Week 3: Penetration Testing and hackers techniques

Ayman El Hajjar

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

6COSC002W - Security and Forensics

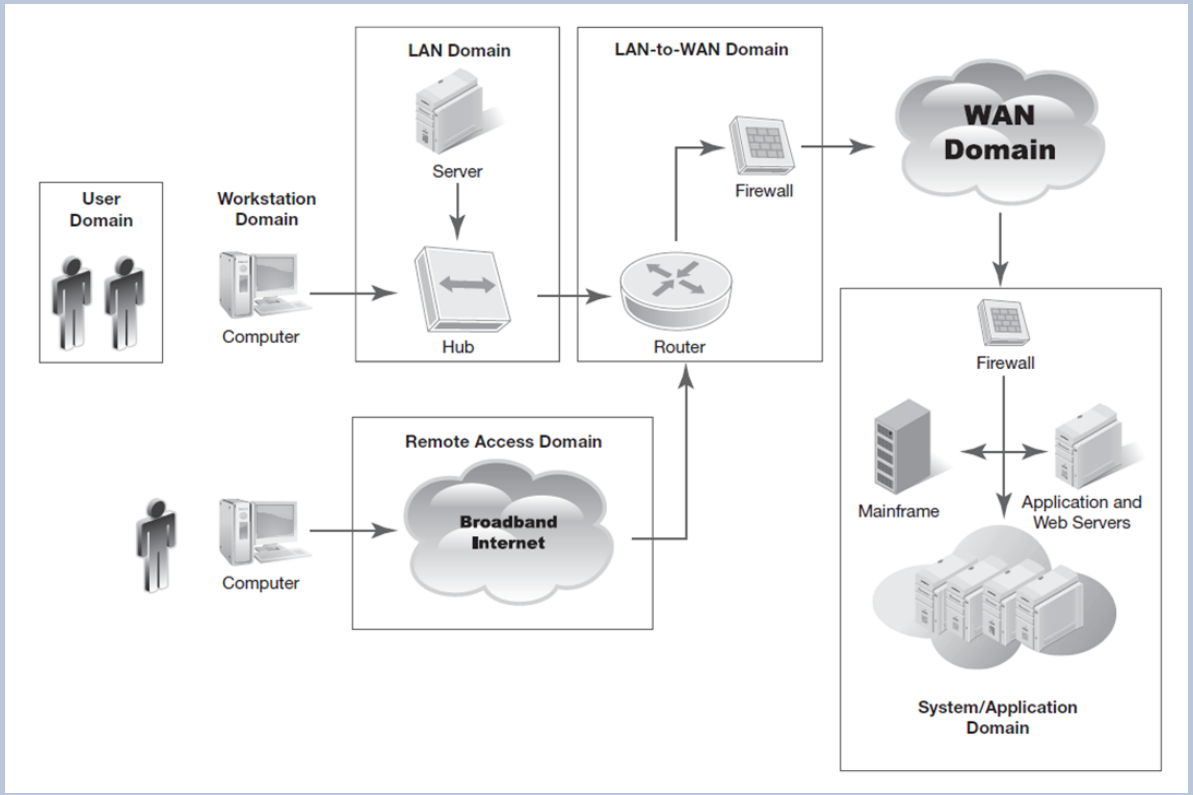
01 February 2020

University of Westminster

