Shaik Osman

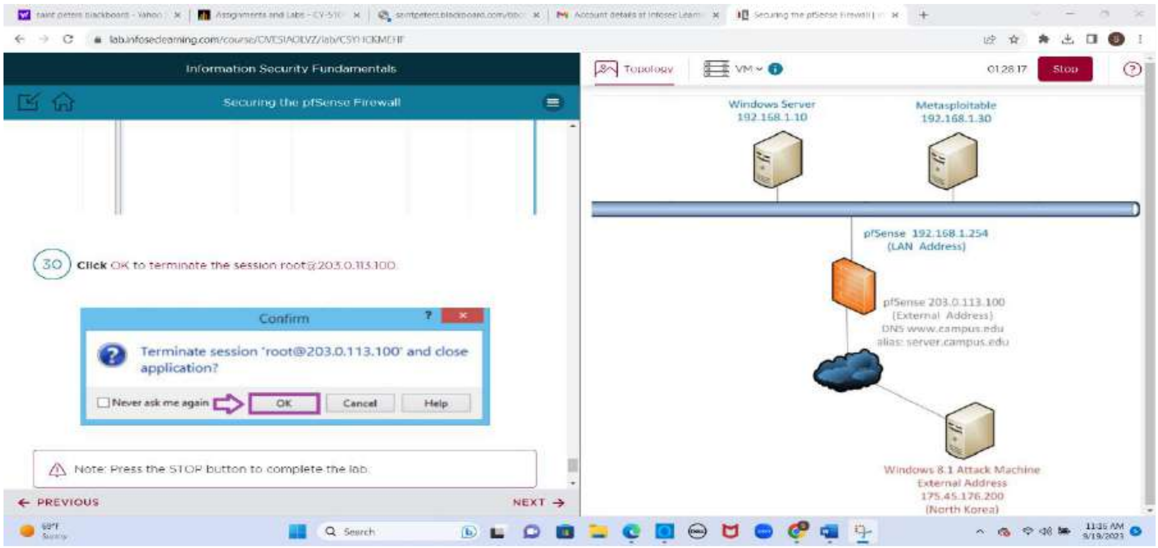
Information Security Fundamentals Lab

Lab 1: <u>Securing the pfSense Firewall</u>

In this lab I have learned how to configure and manage pfSense as a firewall. This includes setting up firewall rules, NAT (Network Address Translation), and port forwarding, to set up Virtual Private Networks (VPNs) on pfSense for secure remote access and site-to-site connectivity, learned various security best practices, such as password management, keeping software and firmware up to date, and implementing strong authentication methods. Understood the concepts of stateful firewall rules and policies to control incoming and outgoing traffic, and the importance of regular updates and patches for pfSense to address vulnerabilities and improve security. Explored techniques for hardening your pfSense installation, including disabling unnecessary services and implementing security-enhancing configurations, and setting up logging and alerting mechanisms to notify administrators of security incidents or suspicious activities. Configure user authentication methods, such as local authentication, to control access to the firewall.

Three lab exercise takeaways:

1. Configure and manage a pfSense firewall effectively. This includes setting up firewall rules, NAT, and port forwarding to control incoming and outgoing traffic, thereby improving your network's security posture.
2. Essential security best practices applicable not only to pfSense but also to network security in general.
3. Monitoring network traffic, setting up logging and alerting mechanisms, and troubleshooting security issues.


saint peters blackboard - Yahoo
Assignments and Labs - CY-510
saintpeters.blackboard.com/bbc
Account details at Infosec Learn
Securing the pfSense Firewall
lab.infosedearning.com/course/CVESIAOLVZ/lab/CSYHCKMEHF
Information Security Fundamentals
Securing the pfSense Firewall
Topology
VM
01:28:17
Stop
Windows Server
192.168.1.10
Metasploitable
192.168.1.30
pfSense 192.168.1.254
(LAN Address)
pfSense 203.0.113.100
(External Address)
DNS www.campus.edu
alias: server.campus.edu
Windows 8.1 Attack Machine
External Address
175.45.176.200
(North Korea)
← PREVIOUS
NEXT →
69°F
Sunny
Search
11:35 AM
9/19/2023

30 Click OK to terminate the session root@203.0.113.100.

Confirm

Terminate session 'root@203.0.113.100' and close application?

