

CEH – Certification: Final Review

Table of Contents

Overview	1
Schedule.....	1
References	3
Testout Course Outline	3
2. Introduction to Penetration Testing	3
2.3.3. Target Selection Facts	4
2.4.3 Assessment Type Facts	7
2.5.4 Legal and Ethical Compliance Facts	9
2.5.6 Engagement Contract Facts	10
3. Social Engineering and Physical Security	12
3.1.2 Social Engineering Overview Facts.....	13
3.1.4 Social Engineering Motivation Facts	15
3.1.6 Social Engineering Techniques Facts.....	18
4. Reconnaissance.....	22
ExamTopics Review Questions.....	23
The end!	23

Overview

Schedule

Weeks	Activities
Week 1: 7/26/21	1. Review ExamTopics Questions <ul style="list-style-type: none">a. Part 1: Questions 1 to 52b. Part 2: Questions 53 to 86c. Part 3: Questions 87 to 122 2. Review Testout Course Material <ul style="list-style-type: none">a. Chapter 1: Introduction to Penetration Testingb. Chapter 2: Social Engineering and Physical Securityc. Chapter 3: Reconnaissance
Week 2: 8/1/21	3. Review ExamTopics Questions <ul style="list-style-type: none">a. Part 3: Questionsb. Part 4: Questions




	<ul style="list-style-type: none"> c. Part 6: Questions 4. Review Testout Course Material <ul style="list-style-type: none"> a. Chapter 4: b. Chapter 5: c. Chapter 6:
9/25/21	Take the exam

References




Testout Course Outline

2. Introduction to Penetration Testing





2.1 Penetration Testing Process and Types

- ✓  2.1.1 Penetration Test Process and Types
- ✓  2.1.2 Penetration Test Process and Types Facts
- ✓  2.1.3 Practice Questions





2.2 Threat Actors

- ✓  2.2.1 Threat Actor Types
- ✓  2.2.2 Threat Actor Type Facts
- ✓  2.2.3 Practice Questions

2.3 Target Selection

- ✓  2.3.1 Choose a Target
- ✓  2.3.2 Additional Scoping Considerations
- ✓  2.3.3 Target Selection Facts
- ✓  2.3.4 Practice Questions

2.4 Assessment Types

- ✓  2.4.1 Assessment Types
- ✓  2.4.2 Special Considerations
- ✓  2.4.3 Assessment Type Facts
- ✓  2.4.4 Practice Questions

2.5 Legal and Ethical Compliance

- ✓  2.5.1 Legal Compliance
-  2.5.2 Ethics
- ✓  2.5.3 Authorization and Corporate Policies
- ✓  2.5.4 Legal and Ethical Compliance Facts
- ✓  2.5.5 Engagement Contracts
- ✓  2.5.6 Engagement Contract Facts
- ✓  2.5.7 Practice Questions

2.3.3. Target Selection Facts

2.3.3 Target Selection Facts

Before beginning a penetration test, there are a lot of details that must be worked out. These details include the type of test being performed and any test limitations. After the

initial plans and details for a penetration test have been put together, there are some additional details that should be considered. These include performing a risk assessment, determining tolerance, scheduling the test, and identifying security exceptions that may be applied to the penetration tester.

This lesson covers the following topics:

- Penetration test planning
- Security exceptions
- Risk assessment
- Determine tolerance
- Scope creep

Penetration Test Planning

Detail	Description
How	One of the first items to consider is the type of test to be performed, internal or external. An internal test focuses on systems that reside behind the firewall. This would probably be a white box test. An external test focuses on systems that exist outside the firewall, such as a web server. This would, more than likely, be a black box test.
Who	Determine if the penetration tester is allowed to use social engineering attacks that target users. It's common knowledge that users are generally the weakest link in any security system. Often, a penetration test can target users to gain access. You should also pre-determine who will know when the test is taking place.
What	The organization and the penetration tester need to agree on which systems will be targeted. The penetration tester needs to know exactly which systems are being tested, and as they cannot target any area that isn't specified by documentation. For example, the organization may have a website they do not want targeted or tested. Some other systems that need to look at include wireless networks and applications.
When	Scheduling the test is very important. Should the test be run during business hours? If so, this may result in an interruption of normal business procedures. Running the tests when the business is closed (during weekends, holidays, or after-hours) may be better, but might limit the test.
Where	Finally, will the test be run on site, or remotely? An on-site test allows better testing results but may be more expensive than a remote test.