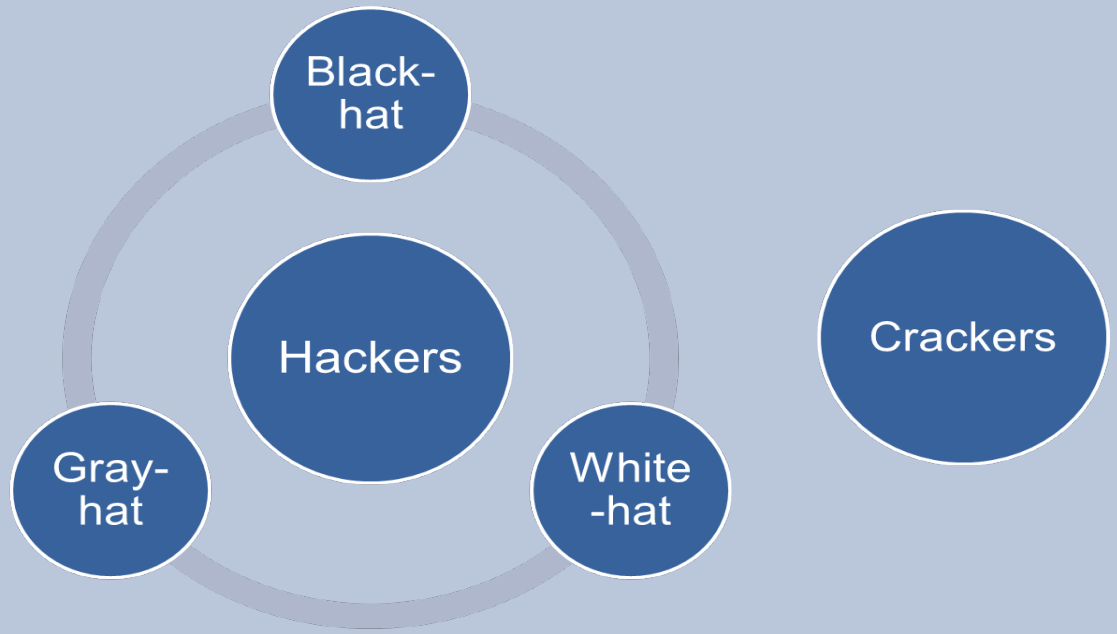
Session Overview

What Are You Trying to Protect?

What Are You Trying to Protect?



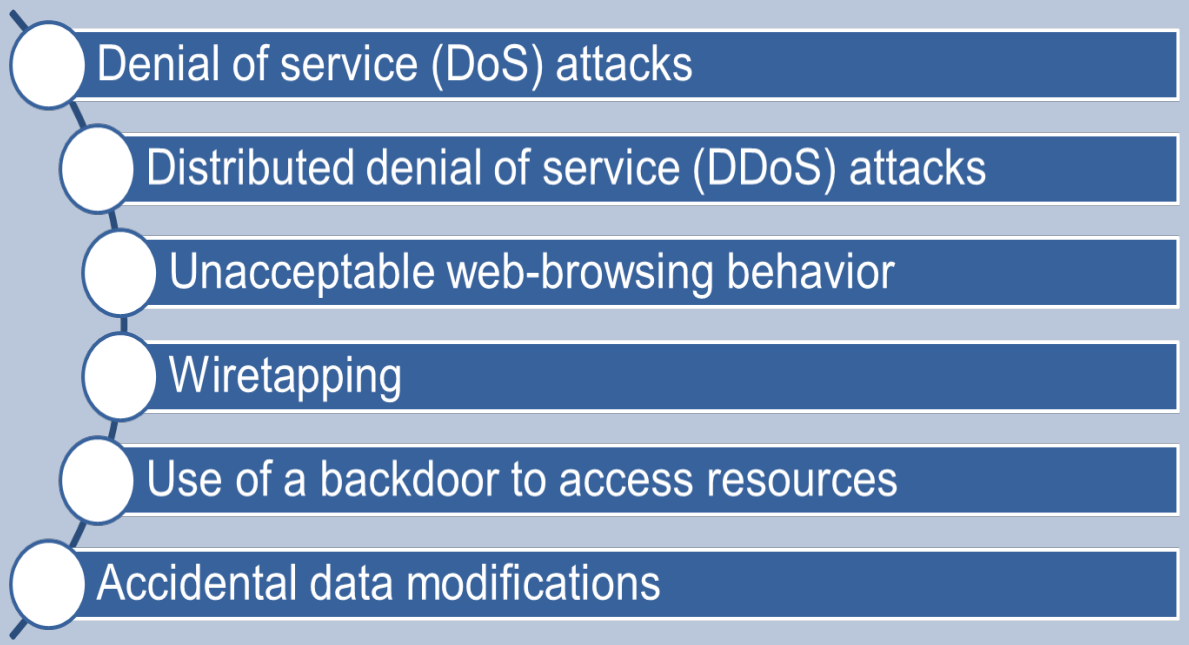
Whom Are You Trying to Catch?



What Is a Security Breach?

