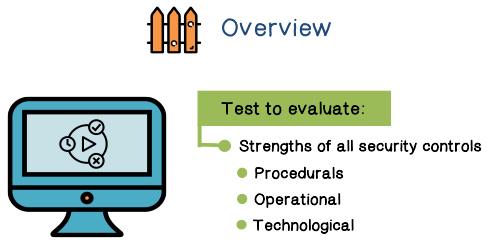
The recommended reading for this lesson is:

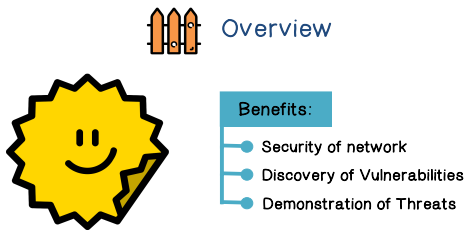
The Hacker Playbook – Practical Guide to Penetration Testing, by Peter Kim

You can find short summary of the paper at the end of the document.

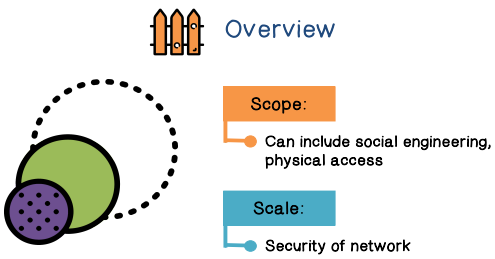
In this lesson, we will discuss the first line of network defense: the basic tools and techniques of penetration testing and security assessments. We will also discuss one of the most powerful tools of the network hacker, you. Yes, you and me. In fact, everyone has a potential to be a hacker's best friend. Social engineering is a fast, low risk method to gain access to data. Pay close attention to the methods used and think about how they can be deployed to make a network more secure.



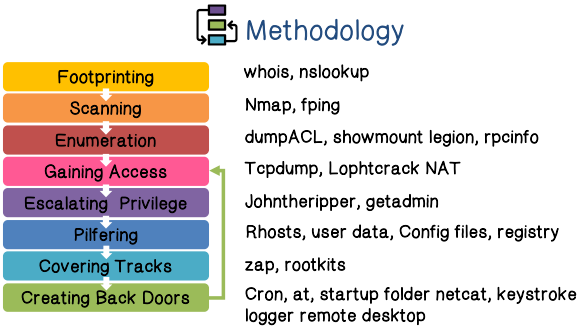
Let us have an overview of what penetration testing is all about. Penetration testing is used to evaluate the security of a network. More specifically, penetration testing is used to evaluate all security controls. These include the security procedures, the operations, and the technologies.



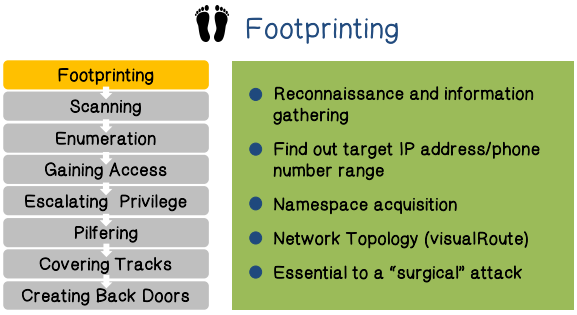
With penetration testing, you can find out how secure your network really is. In particular, you can discover security vulnerabilities. And by actually exploiting the vulnerabilities, you can also demonstrate how likely the threats can take place and what the likely damages associated with these threats are.



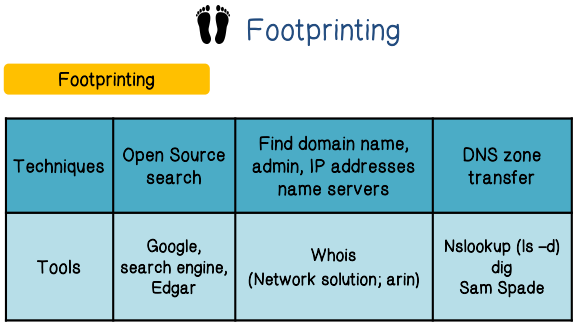
The scope of penetration testing includes not just technical or cyber operations, it can also include social engineering, and also gaining physical access to your organization. The scale of the testing includes the entire network. For example, the testing may include your mobile devices, or BYOD.



