity to the victim, but now they can be much farther away.

It is getting less common to find devices set with their default mode of operation to be discoverable. But don't take anything for granted. When issuing cell phones to employees, always check to make sure that the device is set to be nondiscoverable unless absolutely necessary.

Bluejacking, Bluesnarfing, and Bluebugging

Bluejacking, Bluesnarfing, and Bluebugging are attacks caused by devices being discoverable. Bluejacking involves a Bluetooth user transmitting a business card, a form of text message, to another Bluetooth user. If the recipient doesn't realize what the message is, he or she may allow

the contact to be added to their address book. After that, the sender becomes a trusted user. For example, **Bluejacking** allows someone authorized or unauthorized to send messages to a cell phone. The other threat posed by discoverability is **Bluesnarfing**, which is used to steal data from a phone. **Bluebugging** is an attack in which attackers can use the device being attacked for more than accessing data; they can use the services of the device for purposes such as making calls or sending text messages.

Viruses and Malware

An issue that was not initially addressed when Bluetooth debuted was viruses. Viruses were already a well-known fact of life in the computer world, but there really was not much done in Bluetooth to address viruses being spread. Early viruses leveraged the discoverability feature to locate and infect nearby devices with a malicious payload. Nowadays, most cell phones tend to use connections that require the sender to be authenticated and authorized prior to accepting any data, which severely curtails the capability of an unknown device to spread an infection. With the technology the way it stands now, a user must agree to open a file and install it—diminishing the potential threat, but not eliminating it.

NOTE

Never underestimate the creativity and ambition of an attacker or virus writer. They thrive in adapting their methods to leverage new technologies and devices, and wireless is no different. When Bluetooth debuted, no security was provided because no manufacturer perceived a threat; this opened the door to some notable attacks later.

Securing Bluetooth

Bluetooth isn't going away and shouldn't be shunned because of a few security issues; the technology can be secure if used carefully. The makers of Bluetooth have given us the tools to use the technology safely, and these tools coupled with a healthy dose of common sense can make all the difference.

NOTE

While Bluetooth manufacturers have given us the tools to secure the technology, it is definitely up to us to use them. Manufacturers may or may not enable security features on their devices.

Discovering

Ensure that discoverability on devices is disabled after pairings have been established between devices. In practice, there is no need for discoverability after a pairing has been made so the feature should be shut off unless it's needed for some other reason.

Working with Wireless LANs

Wireless LANs are built upon the 802.11 family of standards and operate in a similar manner to wired networks. The difference between the two beyond the obvious lack of wires is the fundamental functioning of the network itself.

CSMA/CD Versus CSMA/CA

One of the big differences between wired and wireless is the way signals are transmitted and received on the network.

In networks based on the Ethernet standard (802.3), stations transmit their information using what is known as the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) method. Networks that use this method have stations that transmit their information as needed, but collisions are possible when two stations transmit at the same time. To understand the method, think of the way a phone conversation works: Two people can talk and if they happen to talk at the same time, neither will be able to understand what is being said. In this situation, both talkers stop talking and wait to see who is going to talk instead. This is the same method that CSMA/CD uses. In this setup, if two stations transmit at the same time, a collision takes place and is detected; then both stop and wait for a random period of time before retransmitting.

In wireless networks based on the 802.11 standard, the method is a little different, and is called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Networks that use this method "listen" to see whether any other station is transmitting before they transmit themselves. This would be like looking both ways before crossing the street. Much as with CSMA/CD, if a station "hears" another station transmitting, it waits a random period of time before trying again.

FYI

APs offer a tremendous range of capabilities that dictate how the network operates. When choosing an AP, an organization needs to consider its goals, because choosing the wrong AP can severely hamper the performance of the net. For example, in large enterprises the consumer grade AP that can be purchased at an electronics retailer would be completely inappropriate in most cases due to its inability to offer enterprise security and management features.

Role of APs

An item that is present in wireless networks but not in wired networks is the access point (AP). An AP is a device that wireless clients associate to in order to gain access to the network (more on that later). In order for a wireless client to gain access to the services offered on the wired network on which the AP is connected, it must first associate to it.

APs come in many different types, with a diverse range of capabilities from the consumer to commercial grade. The choice of an AP can have a substantial impact on the overall performance and available features of the network, including range, security, and installation options.