Security Exceptions

A security exception is any deviation from standard operating security protocols. The type of test (white box, black box, grey box) will determine what, if any, security exceptions the penetration test will be given.

Risk Assessment

The purpose of a risk assessment is to identify areas of vulnerability within the organization's network. The risk assessment should look at all areas, including high value data, network systems, web applications, online information, and physical security (operating systems and web servers). Often, the penetration test is performed as part of a risk assessment.

Once vulnerabilities have been determined, the organization needs to rank them and figure out how to handle each risk. There are four common methods for dealing with risk:

1. Avoidance: whenever you can avoid a risk, you should. This means performing only actions that are needed, such as collecting only relevant user data.
2. Transference: the process of moving the risk to another entity, such as a third party.
3. Mitigation: this technique is also known as risk reduction. When the risk cannot be avoided or transferred, steps should be taken to reduce the damage that can occur.
4. Acceptance: sometimes the cost to mitigate a risk outweighs the risk's potentially damaging effects. In such cases, the organization will simply accept the risk.

Determine Tolerance

After the risk assessment has been performed and vulnerable areas are identified, the organization needs to decide its tolerance level in performing a penetration test. There may be areas of operation that absolutely cannot be taken down or affected during the test. Areas of risk that can be tolerated need to be placed in the scope of work, and critical areas may need to be placed out of the test's scope.

Scope Creep

In project management, one of the most dangerous issues is scope creep. This is when the client begins asking for small deviations from the scope of work. This can cause the project to go off track and increase the time and resources needed to complete it. When a change to the scope of work is requested, a change order should be filled out and agreed on. Once this is done, the additional tasks can be completed.

2.4.3 Assessment Type Facts

An organization's purpose for completing a penetration test will dictate how the test will be carried out. Depending on the penetration test's goals, the ethical hacker may have specific rules and regulations that need to be observed. There are scenarios that will result in special considerations being made.

This lesson covers the following topics:

- Goal-based penetration test
- Objective-based penetration test
- Compliance-based penetration test
- Special considerations

Goal-Based Penetration Test

A goal-based penetration test will focus on the end results. The goals must be specific and well-defined before the test can begin. The penetration tester will utilize a wide range of skills and methods to carry out the test and meet the goals. When you determine the goals of the exam, you should use S.M.A.R.T. goals.

- S – Specific
- M – Measurable
- A – Attainable
- R – Relevant
- T – Timely

Objective-Based Penetration Test

An objective-based test focuses on the overall security of the organization and its data security. When people think of a penetration test, this is often what they think of. The scope of work and rules of engagement documents specify what is to be tested.

Compliance-Based Penetration Test

Ensuring that the organization is in compliance with federal laws and regulations is a major purpose for performing a penetration test. Some of the main laws and regulations include the following:

Regulation	Description
------------	-------------

Payment Card Industry Data Security Standards (PCI-DSS)	Defines the security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and other types of payment cards.
Health Insurance Portability and Accountability Act (HIPAA)	A set of standards that ensures a person's health information is kept safe and only shared with the patient and medical professionals that need it.
ISO/IEC 27001	Defines the processes and requirements for an organization's information security management systems.
Sarbanes Oxley Act (SOX)	A law enacted in 2002 with the goal of implementing accounting and disclosure requirements that would increase transparency in corporate governance and financial reporting and formalizing a system of internal checks and balances.
Digital Millennium Copyright Act (DMCA)	Enacted in 1998, this law is designed to protect copyrighted works.
Federal Information Security Management Act (FISMA)	Defines how federal government data, operations, and assets are handled.