- Any event that results in a violation of any of the C-I-A security tenets
- Some security breaches disrupt system services on purpose
- Some are accidental and may result from hardware or software failures

Activities that Cause Security Breaches



Penetration testing- An introduction

Penetration testing- An introduction

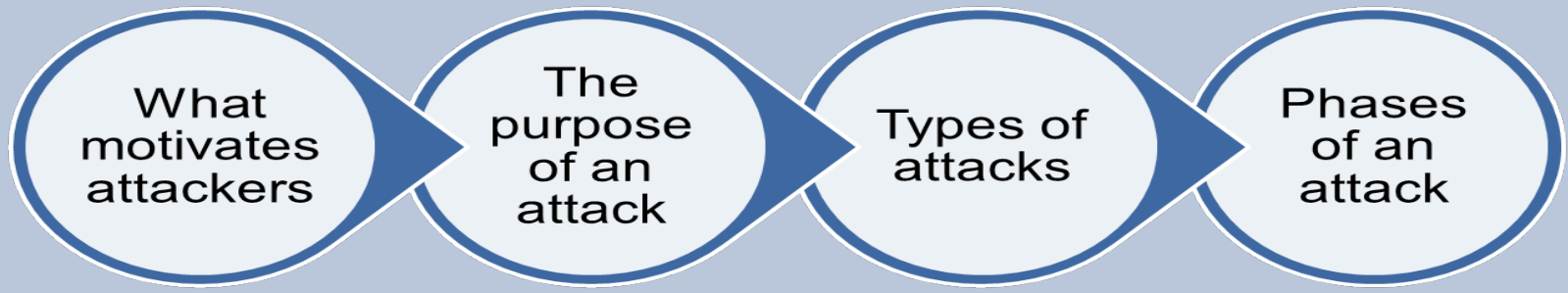
A "simulated attack" with a predetermined goal that has to be obtained within a fixed time

- **Penetration testing** is to test the security of systems and architectures from the point of view of an attacker (hacker, cracker)

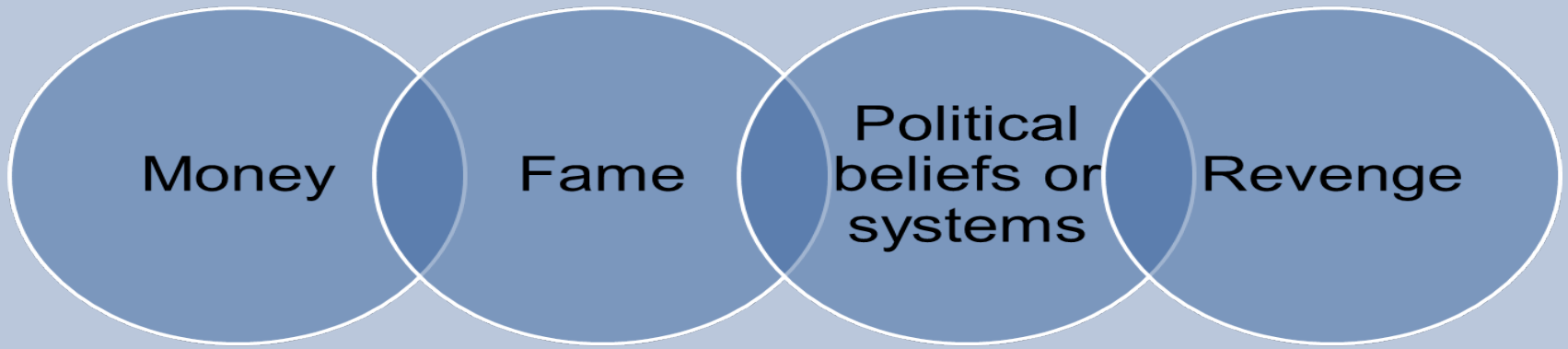
Preparing for a cyber attack / Penetration testing

- To protect your organization from a cyber attack, it's important to understand how an attacker goes about stealing sensitive information.
- Typically, attacks happen in five distinct stages:
  - Reconnaissance
  - Incursion and scanning
  - Discovery
  - Capture
  - Exfiltration
- Each stage uses different tools and techniques.
- In this module, we will be looking at those stages and look at tools to proect your orgnization and ultimately prevent the cybercriminal from achieving their goal.