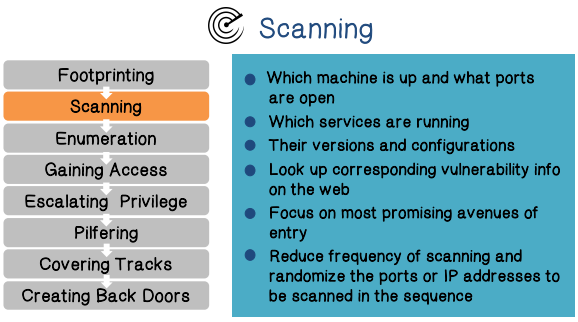
Now let us discuss the methodology of penetration testing. Penetration testing includes several steps. The first step is footprinting. This is about finding the general information of your network. Next step is scanning. This is about finding more detailed information about your network, such as the services available on your network. The third step is enumeration. It finds more target information such as user account. The fourth step is gaining access. It finds vulnerabilities associated with the network services, and then exploit these vulnerabilities to gain access to the network. The fifth step is escalating privilege. The goal here is to gain root or super user access. The sixth step is pilfering. The goal here is to try to steal information from the network. This is one of the standard activities that an attacker would do to a network. The seventh step is covering the tracks. The goal here is to hide an evidence of a break-in so that security admins cannot easily find out that the network has been breached. The last step here is creating back doors. The goal is to create easy access for future malicious activities on the network. The last few steps can be iterated for example to move from one part of the network to another part.



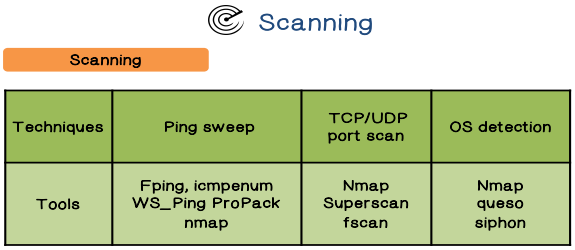
Now, let us discuss these steps in more details. The first step is footprinting. In this step, the attacker, or tester, conducts reconnaissance and information gathering. The important network information includes network IP addresses, the namespace, and topology. Even a phone number range can be used for modem access or social engineering. Such information is critical for planning the next steps of testing or attacks. For example, you will need the IP addresses to decide how to scan the network.



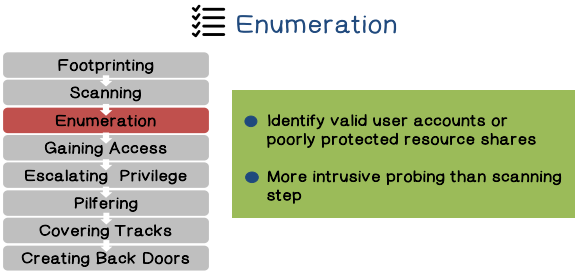
Here we will list the different techniques and the corresponding tools for footprinting. For example, you can use Google to find out the company information and use whois to find out the domain name information of the name servers and IP ranges.



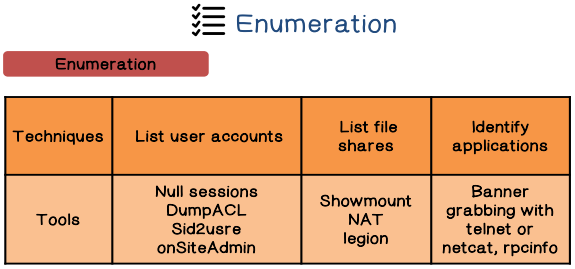
Once you have the general information such as the IP ranges of a network, now you gain more detailed information of the network using scanning. You can find out which machine is up, and which ports are open, and similarly on the servers what services are running. You can even find out the versions and configurations of these services. Then you can look up the corresponding vulnerability information on the web. For example, for a particular version of the Apache web server, you can look it up on the web to see one of the known vulnerabilities, such as what input can cause a buffer overflow. Most promising avenues are typically associated with services that are always up, such as the web services, so you want to focus on analyzing these services. On the other hand, you want to avoid detection, so you want to reduce the frequency and volume of your scanning and analysis.



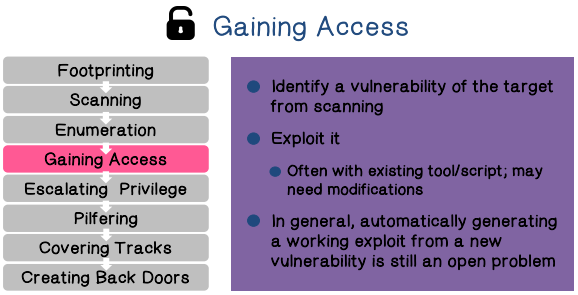
Here are the different techniques and tools for scanning. As you can see, Nmap is one of the most popular tools It can find out which IP's up, which port is open and even perform OS fingerprinting.



