# Intro Slides

PII –

* Definition: Personally Identifiable Information
* Examples: credit cards, intellectual property (IP), passwords, etc.

Ingress Filtering –

* Definition:
  + Inbound communication only allowed from inside (such as on our routers) by default, otherwise excludes inbound communications; in the TCP 3-Way Handshake, ingress filtering on inbound communications is accomplished by blocking incoming SYN packets
  + Outbound communication is permitted from the Internet, except systems outside the network cannot get in
  + Hackers must find another way to get inside, such as: spam emails, phishing, social engineering, etc.

# Cybercrime Slides

The Computer Fraud and Abuse Act (CFAA) (1986) –

* Definition: prosecutes anyone inflicting damage to a *protected computer*, or anything that “affects interstate or foreign commerce or communications of the US”
* Penalties:
  + Felony – 10 years + fines (max); 20 years for subsequent counts
  + Misdemeanor – 1 year + fines (max); 10 years for subsequent counts
* Provisions:
  + Intentional conduct – knowingly transmitting a “program, information, code, or command” resulting in “damage” to a “protected computer”
  + Reckless conduct – knowingly causing damage to a protected computer by an outsider with unauthorized access
  + Negligent conduct – unknowingly causing damage to a protected computer by an outsider (misdemeanor charge only)
  + Threats and/or attempts also illegal

# CH1 Slides – Identifying Risks

Cybersecurity –

* Dilemma that good cybersecurity practices often inverse to a company’s goals:

1. Are costly (increases costs due to software/hardware and cybersecurity staffing)
2. Lower productivity (passwords and two-factor authentication often decrease productivity)

RMF (Risk Management Framework) Risk Assessment –

* Reasons that organizations accept security risks

1. Costs (patching security risks costs too much)
2. Convenience (it’s easier not to fix security risks)
3. Lack of awareness (you’re not actively accepting security risks, but you may be implicitly)

* Three ways to deal with risk:

1. Identify risk
2. Prioritize risk
3. Establish requirements

* We have two concerns in a risk assessment to prioritize:

1. Likelihood of a breach (what breach is most likely to happen)
2. Impact of a breach (what breach is most expensive or impactful to happen)

* We document security risks before controls to assure each requirement,
  + Has at least one control
  + Prevents controls that do not get implemented
  + Has all risks identified

Least Privilege –

* Definition: only allow access if needed
* Example: using Access Control Lists (ACLs) to manage file permissions

Isolation and mediation –

* Definition: isolating/restricting a system or process from accessing others
* Not to be confused with least privilege

Security through obscurity –

* Definition: using old technology that hackers won’t understand

Defense in Depth –

* Definition: securing several layers of defense as hurtles for hackers to overcomes
* Examples: segmenting the network (Target breach failed to do this), security awareness training for employees, patching old software, etc.

MO –

* Definition: Mode of Operation, how threat agents choose targets and operate as an organize
* Example: the hacker organization Anonymous has a typical MO of targeting government orgs

The CIA Triad –

* Definition: the CIA Triad helps to define the impact of risks
* Confidentiality
  + Definition: protecting access to data from non-authorized users accessing that information
  + Example: protecting PII (personally identifiable information) by verifying yourself after not logging in after a while
* Integrity
  + Definition: protecting data from being changed, modified, or deleted by unauthorized users
  + Example: an Access Control List (ACL) having permissions set to deny an unauthorized user from writing to a file they should only have read access to
* Availability
  + Definition: protecting access to a data for authorized users
  + Example: utilizing several off-site servers (redundancy) to host an HTTP server to prevent a focused Denial of Service (DoS) attack on one server

# CH2 Slides – Managing Risks

Vulnerabilities vs. Risks vs. Attacks –

* A risk is always going to happen (it’s a chance)
* A vulnerability is how we set something (an “asset”) up that makes an attack possible (such as a software or network)
* An attack is when a hacker exploits a vulnerability as a weak spot

CVE –

* Definition: Common Vulnerability Exposures, known/published vulnerabilities, fixable with patches (we must choose to implement patches or not, they may break our systems)
* Example: Windows XP has CVE’s that are patched in newer versions of Windows

Zero-Day Vulnerabilities –

* Definition: vulnerabilities that are unknown/unpublished (the opposite of CVE’s) thus we cannot patch them
* Example: when Target finally discovered they were breached, that was a zero-day vulnerability

# CH3 Slides – File Systems

Malware –

* Definition: malicious software that can,
  + Gather information (i.e. passwords)
  + Encrypt files (known as “ransomware”)
  + Establish persistence in a network (planting software to bypass ingress filtering)

Virus –

* Definition: type of malware that spreads to other computers through,
  + Infected flash drives/disk drives
  + Drive-by downloads
  + Worms (malware that replicates itself to spread to other computers)
  + Trojans (emails/files that seem harmless but spread the virus)

Drive-By Downloads –

* Definition: visiting a website as you pass by that asks you to install something (such as malware), problematic if you’re running your web browser in administrator

Deny by Default –

* Definition: start users with no permissions, then begin granting permissions from there, only when needed
* Deny by default is part of least privilege