□ Never ask me again [OK] [Cancel] [Help]

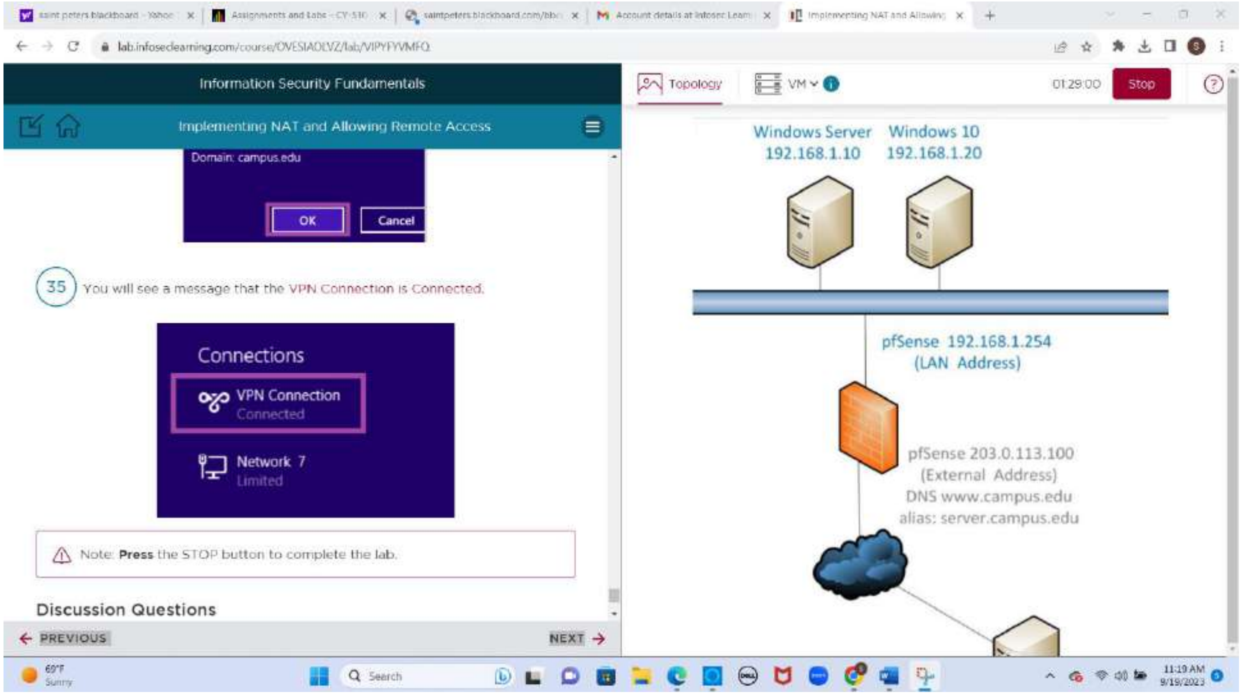
Note: Press the STOP button to complete the lab.

Lab 2: Implementing NAT and Allowing Remote Access

In This lab I learned to configure NAT on a firewall (like pfSense) to translate private IP addresses to a single public IP address. NAT allows multiple devices within a private network to share a single public IP address for internet access, to set up port forwarding rules to allow external traffic to access specific services or devices within your private network. This is essential for enabling remote access to services like web servers, FTP servers, or remote desktops. Explored various remote access protocols, such as SSH (Secure Shell), RDP (Remote Desktop Protocol), VPN (Virtual Private Network), and others. Learned about the security implications of enabling remote access, and the importance of encrypting remote access connections, such as using SSL/TLS for web-based services or SSH for secure command-line access. Set up logging and monitoring for remote access connections to detect and respond to any suspicious or unauthorized access attempts. Gained skills in troubleshooting common issues related to remote access, such as connectivity problems, misconfigured firewall rules, or authentication errors. Learned best practices for remote access implementation and management, including periodic security audits and access reviews.