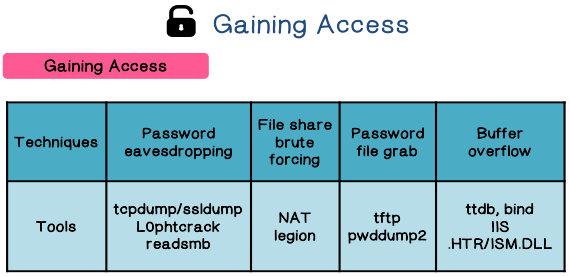
You can also perform more targeted attack or testing by figuring out which user accounts are poorly protected. And obviously, this is more targeted and intrusive than scanning.



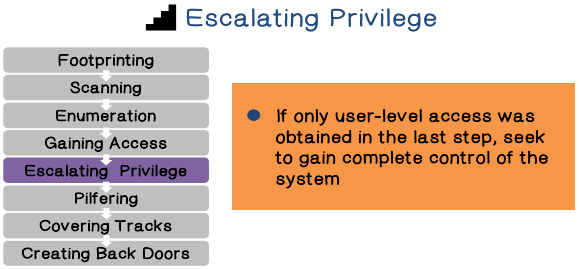
And here are the techniques and tools for enumeration. For example, you can use these tools to list user accounts and find out file sharing information.



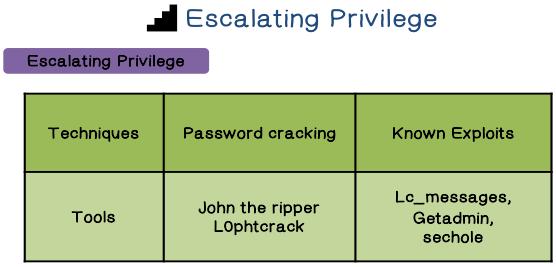
Once you have obtained the relevant information of network services and user accounts, now you can exploit and gain access to the network. Typically, there are existing tools and scripts associated with known vulnerabilities. But of course, you can customize them to suit your needs. On the other hand, if the vulnerability is new or there does not exist a tool or script, then you have to develop the exploit yourself. In general, this is a manual process and can be quite difficult.



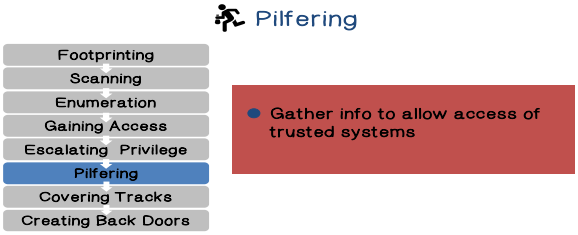
Here are some examples of the techniques and tools for gaining access. For example, you can use tools to capture and crack password. And there are tools that will exploit vulnerabilities in widely used services.



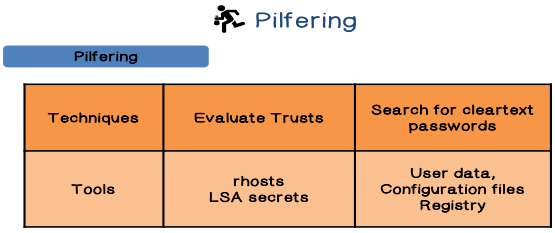
The next step is escalating privilege. And the goal is to gain super user access so that you can gain complete control of the system.



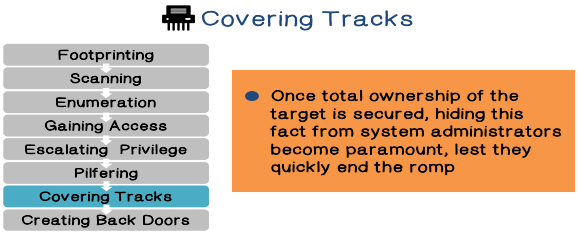
Here are some examples and tools. Again, you can capture and crack the super user passwords. There are tools that will exploit vulnerabilities of privileged services in order to help you gain good access.



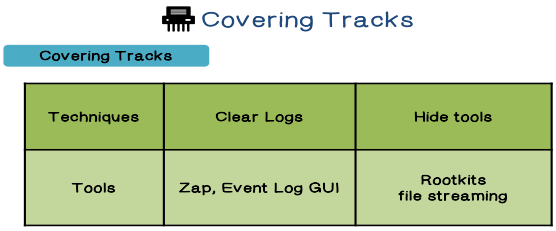
After you have gained access to the system, now you can steal valuable information. Such information can allow you further access to the system.