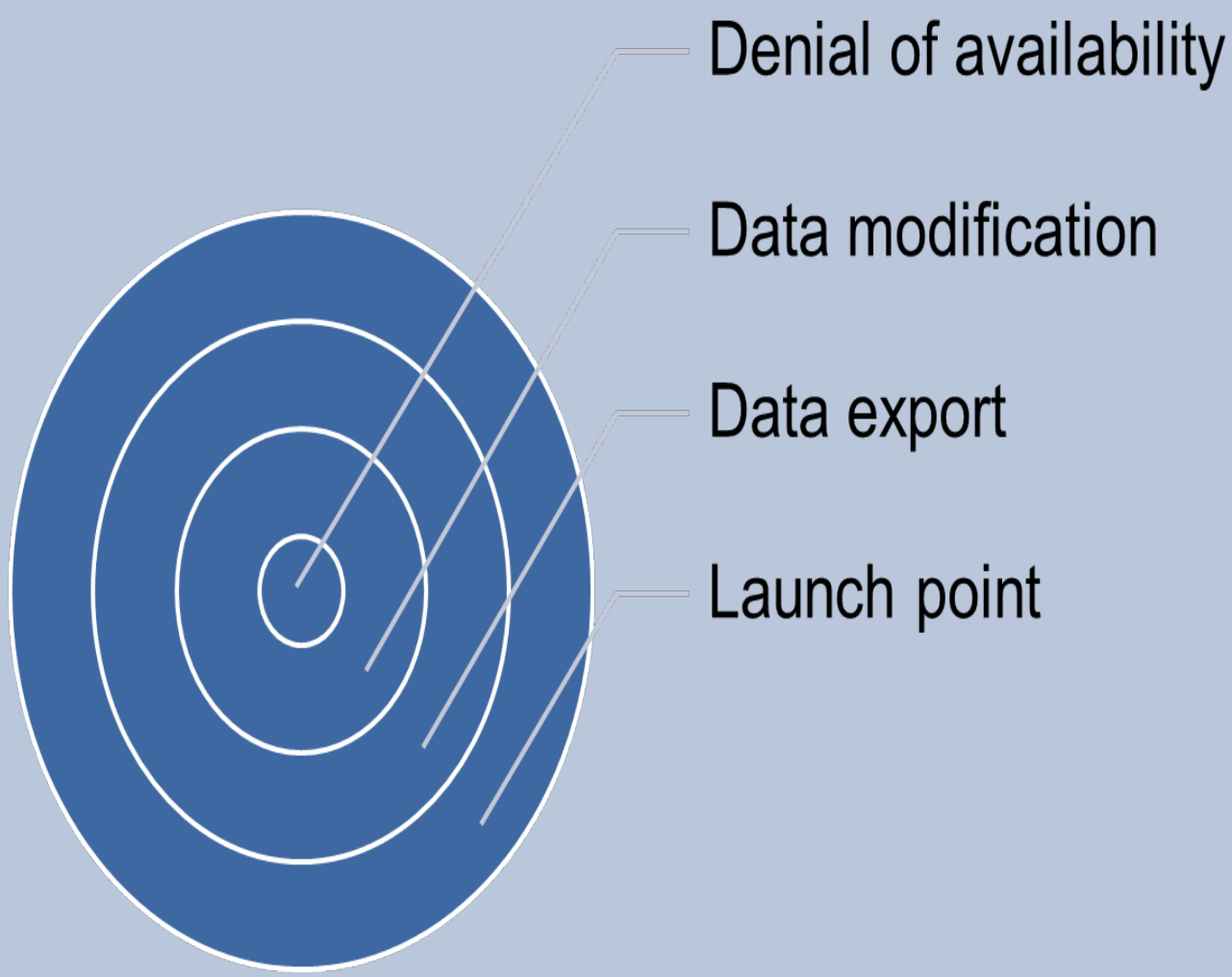
Anatomy of an Attack



What Motivates Attackers?