Special Considerations

There are a few scenarios where extra or special considerations need to be considered, such as mergers and establishing supply chains. During a merger, a penetration test may be performed to assess physical security, data security, company culture, or other facets of an organization to determine if there are any shortcomings that may hinder or cancel the merger. When establishing a supply chain, a penetration test needs to be performed to determine if there are any security issues or violations that could affect everyone involved. The organizations need to ensure that their systems can talk to each other and their security measures align. For these tests, companies may employ red teams and blue teams. They may also utilize purple team members.

2.5.4 Legal and Ethical Compliance Facts

An ethical hacker's role is to break the rules and hack into an organization's network and systems. Before this is done, both the penetration tester and organization must know and agree to everything being done. Once the scope of work is finalized, there may be additional laws that need to be looked at and followed.

This lesson covers the following topics:

- Federal laws
- Cloud-based and third-party systems
- Ethical scenarios
- Corporate policies

Federal Laws

There are two key federal laws that apply to hacking: Title 18, Chapter 47, Sections 1029 and 1030. One thing that stands out in these laws is in most of the statements, the words unauthorized or exceeds authorized access are used. These keywords are what apply to the ethical hacker. The ethical hacker needs to ensure they access only the systems to which they have explicit permission and only to the level they have authorized access.

- Section 1029 refers to fraud and related activity with access devices. An access device is any application or hardware that is created specifically to generate access credentials.
- Section 1030 refers to fraud and related activity with computers or any other device that connects to a network.

In addition to the above two laws, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies was amended in 2013 to include intrusion software. This agreement is between 41 countries that generally hold similar views on human rights. The update in 2013 has led to a lot of issues and confusion in the cybersecurity field, as many of the tools used in the penetration testing process can also be used by black hat hackers for malicious purposes.

In 2018, the Wassenaar Arrangement was updated to clarify some of these policies. This will hopefully make things easier for some penetration testers involved in international testing.

Cloud-Based and Third-Party Systems

When dealing with cloud-based systems or other third-party systems, special considerations need to be made. If an organization is using a cloud-based system, that means the organization doesn't own the system and cannot legally provide permission for a penetration test to be carried out on that system. The penetration tester must make sure to get the explicit permission from the cloud provider before performing any tests.

Third-party systems can also cause some issues for the penetration tester. If systems are interconnected, such as in a supply chain, the penetration tester needs to ensure they do not accidentally access the third party's systems at all. The penetration tester may also run across vulnerabilities that can affect the third party. In this scenario, the penetration tester needs to report findings to the client and let the client handle the reporting.

Ethical Scenarios

Aside from the laws and regulations, the ethical hacker must be aware of scenarios where ethical decisions need to be made. One particular instance that can cause an issue is when the penetration tester resides in one state and the organization is in another state. The laws that govern computer usage and hacking can vary from state to state. When this occurs, the penetration tester and the organization need to agree on which set of laws they will adhere to. Whenever there are any questions or concerns regarding laws and regulations, a lawyer should be consulted.

There will be instances where the ethical hacker will run across data and may not be sure what to do with it. There are instances, such as child pornography, that is considered a mandated report - these sorts of findings must always be immediately reported, no exceptions. In any other situation where data is discovered that is not a **mandated report**, the data should be disclosed to the client. As always, when there is doubt about which course of action to take, a lawyer should be consulted.

Corporate Policies

Corporate policies also play a role in how a penetration test is carried out. Corporate policies are the rules and regulations that have been defined and put in place by the organization. As part of the risk assessment and penetration test, these policies should be reviewed and tested. Some common policies that most organizations have defined are password policies, update frequency, handling sensitive data, and bring your own devices. The organization needs to determine which, if any, of these policies will be tested during an assessment.