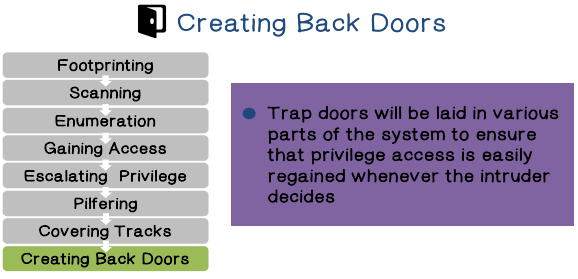
For example, you can discover the trust relationship among the machines on a network, and you can obtain user credentials such as passwords.



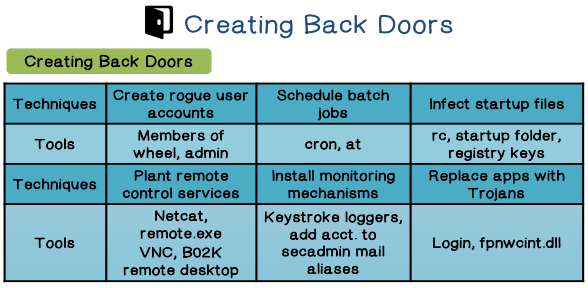
It is important to cover the tracks, so that the attack cannot be detected and stopped easily.



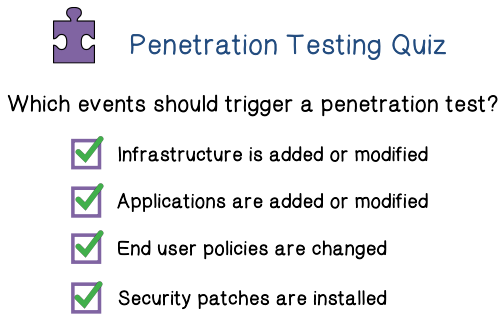
For example, you can use these tools to edit or even clear the system logs, and you can use rootkit to hide your malware.



The first-time gaining access to a network through an exploit is always hard. And you want subsequent access to be easy and look normal, so you will create trap doors or back doors.

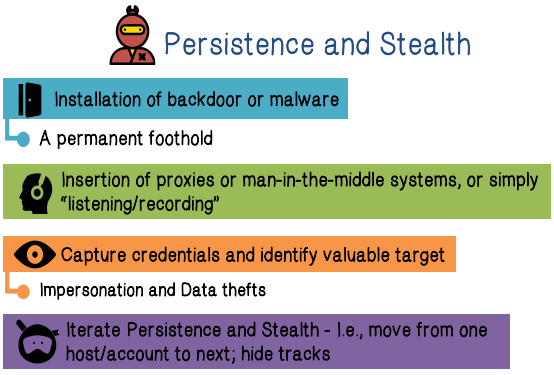


There are many techniques and tools. For example, you can create fake user accounts, or you can plant remote access services. You can also schedule your activities at certain time.

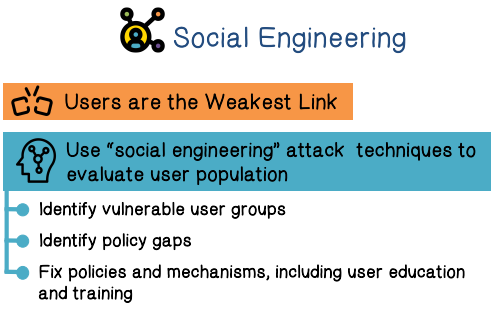


Now let's do a quiz on penetration testing. Which events should trigger a penetration testing?

All of these events should trigger a penetration testing. I should also add that penetration testing should also be done on a regular basis as well as on these triggering events.

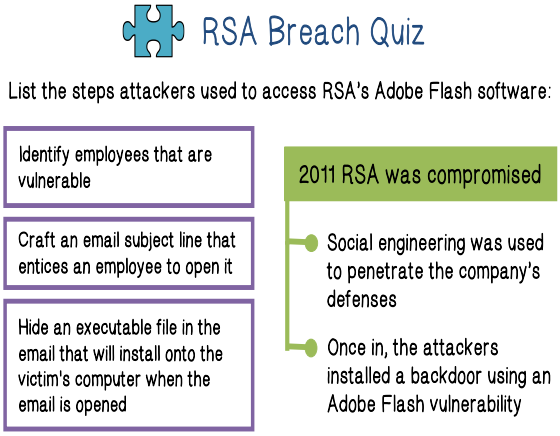


To simulate the modern attacks, such as the so called advanced persistent threats. Penetration testing can try to be persistent and stealth. For example, the tester can install a backdoor through a malware so that there is a permanent foothold in the network. The malware can be placed in a strategic place such as a proxy. And the result can be that now the malware can listen and record all traffic within the network. And by analyzing internal traffic, the malware can capture user credentials and find out valuable information. These steps can be iterated and moved from one port of the network to the next while hiding the tracks.