# CH4 Slides – Group Permissions

Linux file permissions –

* Example: lxw-rx-r 1 maya acct file7
  + lwx are user’s (maya’s) permissions of read (‘r’) and execute (‘x’), the ‘l’ means link file type
  + rx are group (acct’s) permissions of read (‘r’) and execute (‘x’)
  + r are everyone else’s permissions of read (‘r’) only
  + The file is named ‘file7’

ACL –

* Access control list, a list of access to files or networks, says who can access what and with what permissions

~~SELinux –~~

* ~~Definition: Security Enhanced Linux, protects hackers from taking over ACLs~~

End-Point Security –

* Definition: the security of computers connected to the network (the computer systems connected to the network are the ‘endpoints’)
* Examples: firewalls, SELinux, local security policies

Log files –

* Definition: files that list all actions, allows us to investigate events on a system
* Log files are investigative (after something bad happens), whereas ACL’s are preventative (before something bad happens)
* Example: if malware was installed on the system and rebooted, we could see this history in the log files

Industry Security standards –

abide by industry standards and law.

# CH5 Slides – Digital Forensics

Digital Evidence –

* General idea: deleting data off a system doesn’t truly remove a file (it only removes the pointer to that file), items are still trackable and recoverable on disk or flash (unless it’s written over)

Digital Forensics –

* General idea: if we create an image of a disk partition, we don’t have to modify the original (thus tampering with evidence), but we have to prove the image and the original are the same by comparing their hashes

# CH6 Slides – Authentication

Multi-Factor Authentication

* Definition: requiring multiple means of authenticating that you are who you say you are (typically a password and something else)
* Authentication factors:
  + Something you know? (password or PIN)
  + Something you are? (physical location or biometrics: fingerprint, eye, face, etc. scan)
  + Something you have? (key/token on phone)
  + Keywords: know, are, have

Hashing Passwords –

* General idea: even if two passwords are exactly the same, their hashes (at least on Linux, not on Windows) will be different because they’re “salted” with an additional character

One-Way Hash Function –

* Define: a means of cryptography that scrambles and encrypts large amounts of data, protecting *data at rest* or *data in transit*, generating a fixed-size hash
* Example: hashing a password stored in RAM

Password cracking –

* General idea: the bad guys can use a few different means to obtain passwords,

1. Sniffing passwords (intercepting passwords before they’re hashed with keystroke loggers)
2. Password guessing (run a script and see if any passwords match)

Dictionary Attack –

* Definition: a common attack on passwords where hackers compare a “dictionary” (or list) of likely passwords, this “dictionary” often includes passwords stolen from old data breaches

# CH10 Slides – Networking 1

“Packets are like postcards” –

* General idea: we chop transmitted data (or “packets”) into smaller pieces; the source and destination of the packets (where it’s from and where it’s headed) are put at the beginning of packets as a “header” (expressed as a physical/MAC address)

ARP Poisoning –

* Definition: since ARP (address resolution protocol) maps MAC addresses to IP addresses, ARP poisoning remaps LAN addresses to malicious locations from the ARP cache

DNS –

* Definition: Domain Name System, Internet protocol that converts URL names into IP addresses, and vice versa (URLs <=> IP addresses)

Network switches –

* General idea: network switches keep track of which IP addresses in which traffic and only sends traffic to needed places

# CH11 Slides – Networking 2

Network inspection tools –

1. Network gateway – lists devices on the LAN
2. Network sniffers – scans the network for all incoming traffic (i.e. Wireshark)
3. “nmap” – scans the network address range to locate hosts and the open ports on each host

~~Well Known Port Numbers –~~

* ~~1 – FTP~~
* ~~22 – SSH~~
* ~~23 – Telnet~~
* ~~25 – SMTP~~
* ~~53 – DNS~~
* ~~80/443 – HTTP/S~~
* ~~389 – LDAP (AD)~~
* ~~3389 – Remote Desktop~~

# CH12 Slides – Firewalls

TCP 3-Way Handshake –

1. Client sends a SYN packet
2. Server responds with SYN-ACK packet
3. Client completes the handshake with ACK

DHCP –

* Definition: dynamic host configuration protocol, grants you an IP address when you attempt accessing the Internet (generally our router serves as a DHCP server)

Firewalls –

* Definition: “packet filtration,” allows or denies traffic based on the port or protocol that the request comes through
* Example: HTTP runs on port 443, denying traffic on this port would be a firewall

# CH15 Slides – The Web

Dynamic websites –

* Definition: websites being built on demand actively for the client (this is most websites, such as Twitter); this is opposed to a static website
* Cybersecurity problem: dynamic websites are like “custom software,” there’re no CVE’s (known vulnerabilities) which is easier for hackers to exploit

SQL Injection –

* Definition: an attack exploited through a webpage where you would input your username and password (like a form) by a hacker inserting code into those fields which is read by the server as a command to do something bad (such as providing all usernames and passwords)

“Popping a shell” –

* Definition: when a hacker gains access to the terminal

HTTP –

* Definition: web protocol with no encryption

HTTPS –

* Definition: encrypted web traffic (as opposed to HTTP)

Web Certificates

* General idea: shows that a website is valid

# CHA Slides – Enterprise Risks

Insiders’ vs Outsiders –

* General idea: insiders have little hurdles compared to outsiders since they are already on the network

Shadow IT –

* Definition: insiders using their own tech unaware to cybersecurity professionals
* Example: using a software on the company’s computer that’s not approved as safe by the cybersecurity department