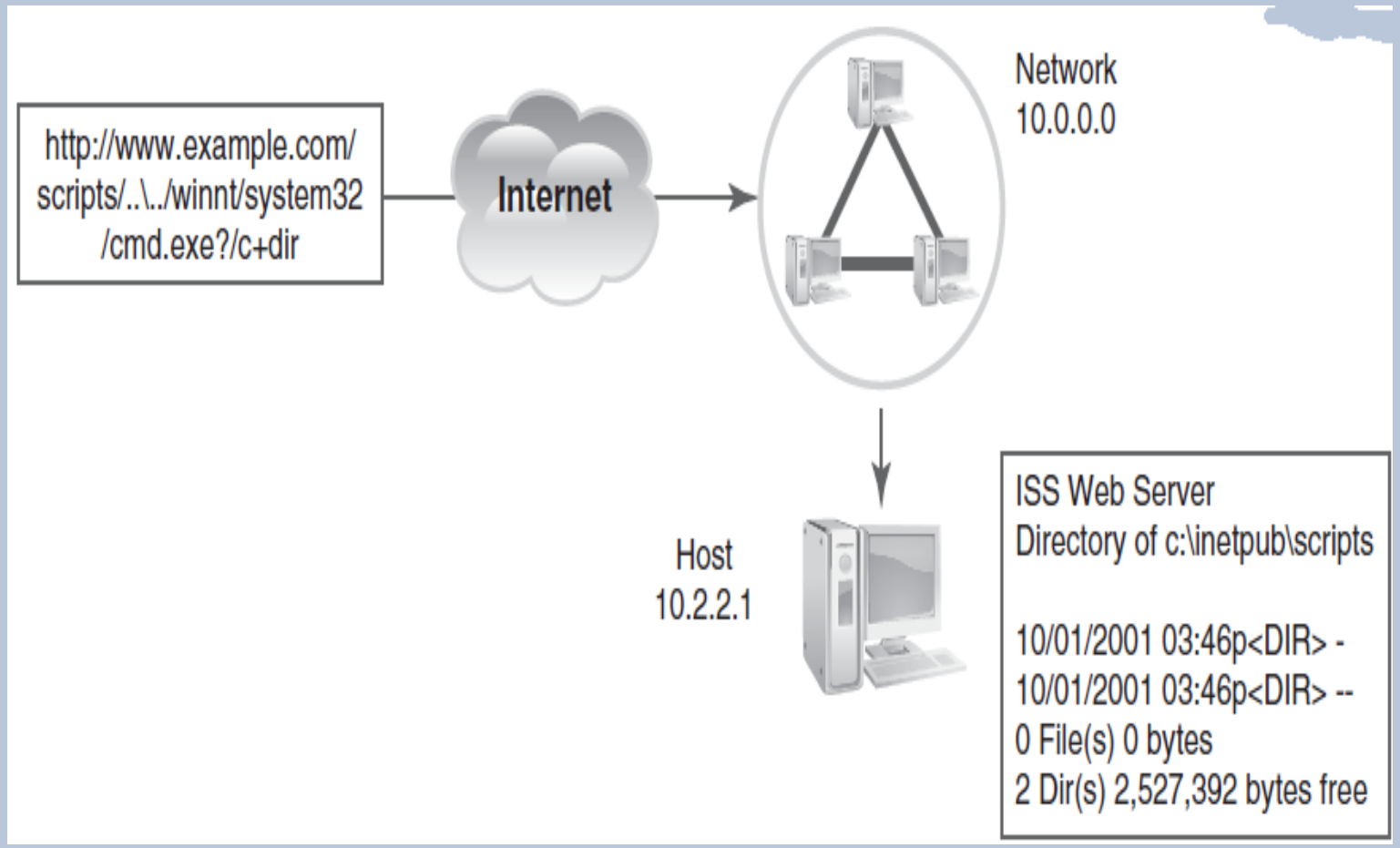
The Purpose of an Attack



Types of Attacks

- Unstructured attacks
- Structured attacks
- Direct attacks
- Indirect attacks

How a Direct Attack Works



Phases of an attack

- Reconnaisance
  - Attackers leverage information from a variety of factors to understand their target including identifying vulnerable servers, insecure applications, or unpatched systems that can be compromised.
- Scanning or probing
  - Once the target is identified, the next step is to identify a weak point that allows the attackers to gain access.
  - This is usually accomplished by scanning an organization's network - with tools easily found on the Internet - to find entry points.
  - This step of the process usually goes slowly, sometimes lasting months, as the attackers search for vulnerabilities.
- Incursion
  - Attackers break into the network, delivering targeted malware to vulnerable systems and people, often without the user being

Access and Escalation

- Capture
  - With access to the network, attackers stay "low and slow" to avoid detection.
  - They then map the organization's defenses from the inside and create a battle plan for information they intend to target.
- Escalate
  - Now that weaknesses in the target network are identified, the next step in the cyber attack is to gain access and then escalate.
  - In almost all such cases, privileged access is needed because it allows the attackers to move freely within the environment.
  - Once the attackers gain elevated privileges, the network is effectively taken over and is now "owned" by the intruders.

