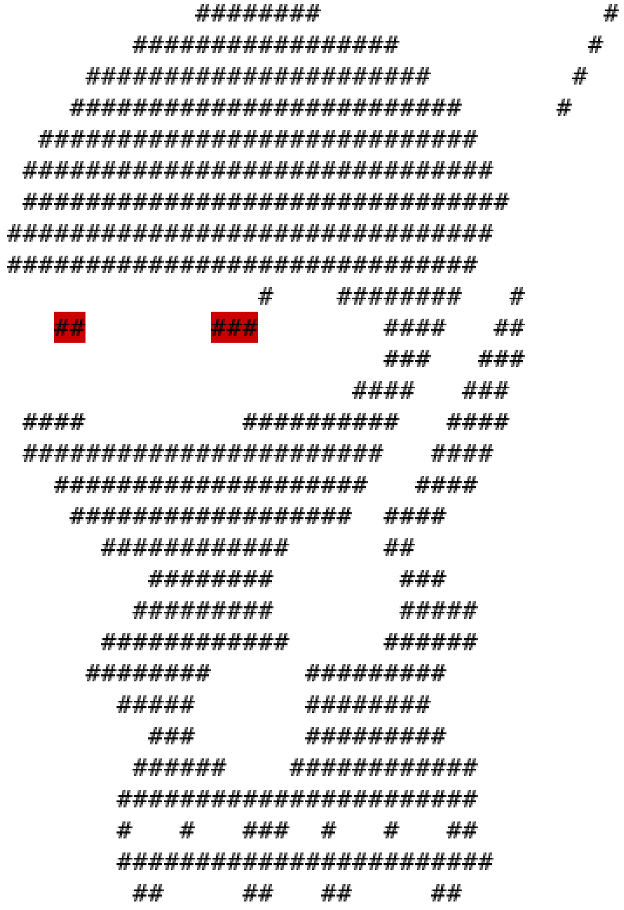
Hacking and Exploits
HACK2200
Dr. Ruba Al Omari



Final Exam Review

Final Practical Exam

Required VMs: 4 virtual machines:

1. Kali Linux
2. Metasploitable 3 Ubuntu
3. Metasploitable 3 Windows Server 2008
4. SEED Ubuntu 20.04 machine

Note: it is your responsibility to ensure you have multiple backup VMs of each of the VMs listed above.

Exam Format

- Open book test. You can use the labs, slides, and the internet to search for help while writing the test.

- Test will be on DC Connect; please ensure you have a working laptop during the test.

- You need internet connection to download the test, and to upload the answer file. You don’t need to be online in-between downloading the test file and uploading the answer file.

Exam Terms

- By proceeding with this test, I promise that I will not lie, cheat, or use any unauthorized aids or assistance to complete this test. Further, I promise that I will not offer any unauthorized assistance to any of my fellow students, and I promise that I will not ask any of my fellow students for unauthorized assistance.
- I promise that the work I submit is my own, and that I will not share this test material with any students.
- I have read the above statement and express my agreement by proceeding to write this test.

What do I need to know?

- You will need to know all of the material from the first class to the last one, including the labs, in order to apply your knowledge and skills to answer the questions.

- Review what is posted on DC Connect including:
  - Lecture notes
  - Tutorials
  - Videos
  - Reading material, and
  - Labs

What should you have learned so far?

Week 1: Ethical Hacking Overview

- CIA Information Security Model
- Information Security Strategies
- What Motivates Cyber-Attackers?
- Attacker Profiles
- Attacker Methods
- Hacking Phases
- What You Can and Cannot Do Legally

Test your knowledge

- What federal law makes it illegal to intercept any type of communication, regardless of how it was transmitted?
  A. Criminal Code Section 184: Interception of Communications
  B. Criminal Code Section 335: Offences Resembling Theft
  C. Criminal Code Section 841: Electronic Documents
  D. All of the above

What should you have learned so far?