2.5.6 Engagement Contract Facts

2.5.6 Engagement Contract Facts






Before a penetration test can begin, there are a few key documents that must be completed and agreed on. These documents are designed to protect both the organization and the penetration tester.

Even though much of this information could be put into a single document, it makes things much clearer when all the details are separated out into the documents described in this table.





Document	Description
Scope of Work	<p>The Scope of Work is one of the more detailed documents for a project. This document spells out in detail the who, what, when, where, and why of the penetration test. Explicitly stated in the Scope of Work are details of all system aspects that can be tested, such as IP ranges, servers, and applications.</p> <p>Anything not listed is off-limits to the ethical hacker. Off-limit features should also be explicitly stated in the Scope of Work document to avoid any confusion. This document will also define the test's time frame, purpose, and any special considerations.</p>
Rules of Engagement	<p>The Rules of Engagement document defines how the penetration test will be carried out. This document defines whether the test will be a white box, gray box, or black box test. Other details, such as how to handle sensitive data and who to notify in case something goes wrong, will be listed in the document.</p>
Master Service Agreement	<p>It is very common for companies to do business with each other multiple times. In these situations, a Master Service Agreement is useful. This document spells out many of the terms that are commonly used between the two companies, such as payment. This makes future contracts much easier to complete, as most details are already spelled out.</p>
Non-Disclosure Agreement	<p>This is a common legal contract outlining confidential material or information that will be shared during the assessment and the restrictions placed on it. This contract basically states that anything the tester finds cannot be shared, with the exception of those people stated in the document.</p>
Permission to Test	<p>This document is often referred to as the get-out-of-jail-free card. Since most people in the client's organization will not know about the penetration test occurring, this document is used if the penetration tester gets caught. This document is used only as a last resort but explains what the penetration tester is doing and that the work is fully authorized.</p>

3. Social Engineering and Physical Security





3.1 Social Engineering

- ✓  3.1.1 Social Engineering Overview
- ✓  3.1.2 Social Engineering Overview Facts
- ✓  3.1.3 Social Engineering Motivation
- ✓  3.1.4 Social Engineering Motivation Facts
- ✓  3.1.5 Social Engineering Techniques
- ✓  3.1.6 Social Engineering Technique Facts
- ✓  3.1.7 Phishing and Internet-Based Techniques
- ✓  3.1.8 Phishing and Internet-Based Technique Facts
- ✓  3.1.9 Use the Social Engineer Toolkit
- ✓  3.1.10 Identify Social Engineering
- ✓  3.1.11 Practice Questions

3.2 Physical Security

- ✓  3.2.1 Physical Security Overview
- ✓  3.2.2 Physical Security Facts
- ✓  3.2.3 Physical Security Attacks
- ✓  3.2.4 Physical Security Attack Facts
- ✓  3.2.5 Practice Questions

3.3 Countermeasures and Prevention

- ✓  3.3.1 Countermeasures and Prevention
- ✓  3.3.2 Countermeasures and Prevention Facts
-  3.3.3 Implement Physical Security Countermeasures
- ✓  3.3.4 Practice Questions

3.1.2 Social Engineering Overview Facts

3.1.2 Social Engineering Overview Facts

Social engineering refers to enticing or manipulating people to perform tasks or relay information that benefits an attacker. Social engineering tries to get a person to do something the person wouldn't do under normal circumstances.

This lesson covers the following topics:

- Manipulation tactics
- Social engineering process

Manipulation Tactics

Social engineers are master manipulators. The following table describes some of the most popular tactics they use on targets.

Manipulation Type	Description
Moral obligation	An attacker uses moral obligation to exploit the target's willingness to be helpful and assist them out of a sense of responsibility.
Innate human trust	Attackers often exploit a target's natural tendency to trust others. The attacker wears the right clothes, has the right demeanor, and speaks words and terms the target is familiar with so that the target will comply with requests out of trust.
Threatening	An attacker threatens when they intimidate a target with threats convincing enough to make them comply with the attacker's request.
Offering something for very little to nothing	Offering something for very little to nothing refers to an attacker promising huge rewards if the target is willing to do a very small favor or share what the target thinks is a very trivial piece of information.
Ignorance	Ignorance means the target is not educated in social engineering tactics and prevention, so the target can't recognize social engineering when it is happening. The attacker knows this and exploits the ignorance to his or her advantage.