Why Pentesting

- Mitigate risk
- Legal and compliance
- Validate/Invalidate Security Controls
- Find and Mitigate Vulnerabilities
- Prevent compromise

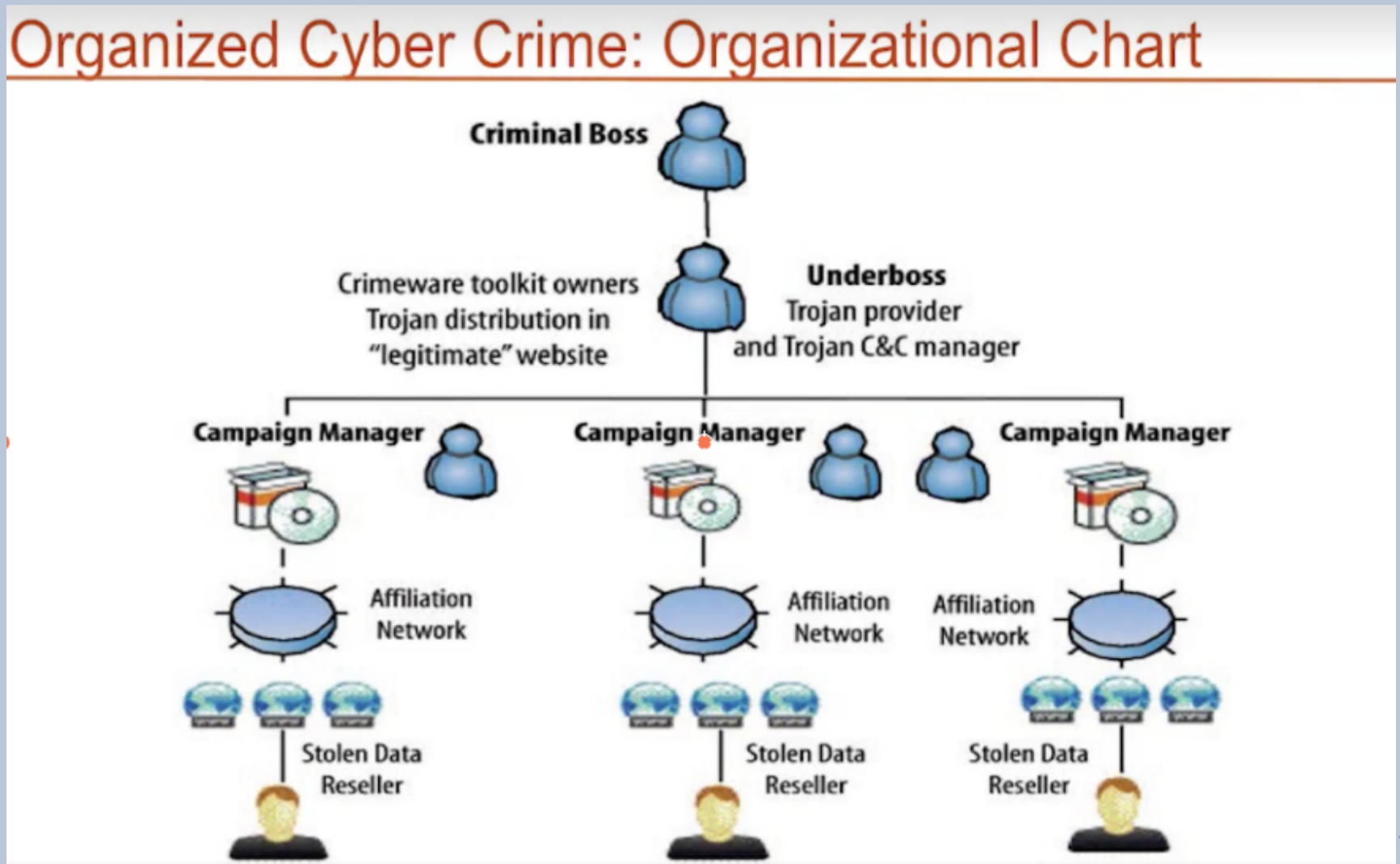
Types of Pentests

- **Black box** treats the system as a "black-box", so it doesn't explicitly use knowledge of the internal structure
- **White box** allows one to peek inside the "box", and it focuses specifically on using internal knowledge of the software to guide the selection of test data