Three lab exercise takeaways:

1. configure Network Address Translation (NAT) effectively, enabling multiple devices within a private network to share a single public IP address for internet access.
2. Set up and manage remote access to internal resources securely.
3. understanding of the security considerations associated with remote access.



35 You will see a message that the VPN Connection is Connected.

Note: Press the STOP button to complete the lab.

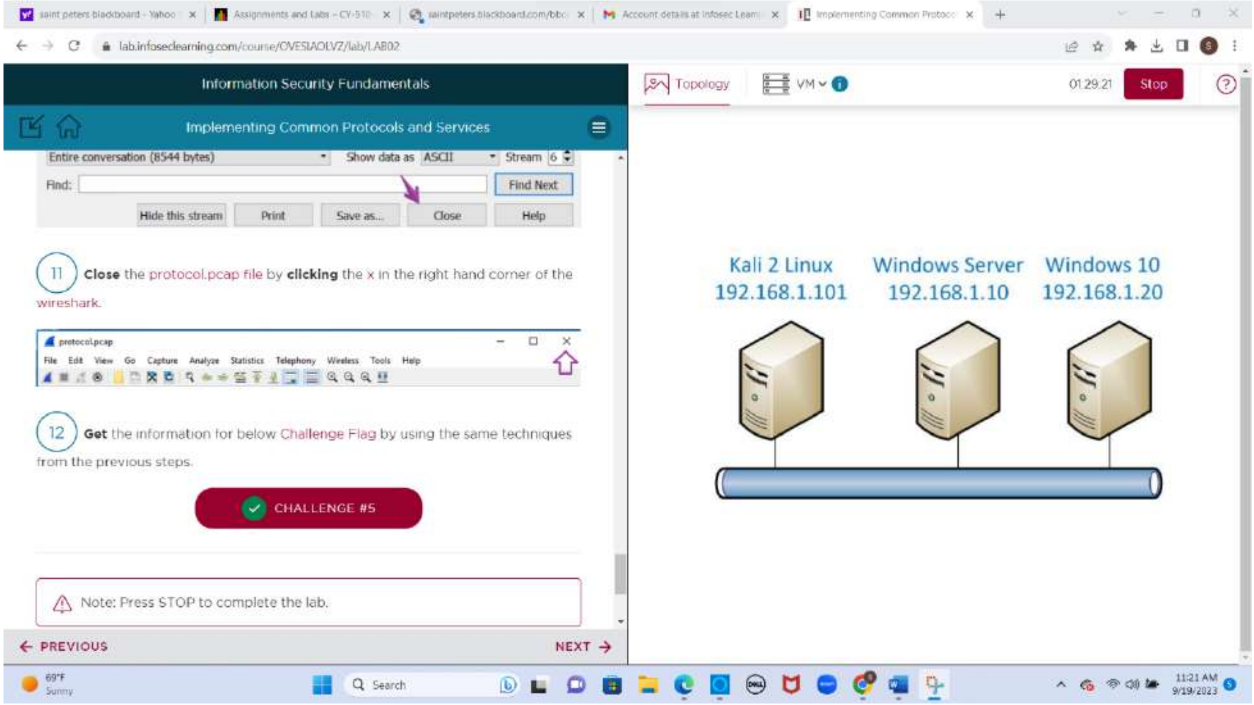
Discussion Questions

Lab 3: Implementing Common Protocols and Services

In this lab I learned how to configure and implement common network protocols such as TCP/IP, ICMP, UDP, DNS, DHCP, HTTP, SMTP, POP3, IMAP, FTP, SSH, and SNMP. Gained practical experience in configuring and managing network services like web servers (e.g., Apache or Nginx), email servers (e.g., Postfix or Microsoft Exchange), file servers (e.g., Samba), and more. Understood how ports and port numbers work and learned how to configure services to listen on specific ports. Gained skills in diagnosing and troubleshooting issues related to protocol and service configuration, learned about load balancing techniques and configuring redundancy for services to ensure high availability and fault tolerance. Understood the importance of logging and monitoring for protocols and services. Learned how to optimize the performance of protocols and services