Social Engineering Process

The social engineering process can be divided into three main phases: **research**, **development**, and **exploitation**. The following table describes each phase.

Phase	Description
Research	<p>In the research phase, the attacker gathers information about the target organization. Attackers use a process called Footprinting, which is using all resources available to gain information, including going through the target organization's official websites and social media; performing dumpster diving; searching sources for employees' names, email addresses, and IDs; going through an organization tour; and other kinds of onsite observation.</p> <p>Research may provide information for pretexting. Pretexting is using a fictitious scenario to persuade someone to perform an unauthorized action such as providing server names and login information. Pretexting usually requires the attacker to perform research to create a believable scenario. The</p>

	more the attacker knows about the organization and the target, the more believable a scenario the attacker can come up with.
Development	The development phase involves two parts: selecting individual targets within the organization being attacked and forming a relationship with the selected targets. Usually, attackers select people who not only will have access to the information or object they desire, but that also show signs of being frustrated, overconfident, arrogant, or somehow easy to extract information from. Once the targets are selected, the attacker will start forming a relationship with them through conversations, emails, shared interests, and so on. The relationship helps build the targets' trust in the attacker, allowing the target to be comfortable, relaxed, and more willing to help.
Exploitation	<p>In the exploitation phase, the attacker takes advantage of the relationship with the target and uses the target to extract information, obtain access, or accomplish the attacker's purposes in some way. Some examples include disclosing password and username; introducing the attacker to other personnel, providing social credibility for the attacker; inserting a USB flash drive with a malicious payload into a organization's computer; opening an infected email attachment; and exposing trade secrets in a discussion.</p> <p>If the exploitation is successful, the only thing left to do is to wrap things up without raising suspicion. Most attackers tie up loose ends, such as erasing digital footprints and ensuring no items or information are left behind for the target to determine that an attack has taken place or identify the attacker. A well-planned and smooth exit strategy is the attacker's goal and final act in the exploitation phase.</p>

3.1.4 Social Engineering Motivation Facts

3.1.4 Social Engineering Motivation Facts

There are many different social engineering techniques, attackers, and types of motivation techniques.

This lesson covers the following topics:

- Social engineering attacks
- Types of attackers
- Types of motivation techniques

Social Engineering Attacks

The following table describes a few social engineering attacks.

Attack	Description
Shoulder surfing	Shoulder surfing involves looking over someone's shoulder while they work on a computer or review documents. This attack's purpose is to obtain usernames, passwords, account numbers, or other sensitive information.
Eavesdropping	Eavesdropping is an unauthorized person listening to private conversations between employees or other authorized personnel when sensitive topics are being discussed.
USB and keyloggers	When on site, a social engineer also has the ability to stealing data through a USB flash drive or a keystroke logger. Social engineers often employ keystroke loggers to capture usernames and passwords. As the target logs in, the username and password are saved. Later, the attacker uses the username and password to conduct an exploit.
Spam and spim	When using spam, the attacker sends an email or banner ad embedded with a compromised URL that entices a user to click it. Spim is similar, but the malicious link is sent to the target using instant messaging instead of email.
Hoax	Email hoaxes are often easy to spot because of their bad spelling and terrible grammar. However, hoax emails use a variety of tactics to convince the target they're real.

Types of Attackers

The following table describes different types of attackers.

Type	Description
Insider	<p>An insider could be a customer, a janitor, or even a security guard. But most of the time, it's an employee. Employees pose one of the biggest threats to any organization. There are many reasons why an employee might become a threat. The employee could:</p> <ul style="list-style-type: none"> • Be motivated by a personal vendetta because they are disgruntled. • Want to make money.