Attacks Motives

- But why would anyone attempt to disrupt or break networks? What coudld the motives be?
  - **Casual snooping** - Inquisitive crackers who look around seeing what they can find, without any of the following motives
  - **Disruption** - preventing or inhibiting legitimate users from use of the system
  - **Espionage** - attempting to extract information from a system (perhaps commercial information).
  - **Use of resources** - once compromised, a system or network can be used to launch attacks on other networks.
  - **Making a statement** - social, political, anarchistic etc.
- There are other motives... These are examples

Attacks Motives



Types of Intruders/Hackers

- **Amateurs**
  - People who steal resources for their own uses
  - Not very sophisticated
- **Crackers**
  - Access resources without permission
  - Typically for fun, but maybe other reasons
- **Career criminal**
  - Well-planned attacks
  - Usually for financial gain
- **Military**
  - Done to disable opposing forces
  - Gain strategic advantage

Types of Intruders/Hackers

- **blackhat**
  - Black hat hackers usually have extensive knowledge about breaking into computer networks and bypassing security protocols.
  - Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime.
- **whitehat**
  - White hat hackers choose to use their powers for good rather than evil. They are also known as "ethical hackers".
  - White hat hackers employ the same methods of hacking as black hats, with one exception- they do it with permission from the owner of the system first.

Types of Intruders/Hackers

- **Hackers**
  - Hackers are those who build and create.
  - They learn and discover different computer systems, networks and often have previous experience in programming which only adds to their extensive knowledge. They build secure environments.
  - Most hackers are usually white hat hackers
- **Crackers**
  - A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system.
  - All crackers are black hat hackers.

Reconnaisance: Information gathering

- It has been said that no information is irrelevant. Those words ring true when it comes to information gathering for hacking purposes.
- Even the slightest detail can lead to a successful social engineering breach.
- Attackers leverage information from a variety of factors to understand their target including identifying vulnerable servers, insecure applications, or unpatched systems that can be compromised.

Social Engineering

What is social engineering

- "Social engineering is lying to people to get information."
- "Social engineering is being a good actor."
- "Social engineering is knowing how to get stuff for free."

- Webster's Dictionary defines social as "of or pertaining to the life, welfare, and relations of human beings in a community."
- It also defines engineering as "the art or science of making practical application of the knowledge of pure sciences, as physics or chemistry, as in the construction of engines, bridges, buildings, mines, ships, and chemical plants or skillful or artful contrivance; manoeuvring."

Social Engineering

- The Different Types of Social Engineers
  - Hackers
  - Penetration testers
  - Spies
  - Identity thieves
  - Scam artist
  - Salespeople
  - Governments
  - Doctors, psychologists, and lawyers and others

Stamps collection

- Sarah Jones, a professional pentester for more than a decade, tells this story
- She was tasked with gaining access to a company that had an almost nonexistent footprint on the Web.
- In one of her searches she found a high-ranking company official who used his corporate email on a forum about stamp collecting and who expressed an interest in stamps from the 1950s.
- Sarah quickly registered a URL and created a website to show her collection

Email craft

Dear Sir, I saw on www.forum.com you are interested in stamps from the 1950s. Recently my grandfather passed away and left me with a stamp collection that I would like to sell. I have a website set up; if you would like to see it please visit www.stampcollection.com. Thanks, Sarah

Stamps collection

- She took the office number from the forum post and placed a phone call to the man about showing his the stamps collection she have just inherited.
- The target was very eager to see this collection and asked her to send him the link by email.
- Sarah sent the email and waited for him to click the link.
- What Sarah did was embed a malicious frame on the website. This frame had code in it that would exploit a vulnerability then known in the popular Internet Explorer browser and give control over the target's computer to Sarah.
- The wait was not long: as soon as the man received the email clicked the link and the company's perimeter was compromised.