Week 2: Reconnaissance / Packet Sniffing and Wireshark

- Reconnaissance
    - Passive Reconnaissance
    - Active Reconnaissance
- Packet Sniffing
- TCP/IP Overview
- The Use of Wireshark

Sample Question

- Given the attached packet capture, find:
  - The third TCP handshake packet numbers
  - What is the IP address of the host who received the handshake
  - In frame 5, what is the source port?
  - Follow the stream …., did the FTP server require a password?

  - Note: in the test, a capture will be provided to you. For practice purposes create your own captures or look for captures online.

What should you have learned so far?

Week 3: Scanning and Enumeration

- Scanning:
  - Scanning Tools
  - Host Discovery
  - Port and Service Discovery
  - OS Discovery
- Enumeration:
  - NetBIOS Enumeration
  - SNMP Enumeration
  - LDAP Enumeration
  - SMTP & DNS Enumeration

Test your knowledge

- What command will you use to find the running services with OS detection?

a) nmap -T4 [target IP address]

b) nmap -sU [target IP address]

c) man nmap

d) nmap –sS –sV -O [target IP address]

What should you have learned so far?

Week 4 : Using Different Metasploit Framework Modules, Exploits, and Payloads to Gain Access:

- System Hacking
- Gaining Access
    - Cracking Passwords
    - Buffer Overflow
    - Identifying Vulnerabilities

Test your knowledge

- Which module in Metasploit framework should you use to bruteforce a password on a victim machine:

a) Exploits

b) Auxiliary

c) Encoders

d) Nops

What should you have learned so far?

Week 5: Using Different Metasploit Framework Modules, Exploits, and Payloads to Maintain Access

- Escalating Privilege
    - Privilege Escalation Techniques
- Maintaining Access
    - Executing Applications
    - Hiding Files

Test your knowledge

- What is a rootkit?

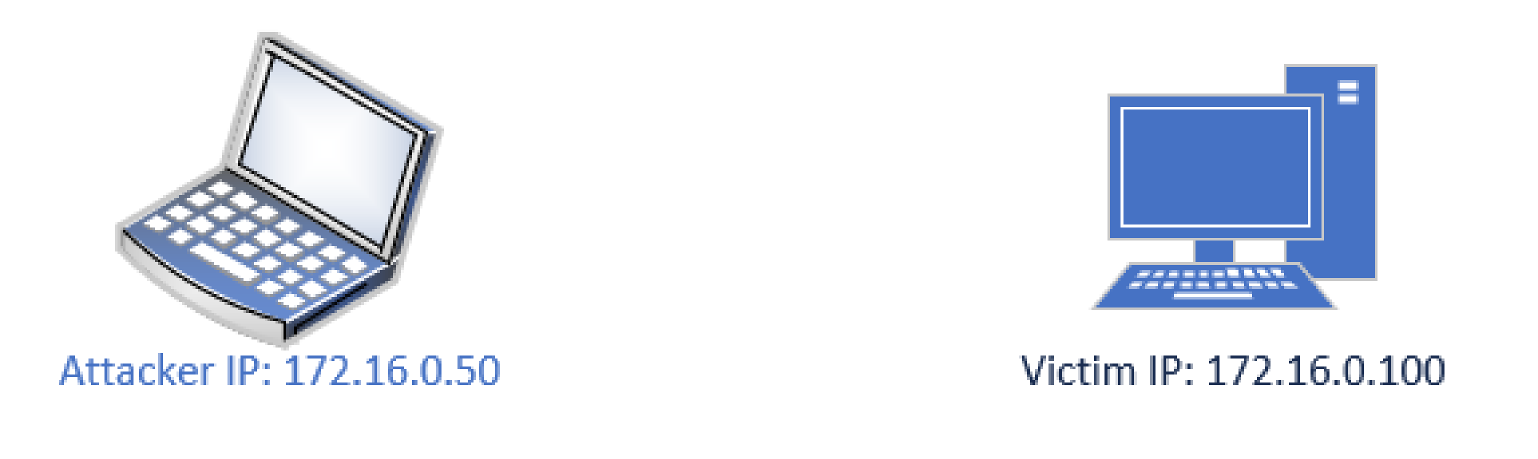
What should you have learned so far?

Week 6: Post Exploitation

- Covering Tracks
- Techniques Used for Covering Tracks

Sample Question

- Write a script to create a reverse shell from the victim to the attacker’s machine shown below using port 7777:-



What should you have learned so far?