	<ul style="list-style-type: none"> • Be bribed into stealing information. <p>Sometimes, an employee can become a threat actor without even realizing it. This is known as an unintentional threat actor. The employee may create security breaches doing what seems to be harmless day-to-day work. An unintentional threat actor is the most common insider threat.</p>
Hacker	<p>Generally speaking, a hacker is any threat actor who uses technical knowledge to bypass security, exploit a vulnerability, and gain access to protected information. Hackers could attack for several different reasons. Some types of hackers are:</p> <ul style="list-style-type: none"> • Those motivated by bragging rights, attention, and the thrill. • Hacktivists with a political motive. • Script kiddies, who use applications or scripts written by much more talented individuals. • A white hat hacker, who tries to help a company see the vulnerabilities that exist in their security. • Cybercriminals, who are motivated by significant financial gain. They typically take more risks and use extreme tactics. Corporate spies are a sub-category of cybercriminal.
Nation state	<p>Attacks from nation states have several key components that make them especially powerful. Typically, nation state attacks:</p> <ul style="list-style-type: none"> • Are highly targeted. • Identify a target and wage an all-out war. • Are extremely motivated. • Use the most sophisticated attack techniques of all the attackers. This often includes developing completely new applications and viruses in order to carry out an attack. • Are well financed.

Types of Motivation Techniques

The following table describes types of techniques a social engineer uses to motivate an employee to provide information.

Technique	Description
Authority and fear	Authority techniques rely on power to get a target to comply without questioning the attacker. The attacker pretends to be a superior with enough power that the target will comply right away without question.

	The attacker could also pretend to be there in the name of or upon the request of a superior. Authority is often combined with fear. If an authority figure threatens a target with being fired or demoted, the target is more likely to comply without a second thought.
Social proof	Social proof means the attacker uses social pressure to convince the target that it's okay to share or do something. In this case, the attacker might say, "If everybody is doing it, then it's okay for you to do it, too."
Scarcity	Scarcity appeals to the target's greed. If something is in short supply and will not be available, the target is more likely to fall for it.
Likeability	Likeability works well because humans tend to do more to please a person they like as opposed to a person they don't like.
Urgency	To create a sense of urgency, an attacker fabricates a scenario of distress to convince an individual that action is immediately necessary.
Common ground and shared interest	Common ground and shared interest work because sharing a hobby, life experience, or problem instantly builds a connection and starts forming trust between two parties.

3.1.6 Social Engineering Techniques Facts

3.1.6 Social Engineering Technique Facts

Not all attackers are the same. They all have different motives, attributes, and attack characteristics. Hackers may also employ several different techniques to obtain what they want from the target.

This lesson covers the following topics:

- Attack types
- Elicitation
- Pretexting, preloading, and impersonation
- Interview and interrogation

Attack Types

A single hacker trying to exploit a vulnerability is going to have a completely different attack profile than an organized crime group waging an assault on your network. The following table describes the differences between the two.

Attack	Description
Opportunistic	An opportunistic attack is typically automated and involves scanning a wide range of systems for known vulnerabilities, such as old software, exposed ports, poorly secured networks, and default configurations. When one is found, the hacker will exploit the vulnerability, steal whatever is easy to obtain, and get out.
Targeted	A targeted attack is much more dangerous. A targeted attack is extremely methodical and is often carried out by multiple entities that have substantial resources. Targeted attacks almost always use unknown exploits, and the hackers go to great lengths to cover their tracks and hide their presence. Targeted attacks often use completely new programs that are specifically designed for the target.

Elicitation

Elicitation is a technique that tries to extract information from a target without arousing suspicion. The following table describes some elicitation tactics.