Social Engineering

- With that knowledge in mind, here are questions that come up with regard to information gathering:
  - How can you gather information?
  - What sources exist for social engineers to gather information?
  - What can you glean from this information to profile your targets?
  - How can you locate, store, and catalog all this information for the easiest level of use?

Sources for Information Gathering

1. Gathering Information from Websites: it can reveal many information depending on how much footprint the organization/person has online. Information can be:
   - What they do
   - The products and services they provide
   - Physical locations
   - Job openings
   - Contact numbers
   - Email naming conventions
   - Special words or phrases that can help in password profiling
2. **Whois** is a name for a service and a database.
   - Whois can lead you to surprisingly specific results like such as a person's email address, telephone number, or even DNS server IP address.

Sources for Information Gathering (Cont.)

3. Public Servers
   - A company's publicly reachable servers are also great sources for what its websites don't say.
   - Fingerprinting a server for its OS, installed applications, and IP information can say a great deal about a company's infrastructure.
   - IP addresses may tell you whether the servers are hosted locally or with a provider; with DNS records you can determine server names and functions, as well as IPs.
   - **NOTE:** In 2007 and 2008, England, France, and Germany passed laws that make unlawful the creation, distribution, and possession of materials that allow someone to break any computer law. Port scanners fall under this description.

Sources for Information Gathering (Cont.)

4. Social Media
   - Many companies have recently embraced social media. It's cheap marketing that touches a large number of potential customers.
   - It's also another stream of information from a company that can provide breadcrumbs of viable information. Companies publish news on events, new products, press releases, and stories that may relate them to current events.
5. Public reports
   - Public data may be generated by entities inside and outside the target company.
   - This data can consist of quarterly reports, government reports, analyst reports, earnings posted for publicly traded companies, and so on.

Sources for Information Gathering (Cont.)

6. Using the Power of Observation
   - Though not used enough as a social engineering tool, simple observation can tell you much about your target.
   - Does the target's employees use keys, RFID cards, or other methods to enter the building?

Sources for Information Gathering (Cont.)

7. Using Profiling Software
   - Password profilers such as Common User Passwords Profiler (CUPP) and Who's Your Daddy (WYD) can help a social engineer profile the potential passwords a company or person may use.
   - A tool like WYD will scrape a person or company's website and create a password list from the words mentioned on that site. It is not uncommon for people to use words, names, or dates as passwords. These types of software make it easy to create lists to try.

Elicitation

- Elicitation means to bring or draw out, or to arrive at a conclusion (truth, for instance) by logic.
- Alternatively, it is defined as a stimulation that calls up (or draws forth) a particular class of behaviors, as in "the elicitation of his testimony was not easy."

NSA definition

the National Security Agency of the United States government defines elicitation as "the subtle extraction of information during an apparently normal and innocent conversation."

- These conversations can occur anywhere that the target is; a restaurant, the gym, a daycare or anywhere.
- Elicitation works well because it is low risk and often very hard to detect.

Pretexting: How to Become Anyone

A good liar...

Honesty is the key to a relationship. If you can fake that, you're in.
––RICHARD JENI

- **What is pretexting?** Some people say it is just a story or lie during a **social engineering** engagement.
- Pretexting is better defined as the background story, dress, grooming, personality, and attitude that make up the character you will be for the social engineering audit.
- Pretexting encompasses everything you would imagine that person to be. The more solid and simple the pretext, the more believable you will be as a social engineer.
- Social Engineering example: Blocking you out of your account *click here for Youtube video*

Influence: The Power of Persuasion

Convince everyone...

If you would persuade, you must appeal to interest rather than intellect. —– BENJAMIN FRANKLIN

- Psychology is a science and a set of rules exists in it that, if followed, will yield a result.
- Social engineering psychology is scientific and calculated.
- Influence and persuasion are much like art that is backed up by science. Persuasion and influence involve emotions and beliefs . **You have to know how and what people are thinking.**
- Influence and the art of persuasion is the process of getting someone else to want to do, react, think, or believe in the way you want them to.

References

- The lecture notes and contents were compiled from:
  - Christopher Hadnagy, Social Engineering: The Art of Human Hacking, John Wiley & Sons, December 2010, Indianapolis, USA.