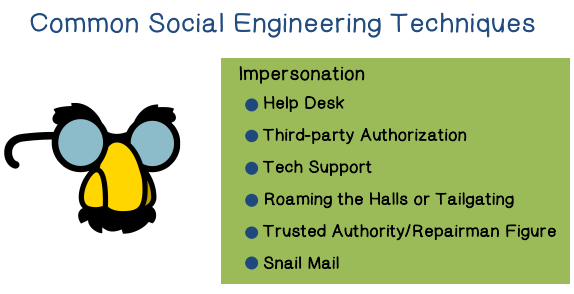
As we discussed earlier, penetration testing can include social engineering. So now let us discuss social engineering. We all know that users are the weakest link in security, so the goal here is to use social engineering techniques to evaluate how vulnerable your user population really is. In particular, you will want to find out which user groups are particularly vulnerable. You will likely discover policy gaps, so you will want to fix these policies and develop new mechanisms including educating and training the users.

Social engineering is effective when the users are manipulated into undermining the security of their own systems. This can be accomplished by abusing the trust relationships among the users. Social engineering can be very easy and cheap for the attacker because the attacker does not need any specialized tools or technical skills.

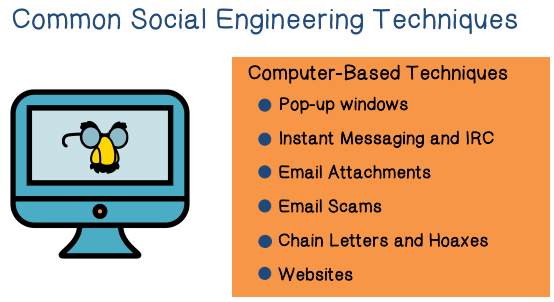


Now let's do a quiz. In 2011, the security company, RSA, was compromised. And it began with social engineering. Once gaining access, the attackers then installed backdoor using an Adobe Flash vulnerability. In this quiz, list the steps the attackers used to access RSA's Adobe Flash software.

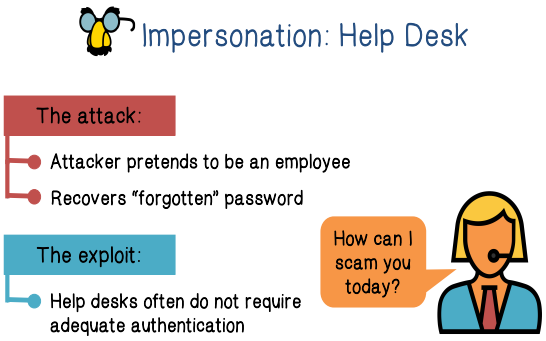
The first step is to identify employees that are vulnerable. The second step was crafting an email with an enticing subject line. In particular, the subject line was a provocative "2011 recruitment plan". And one employee was intrigued enough to open it. The first step is to hide an executable file in the e-mail, so that it will install on the victim's computer when the e-mail is opened. In this case, the attachment is an Excel spreadsheet, that contains a zero-day exploit that leads to a back door through Adobe Flash. This one e-mail resulted in a loss of $66 million for RSA.



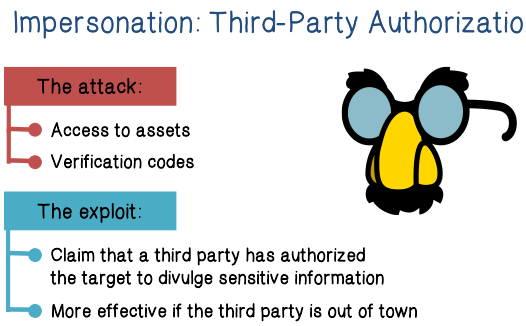
Now let us discuss the common social engineering techniques. The first category is impersonation. For example, you can impersonate help desks, third-party authorization, technical support. Or you can roam the halls or tailgate, or you can impersonate a trusted authority. And you can even send snail mail.