Service Set Identifier (SSID)

A detail that is universally available in wireless networks is the service set identifier (SSID). The SSID **is used to uniquely identify a network**, thereby ensuring that clients can locate the correct **wireless local area network (WLAN)** that they should be attaching to. The SSID is attached to each packet as it is generated and is represented as a **32-character sequence uniquely identifying the network**.

The SSID is one of the first details that wireless clients will "see" when connecting to a network, so a few things should be considered. First, in most APs the SSID is set to a default setting such as the manufacturer's name (for example, "Linksys" or "dlink"), which should be changed to something more appropriate. Second, considerations should be made to turn off broadcast of the SSID where appropriate. By default in most networks the SSID broadcast is turned on, which means that the **ID will be broadcast, unencrypted**, in beacon frames. These beacon frames allow clients to much more easily associate with their AP, but also have the side effect of allowing software such as Netstumbler to identify the network and find its physical location.

OFF OR ON

There has been some debate about whether turning the SSID on or off is a good idea. On one side of the argument, turning it off makes it more difficult to locate an AP (but not impossible). In fact, **some experts have argued that turning off the broadcast isn't even worth doing because a serious attacker will find it more** of a speed bump than a wall in finding your network. On the other hand, turning the SSID broadcast on makes it easier for legitimate clients to find the network as well as making it easier for an attacker to locate. The question you have to answer in your situation is what the tradeoff of security versus convenience is for your clients and organization.

Association with an AP

Before a wireless client can work with a wireless network, a process known as association must take place. This process is actually quite simple, at least for our purposes, because association occurs when a wireless client has the SSID preconfigured for the network it is supposed to be attaching to. When it is configured in a wireless client, it will look for and then associate to the network whose value has been configured.

The Importance of Authentication

While not required, it is desirable to make sure that only those clients that you want to attach to your wireless network can do so. In order to restrict this access, **authentication is performed prior to the association process**. Authentication can be performed either in an open or preshared key situation, both offering features that may be desirable. With open keys, no secure authentication is performed and anyone can connect. When using this mode, no encryption is performed, so all information is sent in the clear unless another mechanism provides this feature. In **preshared key (PSK)** situations, **both the AP and client have the same key entered ahead of time and therefore can authenticate and associate securely**. This also has the benefit of encrypting traffic as well.

Working with RADIUS

In some organizations it is possible that you may have existing tools or infrastructure in place that can be used to authenticate wireless clients. One of these options is RADIUS or Remote Authentication Dial-In User Service.

The RADIUS service is one that is designed to centralize authentication, authorization, and accounting, or AAA. The service allows user accounts and their authorization levels to be stored on a single server and have all authentication and authorization requests forwarded to this location. By consolidating management in this manner it is possible to simplify administration and management of the network by making a single location to carry out these tasks.

NOTE

RADIUS is available on a wide range of operating systems and is supported by a wide range of enterprise level access points.

In practice when a user connects to wireless access point, his or her connection request can be forwarded to a RADIUS server. This request is then authenticated, authorized, and recorded (accounted), and access takes place as authorized.

Network Setup Options

Wireless networks and APs can relate in two ways: ad hoc or through infrastructure. Each of these options has advantages and disadvantages that make them attractive options. The following sections show you how they work.

Ad Hoc Network

Ad hoc networks can be created very quickly and easily because no AP is required in their setup. Ad hoc networks can be thought of as peer-to-peer networks in which each client can attach to any other client to send and receive information. These clients or nodes become part of one network sharing a form of SSID known as an Independent Basic Service Set (IBSS). While these networks are quick to set up, which is the primary advantage, they do not scale well because they become harder to manage and less secure as the number of clients grows.

Infrastructure Network

Infrastructure-based wireless networks are networks that use an AP that each client associates to. Each client in the network setup will be configured to use the SSID of the AP that will be used to send and receive information. This type of network scales very well compared with the ad hoc-based networks and is much more likely to be used in production environments. Additionally, infrastructure networks can scale to a much larger degree by simply adding more APs to create what is known as an extended service set (ESS).

Threats to Wireless LANs

Wireless networks offer many benefits similar to wired networks, but differ in the threats they face. Wireless networks have many threats that are unique to the way the technology works and each must be understood thoroughly prior to deploying the proper defenses.