Week 7: Network Attacks

- Network Attacks
  - ARP Poisoning
  - Rogue DHCP
  - Rogue AP
  - DoS
- Malware

Sample Question

- Write a simple virus that will …. Examples:
  - Delete all files on a specific partition
  - Delete a specific registry key
  - Release the IP address of the victim
  - Shutdown the victim’s machine
  - Delete the boot.ini
  - Encrypt files
  - Display a message to the victim

What should you have learned so far?

Week 8: Web Security - Cross Site Scripting (XSS)

- Web Application Security
- Cross Site Request Forgery (CSRF) and Countermeasures
- Cross-Site Scripting attacks (XSS) and Countermeasures
  - Reflected XSS (r-XSS)
  - Persistent XSS (s-XSS)
  - DOM-Based XSS
  - Impact of Cross-Site Scripting

Sample question

- Which Cross Site Scripting attack will infect a user by visiting an infected site only, and without them having to click a link on the infected website?
  a. Reflected XSS
  b. Persistent XSS

What should you have learned so far?

Week 9: Software Security - Buffer Overflow

- Software Security
- Buffer Overflow Attack
    - What is Buffer Overflow?
    - Stack-Based Buffer Overflow
    - Countermeasures

Test your knowledge

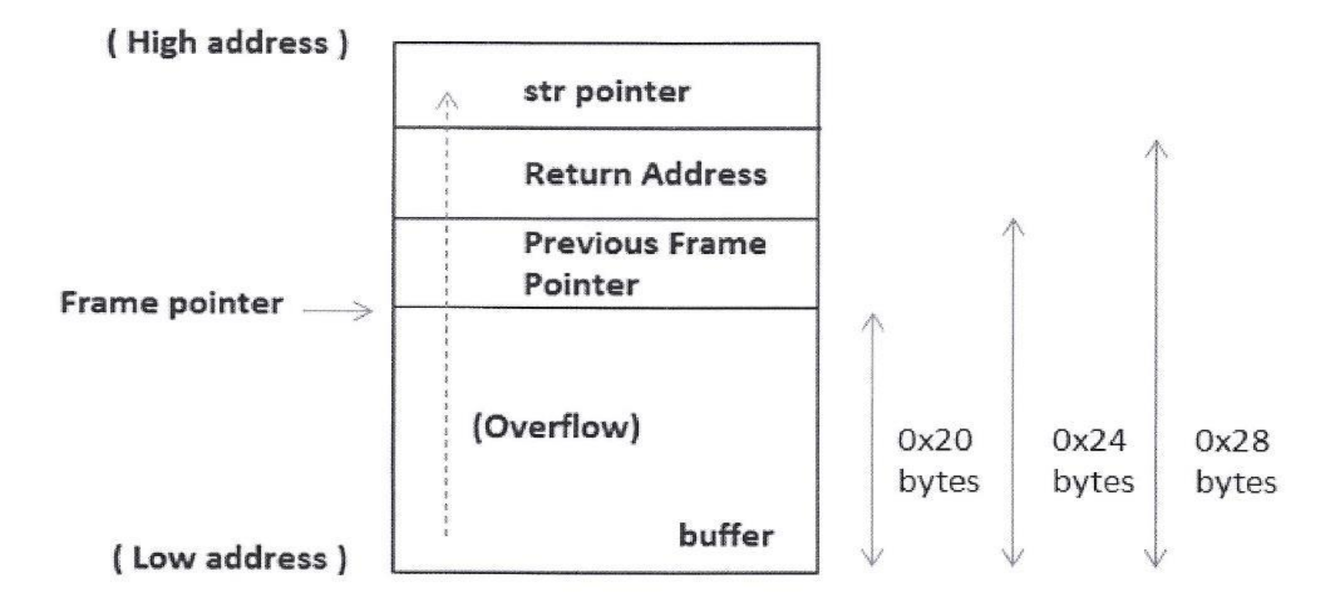
- The buffer (shown below) start address is 0x7C941EED. To inject a code, the returning address shown in the figure should be set to at least:

a) 0x7C941EED

b) 0x7C941F05

c) 0x7C941F15

d) 0x7C941F0D



What should you have learned so far?