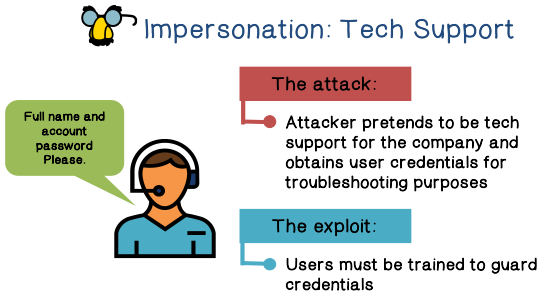
The other category of social engineering techniques involves the use of computers. These include pop-up windows, instant messages and IRC, email attachments, email scams, chain letters, and websites.



Let us discuss the impersonation techniques first. For example, an attacker can pretend to be an employee and call the help desk and claim that he has forgotten his password. A common weakness is that, the help desk does not require adequate authentication. For example, the help desk may just ask for the mother's maiden name. And the attacker may only know this, because he has read the Facebook information of the employee.



Another impersonation technique is to fake a third-party authorization. For example, the attacker can claim that a third-party has authorized him to access the network. And if the attacker can provide the information to convince people that he really knows the third party, then, he will have easy time gaining the trust and the access to the network, in particular, if the third-party is not present.

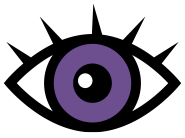


Another very effective impersonation technique is to pretend to be a tech support person. For example, the attacker can claim that the company needs to reconfigure its systems and ask for user credentials. If the users have not been properly trained to guard their credentials, then this attack can easily succeed.

Impersonation: Roaming the Halls

The attack:
- Attacker dresses to blend in with the environment

The exploit:
- Looks for sensitive information that has been left unattended
  - Passwords written down
  - Important papers
  - Confidential conversations



Another old-fashioned way of impersonation is to just walk around and see what information is valuable, for example, passwords or sticky notes, or other kind of important documents, or even overhearing important conversations.

Impersonation: Repairman

The attack:
- Attacker wears the appropriate uniform
- Often allowed into sensitive environments
- May plant surveillance equipment
- Could find sensitive information

The exploit:
- People rarely question someone in a uniform

An attacker can dress up like a repairman, because a repairman is typically allowed access to the facility. The attacker can then plant listening devices to capture useful information. This exploit works because users typically do not question people in uniform.

Impersonation: Trusted Authority Figure

The attack:
- Attacker pretends to be someone in charge of a company or department
- Similar to "third-party authorization" attack
- Impersonation in person or via telephone

The exploit:
- Trust in perceived authority

Similarly, an attacker can pretend to be someone in charge of a department or company. For example, the attacker can pretend to be medical personnel, a home inspector, or school superintendent. In each of these examples, the attacker can actually gain useful information from a user such as address, mother's maiden name, and so on. And this information can then be used to impersonate the employee through the call to a help desk. Again, this exploit works because users tend to trust authority.

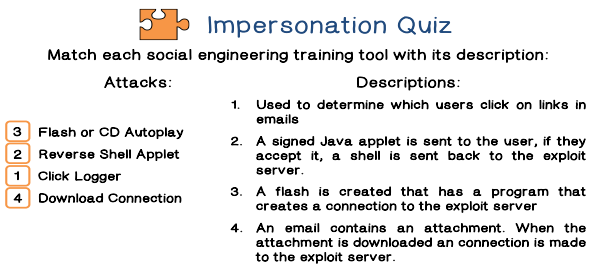
Impersonation: Snail Mail

The attack:
- Attacker sends mail that asks for personal information

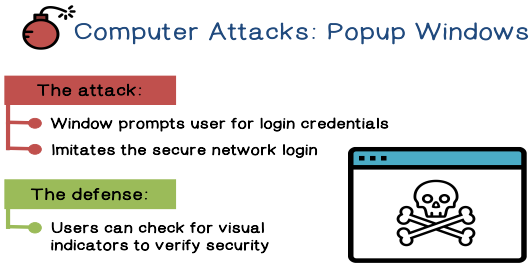
The exploit:
- People are more trusting of printed words than webpages

Examples
- Fake sweepstakes
- Free offers
- Rewards programs
- More effective on older generations

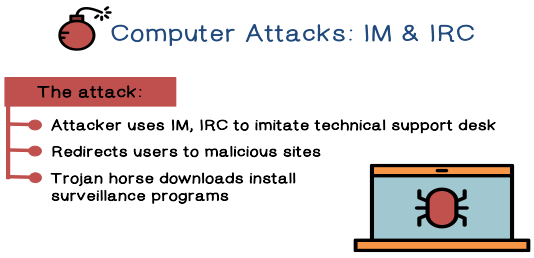
Impersonation can also take place in snail mail. For example, an attacker can send mail to a user pretending to be an authority and ask for personal information. This exploit works because users tend to trust the printed materials more than webpages and emails. These are examples that I am sure you are familiar with.