Wardriving

Wardriving is the process of an attacker traveling through an area with the goal of detecting wireless APs or devices. An attacker who wants to engage in wardriving can do so with very basic equipment, usually a notebook with a wireless card and special software designed to detect wireless networks. In most cases those engaging in wardriving are looking to get free Internet access; however, it is more than possible for them to do much worse, such as accessing computers on the network, spreading viruses, or even downloading illegal software on someone else's dime.

Wardriving has led to a family of so-called "war" attacks that are all variations of the same concept:

- **Warwalking**—Attackers use a wireless-enabled device to detect wireless networks as they walk around an area.
- **Warbiking**—Same technique as warwalking, but on a bike
- **Warflying**—Relatively advanced technique that requires the same equipment as wardriving, but the process uses an aircraft instead of a car
- **Warballooning**—An attacker places a GPS and wireless detection gear on a cluster of small balloons and lets them float over an area. The device is later retrieved and the data imported into the appropriate software.

X MARKS THE SPOT

Another activity that occurs with all the "war" activities is warchalking. Someone finds a wireless network and places a marker identifying an AP on a curb, sign, wall, or other location. Warchalkers have developed their own symbols to mark locations and the type of AP (open, secured, and so on) that can be looked up online. The name comes from their usage of chalk to mark symbols in these locations.

Misconfigured Security Settings

Every AP, piece of software, or associated hardware has recommended security settings provided by the vendor by default or in the instruction booklet. In a vast number of cases, such as residential or small businesses, APs end up getting implemented without these most basic of settings configured. In some cases, such as with consumer-grade APs, the default settings on the equipment allow the device to work "out of the box," meaning that those that don't know otherwise will assume that everything is OK as is.

Unsecured Connections

Another concern with wireless security is what employees or users may be attaching to. It has been shown that at least 25 percent of business travelers attach to unsecured APs in locations such as hotels, airports, coffee shops, and other locations. This number is expected to increase as companies allow more individuals to travel and work in the field with the associated notebooks and similar devices. The concern with this situation is twofold: what users are transmitting and what is stored on their systems. Transmitting information over an unsecured AP can be extremely problematic and users who leave wireless access such as Bluetooth enabled on a notebook or cell phone may open themselves up to data theft or other dangerous situations.

PLUG AND PRAY?

It is not uncommon for home users or small businesses to purchase a consumer grade wireless router or AP and then simply plug it in and hope it works. In most cases, the manufacturer of a given piece of hardware configures the device so it will work out of the box to eliminate potential frustration on the part of the user when the device doesn't just plug in and work like a TV. The problem is that if a consumer plugs in a device such as a wireless router and it already works, he or she more than likely will not take the basic steps to secure it.

In other cases consumers have the attitude that they have nothing an attacker would want. It is not uncommon for a user to believe that the data is what an attacker wants, totally forgetting about the APs.

HERE, THERE, EVERYWHERE

Rogue APs can appear anywhere and attackers know this—but so do businesses. Some businesses have taken advantage of the basic human desire to get something for nothing, such as Internet access. For example, several businesses have placed rogue APs in different locations up and down the Las Vegas strip. In most cases, the APs are located outside large hotels where people will try to connect instead of paying the hotel to use their Internet. The problem with these APs is that many of them go to only one site that may offer anything from travel and entertainment to adult services.

Rogue APs

A problem with wireless is the appearance of rogue APs that have been installed without authorization. The problem with rogue APs comes on a few fronts because they are unmanaged, unknown, and unsecured in most cases. Rogue APs that are installed without the knowledge of the IT department are by their very nature unmanaged and have no controls placed upon them. They are known only to specific individuals, both good and bad. Finally, APs installed in this situation are frequently subject to little or no security, leading to unrestricted access by any party that locates the AP.

A new twist on rogue APs adds an element of phishing. In this attack, an attacker creates a rogue AP with a name that looks the same or is the same as a legitimate AP with the intention that unsuspecting users will attach to it. Once users attach to this AP, their credentials can be captured

by the attacker. By using the same method, an attacker can even capture sensitive data as it is transmitted over the network.

Promiscuous Clients

Promiscuous clients are APs that are configured to offer strong signals and the offer of good performance. The idea behind these types of APs is that a victim will notice the AP and how strong the signal is and how good the performance is, and then attach to it. When these APs are nearby, they may be owned by an attacker who has the same goals as the malicious owner of a rogue AP: to capture information.