Tactic	Description
Compliments	Attackers may give a target a compliment about something they know the target did in hopes that the target will take the bait and elaborate on the subject. Even if the target downplays the skill or ability involved, talking about it might give the attacker valuable information.
Misinformation	Attackers might make a statement with the wrong details. The attacker's intent is that the target will give the accurate details that the attacker wanted to confirm. The more precise the details given by the attacker, the better the chance that the target will take the bait.
Feigning ignorance	Attackers might make a wrong statement and then admit to not knowing much about the subject. This statement will hopefully get the target to not only correct the attacker, but also explain why the attacker is wrong in detail. The explanation might help the attacker learn, or at least have a chance to ask questions without looking suspicious.

Being a good listener	An attacker may approach a target and carefully listen to what the target has to say, validate any feelings they express, and share similar experiences (which may be real or fabricated). The point is to be relatable and sympathetic. As the target feels more connected to the attacker, barriers go down and trust builds, leading the target to share more information.
-----------------------	---

Pretexting, Preloading, and Impersonation

All the social engineering techniques involve some pretexting, preloading, and impersonation. The following table describes these steps.

Step	Description
Pretexting	Pretexting is doing research and information gathering to create convincing identities, stories, and scenarios to be used on selected targets.
Preloading	Preloading is used to set up a target by influencing the target's thoughts, opinions, and emotions.
Impersonation	Impersonation is pretending to be trustworthy and having a legitimate reason for approaching the target to ask for sensitive information or access to protected systems.

Interview and Interrogation









Another technique social engineers use often is the concept of interviews and interrogation. The following table describes some of the most important aspects of conducting a successful interview and interrogation.

Concept	Description
Interview vs interrogation	In the interview phase, the attacker lets the target do the talking while the attacker mostly listens. In this way, the attacker has the chance to learn more about the target and how to extract information from them. Then the attacker leads the interview phase into an interrogation phase. It's most effective when done smoothly and naturally and when the target already feels a connection and trust with the attacker. In the interrogation phase, the attacker talks about the target's statements. At this point, the attacker is mostly leading the conversation with questions and statements that will flow in the direction the attacker has in mind to obtain information.











Environment	<p>The environment the attacker chooses for conducting an interview and interrogation is essential to setting the mood. The location should not be overly noisy or overly crowded. It should be a relaxing and stress-free environment that puts the target at ease. The attacker shouldn't sit between the target and the door. The target should never feel trapped in any way. Lighting should be good enough for both parties to see each other clearly. This will allow the attacker to better read the target's micro expressions and movements. It will also inspire trust in the target.</p>
Observation	<p>During these interviews and interrogations, the hacker pays attention to every change the target displays. This allows the attacker to discern the target's thoughts and topics that should be investigated further. Every part of the human body can give a clue about what is going on inside the mind. Most people don't even realize they give many physical cues, nor do they recognize these cues in others. A skilled observer pays close attention and puts these clues together to confirm another person's thoughts and feelings.</p>

4. Reconnaissance

4.1 Reconnaissance Overview

- ✓  4.1.1 Reconnaissance Processes
- ✓  4.1.2 Reconnaissance Process Facts
- ✓  4.1.3 Reconnaissance Tool Facts
- ✓  4.1.4 Google Hacking for Office Documents
- ✓  4.1.5 Perform Reconnaissance with theHarvester
- ✓  4.1.6 Perform Reconnaissance with Nmap
- ✓  4.1.7 Perform Reconnaissance with Nmap
- ✓  4.1.8 Practice Questions

4.2 Reconnaissance Countermeasures

-  4.2.1 Reconnaissance Countermeasures
- ✓  4.2.2 View Windows Services
- ✓  4.2.3 Disable Windows Services
- ✓  4.2.4 View Linux Services
- ✓  4.2.5 Manage Linux Services
- ✓  4.2.6 Enable and Disable Linux Services
- ✓  4.2.7 Reconnaissance Countermeasure Facts
- ✓  4.2.8 Disable IIS Banner Broadcasting
- ✓  4.2.9 Hide the IIS Banner Broadcast
- ✓  4.2.10 Practice Questions

ExamTopics Review Questions

The end!