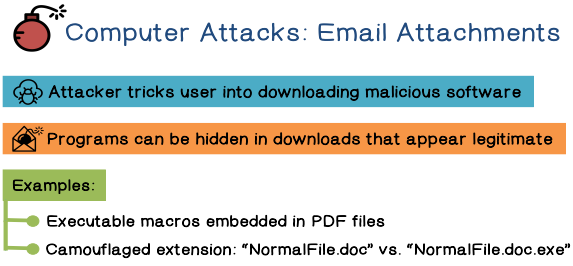
Now let's do a quiz on impersonation. Match each tool with its description.



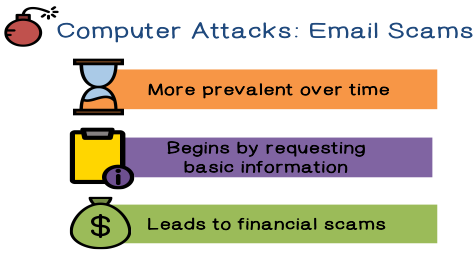
Now let's discuss social engineering attacks that involves computers. The first kind is popup windows. For example, a popup window can pretend to be a login window. This exploit will work if the users have not been properly trained to tell the difference between the fake and the legitimate login windows.



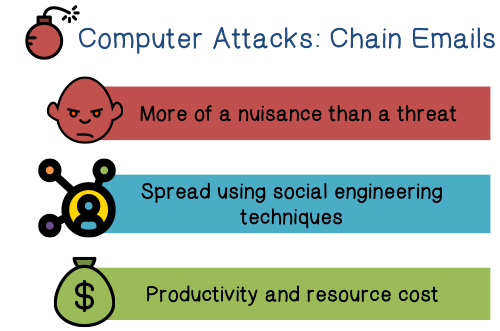
The attacker can also use IM or IRC to fake a technical support desk. And the users would be redirected to a malicious site and malware can then be downloaded.



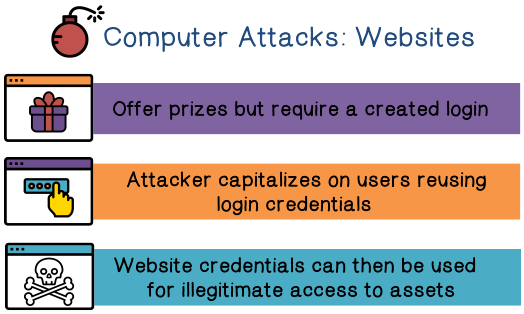
An attacker can also trick the user to open an email and download email attachment which includes malicious software. There are many ways to hide malicious programs in email attachments that may appear to be legitimate. For example, PDF files can include executable macros and a .exe file can be camouflaged into a .doc file.



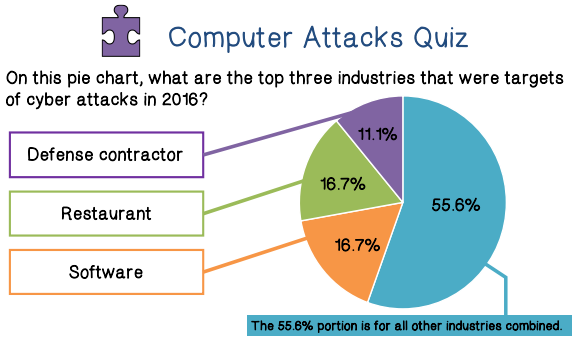
And of course, we are familiar with various kinds of email scams.



The attackers can amplify the effects of email scams using chain emails. For example, an email can be sent to everybody on your address book.

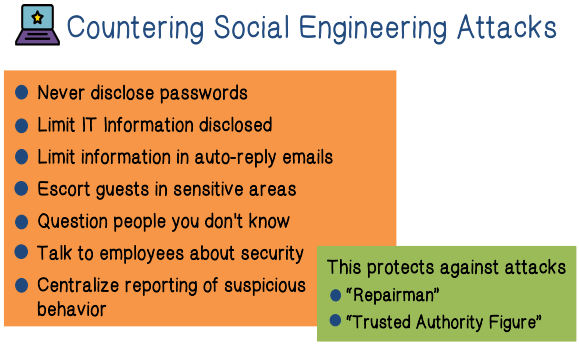


An attacker can create a website that claims to offer prizes but require the user to create login and passwords. The goal of the attacker is to harvest user credentials since many users uses same username and password on many websites. The attacker can then use the credentials obtained from his website on other websites.