Week 10: Web Applications Security - SQL Injection

- Injection Attacks
- SQL Injection Attacks
    - In-Band SQL Injection
    - Blind/Inferential SQL Injection
    - Out-of-Band SQL injection

Test your knowledge

- SQL Injection is a code injection technique that exploits the vulnerabilities in the:

a) Remote code execution

b) Username enumeration

c) Format string vulnerabilities

d) Web application interface between the user and database servers

Test your knowledge

- What type of SQL Injection is:

```
SELECT * FROM users WHERE name = ‘’ OR ‘1’=‘1’;
```

What should you have learned so far?

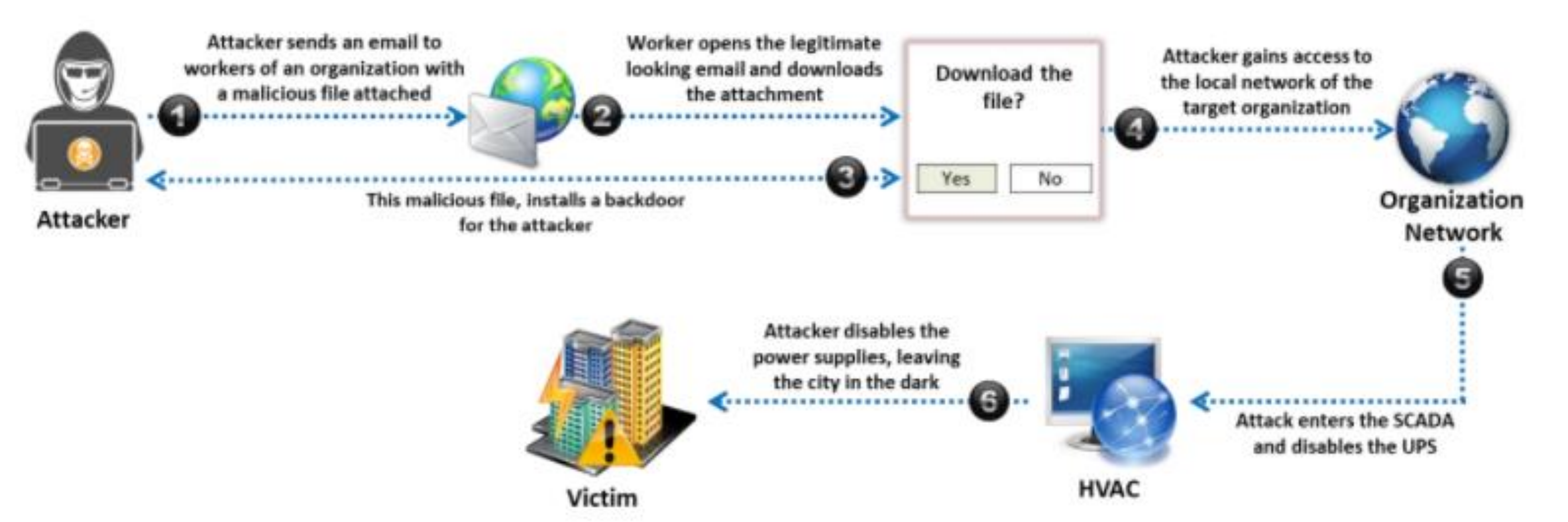
Week 11: Cloud and IoT Security

- IoT
  - What is IoT?
  - How IoT Works
  - IoT Communication Models
  - IoT Security

- Cloud Computing
- Cloud Security - Shared Responsibility Model

Test your knowledge

- What type of attack is shown below



Attacker
1
Attacker sends an email to workers of an organization with a malicious file attached
2
Worker opens the legitimate looking email and downloads the attachment
Download the file?
Yes
No
3
This malicious file, installs a backdoor for the attacker
4
Attacker gains access to the local network of the target organization
Organization Network
5
Attack enters the SCADA and disables the UPS
HVAC
6
Attacker disables the power supplies, leaving the city in the dark
Victim

Good luck!