Wireless Network Viruses

Viruses exist that are specifically designed to leverage the strengths and weaknesses of wireless technologies. Wireless viruses are different because they can replicate quickly using the wireless network, jumping from system to system with relative ease. For example, a virus known as MVW-WIFI can replicate through wireless networks by using one system to detect other nearby wireless networks; it then replicates to those networks, at which point the process repeats.

NOTE

While wireless viruses are restricted to 802.11 networks, they can and have appeared on other wireless technologies, including Bluetooth devices. In concept, 802.11 viruses and Bluetooth are the same, but the difference in practice is how they use their underlying technologies (wireless or Bluetooth).

Countermeasures

Protection on a wireless network is absolutely essential to consider and consider carefully. There are several techniques that you may use to protect yourself and your employees from harm, these include:

- **Firewalls**—In the case of roaming or remote clients that connect to wireless networks at the office or at the local coffee shop or airport, a good personal firewall can provide a much needed level of protection.
- **Antivirus**—An antivirus should be installed on every computer, and a wireless client is no exception, especially due to its higher exposure to threats.
- **VPN**—A virtual private network can enhance protection to a high degree by encrypting all traffic between the roaming client and the company network. By using this technique it is possible to work on a wireless network that has no protection itself and provide this through the VPN.

Wireless Hacking Tools

There are a number of wireless hacking tools available to the attacker who wants to break into or discover wireless networks. Some of the more common ones include:

- Kismet
- Netstumbler
- Medieval Bluetooth Scanner
- inSSIDer
- Coreimpact
- CFI LANguard Network Security Scanner
- Cowpatty
- Wireshark

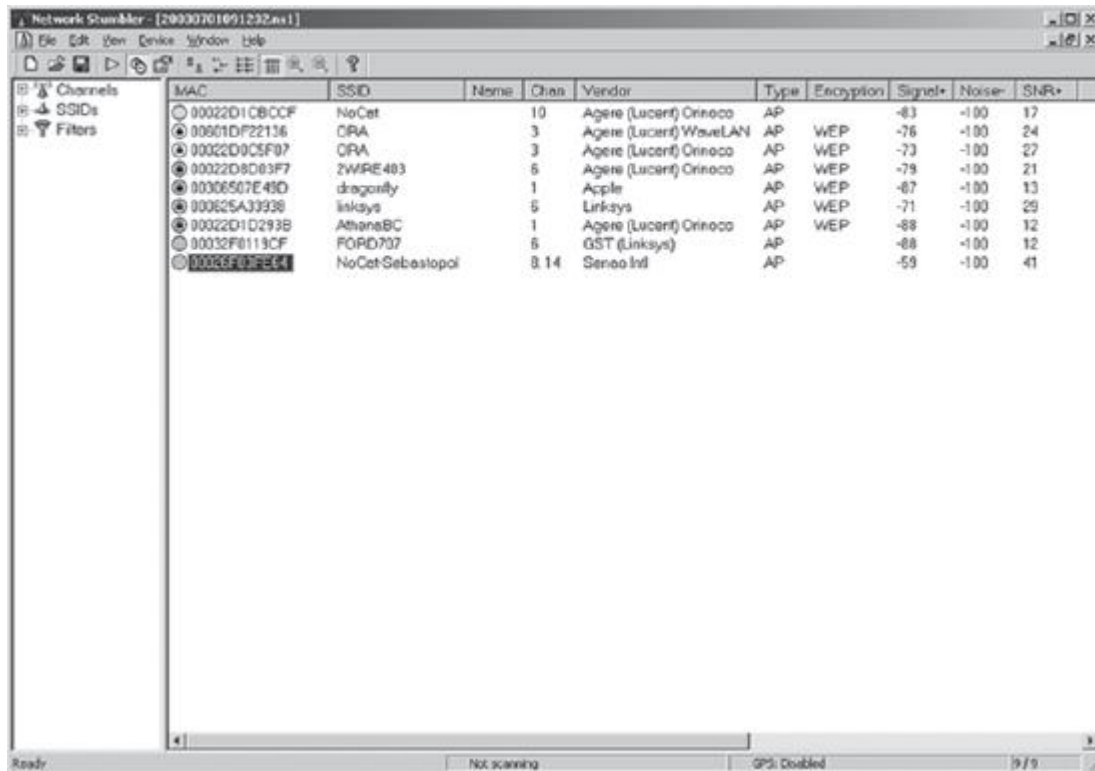


Figure 8-1. Netstumbler interface.