through configuration settings, caching mechanisms, and resource management. Explored how different protocols and services interact with each other and the importance of ensuring compatibility and interoperability in complex network environments.

Three Lab exercise takeaways:

1. Experience in setting up and configuring a variety of common network protocols and services.
2. The importance of security when implementing network services.
3. Developing troubleshooting skills for diagnosing and resolving issues related to protocol and service configuration.


saint peters blackboard - Yahoo
Assignments and Labs - CY-510
saintpeters.blackboard.com/bbc
Account details at Infosec Learn
Implementing Common Protoco
lab.infosedearning.com/course/OVESIAOLVZ/lab/LAB02
Information Security Fundamentals
Implementing Common Protocols and Services
Entire conversation (8544 bytes)
Show data as
ASCII
Stream
6
Find:
Find Next
Hide this stream
Print
Save as...
Close
Help

11 **Close** the protocol.pcap file by **clicking** the x in the right hand corner of the wireshark.

protocol.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

12 **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

Note: Press STOP to complete the lab.

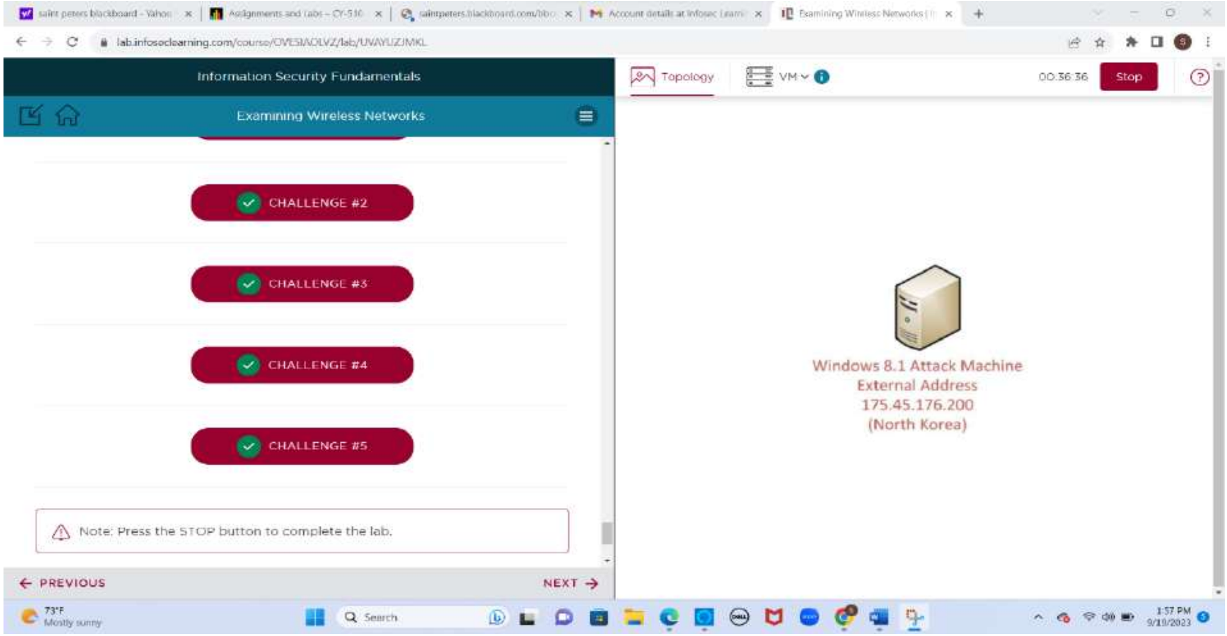
PREVIOUS
NEXT
Topology
VM
01:29:21
Stop
Kali 2 Linux
192.168.1.101
Windows Server
192.168.1.10
Windows 10
192.168.1.20
69°F
Sunny
Search
11:21 AM
9/19/2023