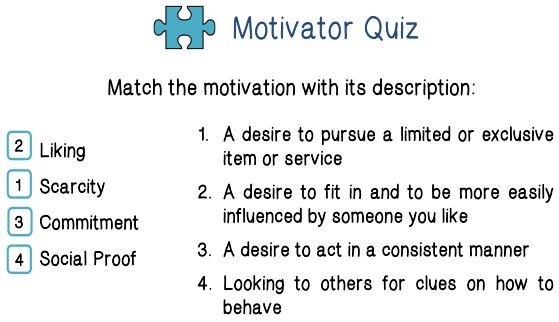
Now let us do a quiz. On this pie chart, what are the top three industries that were targets of cyberattacks in 2016?

Defense contractors, restaurants, and software companies. The other 56% consists of industries. They are targeted about 5.6% each.



Here's how we should educate users to counter social engineering attacks. Never disclose passwords to anybody. Only the IT staff should discuss details of the network and system configurations and IT staff should not answer survey calls. They should also check whether the call from the vendor is legitimate or not. Also, we should limit information in all auto-reply emails. Keep information in all auto-reply emails to a bare

minimum. We should always escort our guests. This protects against attacks such as attackers dressing up like repairmen or trusted authority figure. We should always question people that we do not know. We should educate all employees about security, both physical and IT security. We should have a central reporting and management of all suspicious behavior.



Let us do a quiz on human behaviors. Match the motivation with its description.

Liking is a desire to fit in. Scarcity is a desire to pursue a limited or exclusive item or service. Commitment is a desire to act in a consistent manner. Social proof is looking to others for clues on how to behave.

The Hacker playbook – Practical guide to Penetration Testing

The book is split into ten major parts:

1. Pregame – This section talks about how you set up the different attacking machines that are required in the process of Penetration testing and the tools that are needed to effectively execute the tests. It talks about how to setup a penetration testing box, the accompanying hardware and commercial software required. It gives an introduction to Kali Linux and a step-by-step setup of the environment.

2. Before the Snap – This section explores the scanning methods used generally for network scanning in penetration testing. It provides a comprehensive list of methods for external and internal discovery. This is followed by a detailed explanation of network and web application scanning and the methods to achieve it.

3. The Drive – After scanning the network and related resources, this section gives a high-level overview of the vulnerabilities identified by the scans and different methods used to exploit these vulnerabilities. The section looks at Nexpose, Nessus and Metasploit. It gives a baseline overview on how to take the findings from the scanner results and put them into action.

4. The Throw – This section focuses on taking the findings from the web application scanning and use it for manual testing to achieve system compromise. It covers SQL injection, cross-site scripting, cross-site forgery attacks, session token entropy, fuzzing or input validation and business logic. Each type of attack is explained with examples and will help the students implement these attacks with ease.

5. The Lateral Pass – This section talks about efficient ways to move through the network and gain access to domain administrative accounts. It explains how to access the network without having any credentials for that network. It explains what must be done post exploit using powersploit and powershell. Address resource poisoning is discussed along with steps to spoof ARP and what can be done post exploitation.

6. The Screen – This section is dedicated to social engineering attacks. It starts off with explaining doppelganger domains and how these can be used to effectively brute force domains for valid subdomains that have important MX records. Spear phishing, the social engineering toolkit on Kali Linux and social engineering using Microsoft excel are explained in detail in this chapter.

7. The Onside Kick – It discusses the types of attacks that require physical access to the resources to execute them. They explore exploiting wireless networks, physical penetration tests (card cloning, penetration drop box) and physical social engineering.

8. The Quarterback sneak – This chapter focuses on how to evade Anti-virus technologies while performing penetration tests. It talks about different methods to evade using Python and Evade.

9. Special Teams – This includes all the miscellaneous trips and tricks that do not fall under the other categories of penetration testing. This includes password cracking, vulnerability searching, how to use RC scripts within Metasploit, and hiding files on Windows.

10. Post-Game Analysis – An important aspect of penetration testing is reporting, it is as important as the test itself. A good pen tester must know how to record and display his findings in a way that the company understands and can use this information to take useful actions to patch these vulnerabilities. This section contains a list of best habits while writing reports for the penetration tests.