Netstumbler

Netstumbler is one of the more common tools for locating wireless networks of the 802.11 persuasion. The software is designed to detect any wireless network that your wireless network adapter supports (802.11a, 802.11b, 802.11g, and so on). The software also has the ability to interface with a USB global positioning system (GPS) to map out the location of the APs it detects, usually within a good distance of the actual AP. Netstumbler does not have many options and is very simple to use (see [Figure 8-1](#)).

NOTE

Netstumbler also comes in a version known as mini-stumbler, designed especially for PDAs.

inSSIDer

While Netstumbler software offers a good amount of functionality, it is not the only product that can perform wireless network scanning. Another piece of software that can do the same thing is inSSIDer. Metageek, the makers of inSSIDer, describe the benefits of their tool as follows.

Features unique to inSSIDer include:

- Uses Windows Vista and Windows XP 64-bit
- Uses the Native Wi-Fi application protocol interface (API) and current wireless network card
- Can group by Mac Address, SSID, Channel, received signal strength indicator (RSSI), and "Time Last Seen"
- Compatible with most GPS devices (NMEA v2.3 and higher)

The inSSIDer tool can do the following:

- Inspect your WLAN and surrounding networks to troubleshoot competing APs
- Track the strength of received signals in dBm (a measurement of decibels) over time
- Filter APs in an easy-to-use format
- Highlight APs for areas with high Wi-Fi concentration
- Export Wi-Fi and GPS data to a Keyhole Markup Language (KML) file to view in Google Earth

NOTE

Netstumbler has been a staple of wardriving techniques for awhile, but for all its popularity it does have some limitations, one of which is a lack of 64-bit support. The inSSIDer tool is a full featured replacement for Netstumbler.



Figure 8-2. The inSSIDer interface

The inSSIDer interface is shown in [Figure 8-2](#).

Once a target has been identified and its identifying information noted, the attack can begin.

Protecting Wireless Networks

Wireless networks can be secured if care is taken and knowledge of the vulnerabilities is possessed by the security professional. In some ways a wireless network can be secured like a wired network, but there are techniques specific to wireless networks that must be considered as well.

NOTE

Using a piece of software such as Netstumbler can discover APs. When one is detected, it is easy to look at the name of the AP and infer that whoever didn't change the name from something such as "Linksys" or "dlink" probably didn't do anything else, either.

Default AP Security

Every AP ships with certain defaults already set; these should always be changed. Every manufacturer includes some guidance on what to configure on its APs; this advice should always be followed and mixed with a healthy dose of experience in what is best. Not changing the defaults on an AP can be a big detriment to security because the defaults are generally posted on the manufacturer's Web site.

Placement

Placement of a wireless AP can be a potent security measure if undertaken properly. An AP should be placed to cover the areas it needs to, and not as much of the ones it doesn't. For example, an AP should not be located near a window if the people that will be connecting to it are deeper inside the building or only in the building. Positioning an AP near a window gives the signal more distance to emanate outside the building.

Of course, other issues with placement need to be addressed, in particular the issue of interference. Placement of APs near sources of electromagnetic interference (EMI) can lead to unusable or unavailable APs. EMI can lead to APs being available to clients, but with such poor performance that it makes the technology worthless to the organization.

Emanations

Not much can be done about emanations in wireless network, but there is something that can be done to control the scope and range of these emanations. In some cases, wireless directional antennas can be used to concentrate or focus the signal tightly into a certain area instead of letting it go everywhere. One type of antenna is the Yagi antenna, which can focus a signal into a narrow beam, making it difficult to pick up by others outside the select area.

Rogue APs

Rogue APs are somewhat tough to stop, but they can be detected and deterred. The first action to address with rogue APs is the installation of unauthorized ones by employees. In this case, education is the first line of defense; let employees know that installation of rogue APs is not allowed and why. Additionally, perform site surveys using tools such as Netstumbler, Kismet, or any number of commercial wireless site survey packages to detect rogue APs.

The second issue to deal with is individuals connecting to the wrong or to unauthorized APs. In these cases education is again key. Let employees know the names of company-controlled APs and give them information about the dangers of connecting to unknown APs.

Use Protection for Transmitted Data

By its very nature, wireless data is transmitted so that anyone who wants to listen in can do so. In order to protect wireless networks an appropriate authentication technology should be used. The three that are currently in use are:

- **Wired Equivalent Privacy (WEP)**—Not much used anymore because it is weak and only marginally better than no protection at all. WEP was available on all first-generation wireless networks, but was replaced later with stronger technologies such as WPA.