Lab 4: Examining Wireless Networks

In this lab I understood the components of a wireless network, including wireless access points (APs), wireless routers, wireless clients (devices), and how they interact in a wireless network topology, different wireless standards like Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), and Wi-Fi 6 (802.11ax). Understand the role of protocols like 802.11i (WPA2) and 802.11w (Protected Management Frames) in wireless security. Gained practical experience in setting up and configuring a wireless network, including choosing SSIDs (Service Set Identifiers), setting up encryption (e.g., WPA3), and configuring DHCP (Dynamic Host Configuration Protocol) for wireless clients. Explored various wireless security mechanisms, such as encryption (WPA3, WPA2, WEP), MAC address filtering, disabling SSID broadcast, and the importance of strong and unique pre-shared keys (PSKs) or passwords. Learned how to conduct a wireless site survey to determine optimal AP placement, signal coverage, and channel selection for minimizing interference and maximizing performance. Developed skills in diagnosing and troubleshooting common wireless network issues, such as signal interference, connectivity problems, and slow performance. Learned how to set up and manage guest networks with limited access to the internal network to provide internet access for visitors while maintaining security.

Three Lab exercise takeaways:

1. Importance of wireless network security, such as encryption, MAC filtering, and disabling SSID broadcasting, to protect wireless networks from unauthorized access and potential threats.
2. Configuring and setting up wireless networks, including knowledge of encryption methods, SSID configuration, and DHCP setup.
3. Troubleshooting skills for identifying and resolving common wireless network issues.



lab.infosoclearning.com/course/OVESIAOLVZ/lab/UVAYUZJMKL

Information Security Fundamentals

Examining Wireless Networks

Note: Press the STOP button to complete the lab.

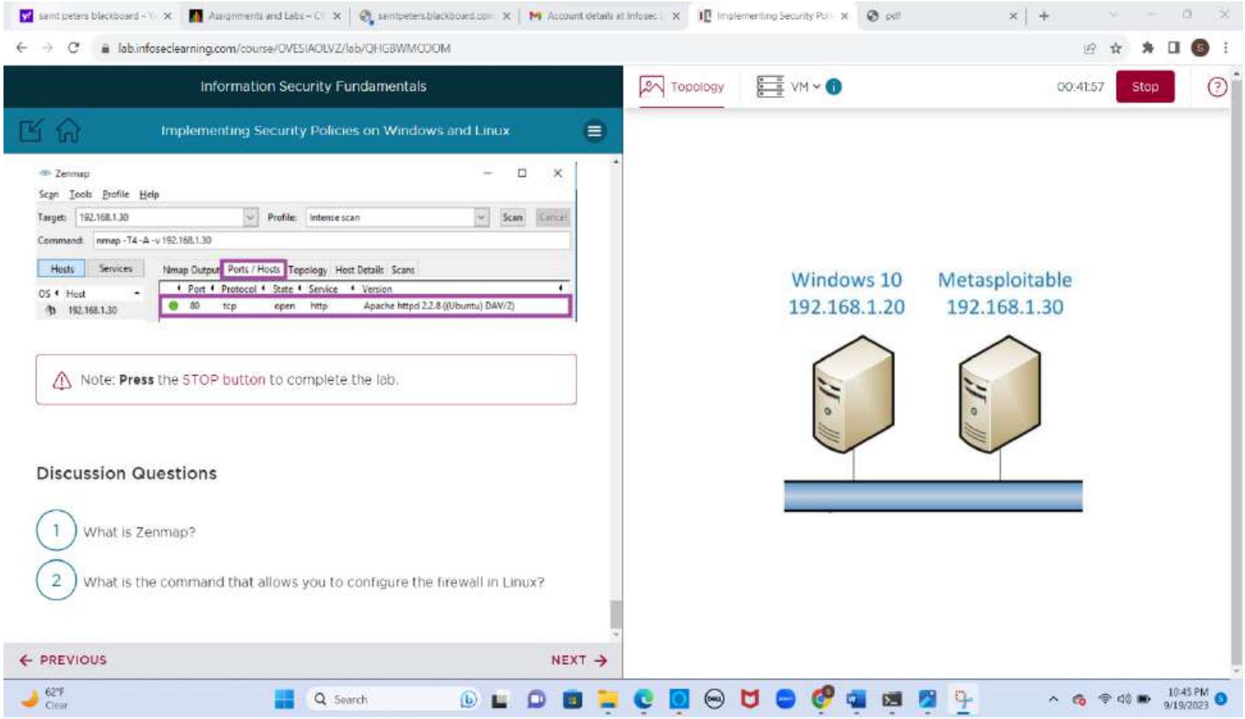
saint peters blackboard - Yahoo
Assignments and labs – CY-510
saintpeters.blackboard.com/bbc
Account details at Infosec Learn
Examining Wireless Networks
CHALLENGE #2
CHALLENGE #3
CHALLENGE #4
CHALLENGE #5
PREVIOUS
NEXT
Topology
VM
00:36:36
Stop
Windows 8.1 Attack Machine
External Address
175.45.176.200
(North Korea)
73°F
Mostly sunny
Search
1:57 PM
9/19/2023

Lab 5: Implementing Security Policies on Windows and Linux

In this lab I Learned how to create, modify, and manage user accounts and groups on both Windows and Linux systems. Configure and enforce password policies, including password complexity requirements, password expiration, and account lockout policies to strengthen authentication security. Understood how ACLs work on both Windows (NTFS permissions) and Linux (file system permissions). Gained experience in configuring firewalls on both Windows and Linux systems to control inbound and outbound network traffic, configure security auditing and logging on both Windows and Linux systems to record security events and activities. Understood how to align system configurations with organizational security policies and compliance standards, such as PCI DSS, HIPAA, or CIS benchmarks. Implementing security hardening practices to reduce the attack surface of both Windows and Linux systems. Developed incident response procedures and protocols for both Windows and Linux systems to efficiently respond to security breaches or incidents, configure secure remote access methods like SSH for Linux and RDP for Windows while implementing strong authentication and encryption for remote connections.

Three Lab exercise takeaways:

1. Configuring and enforcing security policies, including user management, access control, firewall configuration, and security updates.
2. Aligning system configurations with organizational security policies and compliance standards.
3. Developing incident response plans to address security incidents efficiently.



Target: 192.168.1.30 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.30

OS	Host
	192.168.1.30

	Port	Protocol	State	Service	Version
●	80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Note: **Press** the STOP button to complete the lab.