In theory, WEP was supposed to provide protection, but in practice poor implementation resulted in the use of weak keys. It was found that with enough weak keys simple cryptanalysis could be performed, and a WEP passphrase can now be broken in a few minutes (sometimes 30 seconds).

- **Wi-Fi Protected Access (WPA)**—More robust than WEP, it was designed to replace it in new networks. WPA introduces stronger encryption and better key management that makes for a stronger system.

WPA is supported on most wireless APs manufactured after 2003, and some manufactured prior to this can have their firmware upgraded. WPA should be used if the AP offers the ability to use WEP or WPA.

- **Wi-Fi Protected Access version 2 (WPA2)**—WPA2 is an upgrade to WPA that introduces stronger encryption and eliminates a few of the remaining weaknesses in WPA.

NOTE

WEP is listed here in the interest of completeness; however, in practice WEP should be avoided at all costs due to its well-known weaknesses. Using an alternative method such as WPA or WPA2 would be much more secure.

Using the appropriate protection for a wireless network is important because it can protect the network from eavesdropping and other attacks in which an attacker can see network traffic. Of course, just having a good protection scheme does not make for a safe environment by itself; there are other factors. In the case of WPA and WPA2, the keys in use make a major difference for how effective the technology is. Using poorly chosen or short passwords (or keys) can weaken the protection and make it breakable by a knowledgeable attacker. When choosing a key it should be random, be of sufficient length, and adhere to the rules for complex passwords.

NOTE

While MAC filtering does provide a level of protection, a determined attacker can get past it with some knowledge of how networks work. It is also very difficult to use in all but the smallest environments, as managing MAC lists can become very cumbersome.

MAC Filtering

Media access control (MAC) address filtering is a way to enforce access control on a wireless network by registering the MAC addresses of wireless clients with the AP. Because the MAC address is supposed to be unique, clients are limited to those systems that have their MAC

preregistered. To set up MAC filtering you need to record the MAC addresses of each client that will use your AP and register those clients on the AP.

CHAPTER SUMMARY

Wireless communication and networking are technologies that have seen rapid growth and adoption over the past few years. Many organizations have chosen to use wireless technologies due to the increased mobility and ability to extend networks that wireless offers. Wireless has become one of the most widely used technologies by both consumers and businesses, and will most likely continue to be so.

For all the benefits that wireless offers, the big concern for the security professional is security. Wireless technologies have many security issues, both real and potential, that must be addressed by the security professional. The technology suffers from poor or even overlooked security options by those who either adopted the technology too quickly or didn't take the time to understand the issues.

This chapter explored how to use wireless technology in an organization, reaping its benefits and doing so securely. Like any technology, wireless can be used safely; it is only a matter of understanding the tools available to make the system secure. To make wireless secure, you can leverage techniques such as encryption and authentication together with other features designed to make the system stronger and more appealing to the business.

KEY CONCEPTS AND TERMS

- 802.11
- Bluebugging
- Bluejacking
- Bluesnarfing
- Multiple input and multiple output (MIMO)
- Personal Area Networking (PAN)
- Preshared key (PSK)
- Wi-Fi
- Wireless local area network (WLAN)

CHAPTER 8 ASSESSMENT

1. Wireless refers to all the technologies that make up 802.11.
 1. True
 2. False
2. _____ operates at 5 Ghz.
 1. 802.11a
 2. 802.11b
 3. 802.11g

4. 802.11n
3. _____ is a short range wireless technology.
4. Which type of network requires an AP?
 1. Infrastructure
 2. Ad hoc
 3. Peer-to-peer
 4. Client Server
5. _____dictate(s) the performance of a wireless network.
 1. Clients
 2. Interference
 3. APs
 4. All of the above
6. _____blocks systems based on physical address.
 1. MAC Filtering
 2. Authentication
 3. Association
 4. WEP
7. An ad hoc network scales well in production environments.
 1. True
 2. False
8. Which of the following is used to identify a wireless network?
 1. SSID
 2. IBSS
 3. Key
 4. Frequency
9. Several APs group together form a(n)_____.
 1. BSS
 2. SSID
 3. EBSS
 4. EBS
10. _____uses trusted devices.
 1. 802.11
 2. Infrared
 3. Bluetooth
 4. CSMA