Discussion Questions

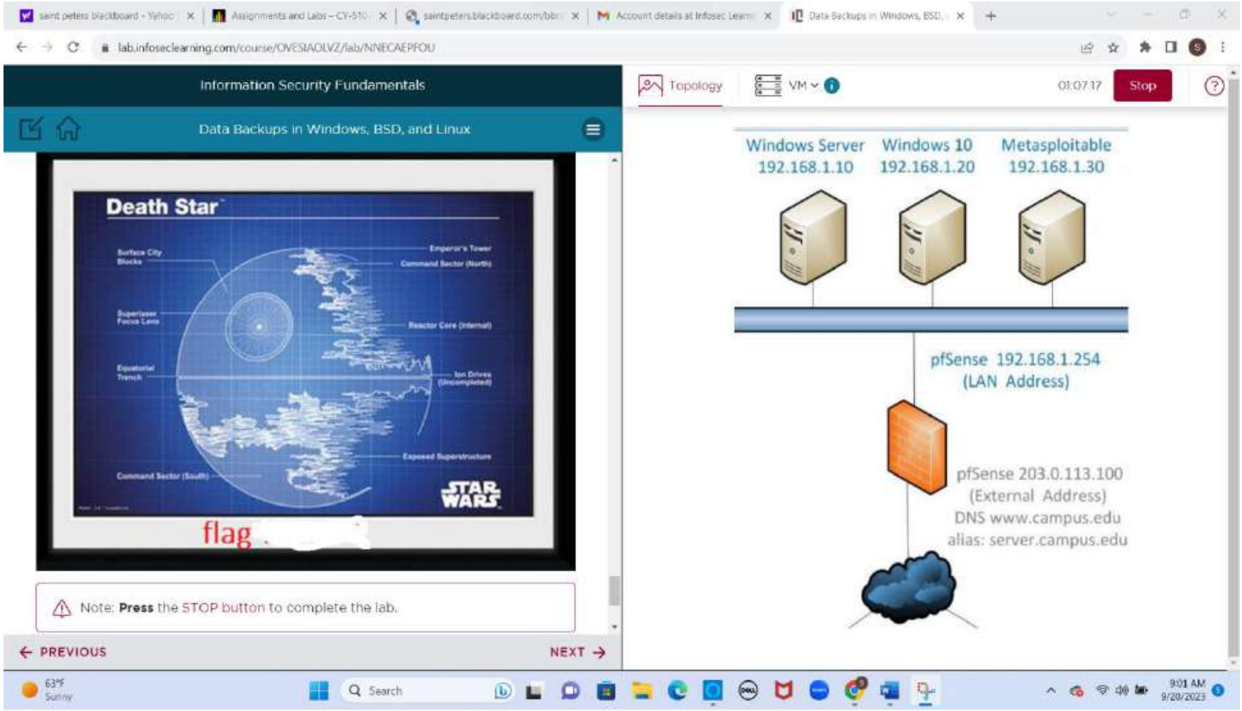
1. What is Zenmap?
2. What is the command that allows you to configure the firewall in Linux?

Lab 6: <u>Data Backups in Windows, BSD, and Linux</u>

In this lab I learned the fundamental concepts of data backup, including the importance of regular backups, data retention policies, and the difference between full, incremental, and differential backups, and about backup tools and utilities available on Windows, BSD, and Linux systems, such as Windows Backup and Restore, tar, rsync, dd, and specific backup solutions. Understood how to select and include specific files, directories, or system components in your backups based on your data protection requirements. Learned how to automate backup tasks by setting up scheduled backup jobs to ensure that backups are performed regularly without manual intervention. Understood the benefits of data compression and encryption during backup processes to save storage space and enhance security. Explored techniques for creating versioned backups or snapshots to maintain multiple historical copies of data, allowing for point-in-time recovery. Gained insights into backup best practices, including data retention policies, off-site storage, and the 3-2-1 backup rule.

Three Lab exercise takeaways:

1. The importance of establishing a comprehensive backup strategy that includes selecting appropriate backup methods, storage solutions, and data retention policies.
2. To set up backup systems that ensure data recovery in the event of data loss or system failure.
3. The ability to design and implement effective backup solutions tailored to their organization's needs.


saint peters blackboard - Yahoo
Assignments and Labs – CY-510
saintpeters.blackboard.com/bbc
Account details at Infosec Learn
Data Backups in Windows, BSD,
lab.infoseclearning.com/course/OVESIAOLVZ/lab/NNECAEPFOU
Information Security Fundamentals
Data Backups in Windows, BSD, and Linux
Death Star
Surface City Blocks
Superlaser Focus Lens
Equatorial Trench
Command Sector (South)
Emperor's Tower
Command Sector (North)
Reactor Core (Internal)
Ion Drives (Uncompleted)
Exposed Superstructure
STAR WARS
Topology
VM
01:07:17
Stop
Windows Server 192.168.1.10
Windows 10 192.168.1.20
Metasploitable 192.168.1.30
pfSense 192.168.1.254 (LAN Address)
pfSense 203.0.113.100 (External Address)
DNS www.campus.edu
alias: server.campus.edu
PREVIOUS
NEXT
63°F Sunny
Search
9:01 AM
9/20/2023

flag [redacted]

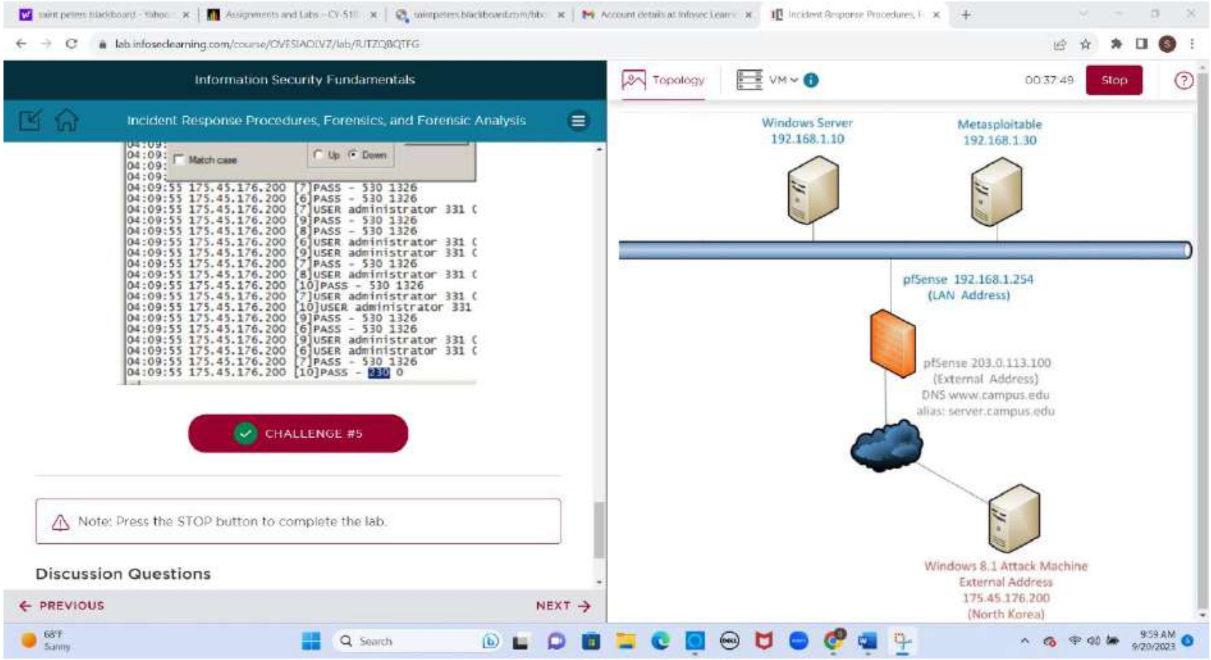
Note: **Press** the STOP button to complete the lab.

Lab 7: <u>Incident Response Procedures, Forensics, and Forensic Analysis</u>

In this lab I understood the importance of having a well-defined incident response plan in place. Learned how to create, update, and implement IRPs tailored to your organization's needs, and to categorize security incidents based on severity and impact to prioritize response efforts effectively. Explored methods and tools for detecting security incidents, including intrusion detection systems (IDS), security information and event management (SIEM) solutions, and manual monitoring. Gained skills in quickly assessing the scope and impact of an incident, as well as the resources required to contain and investigate it. Learned the principles of collecting digital evidence while preserving its integrity and chain of custody. Understand how to use digital forensics tools to capture volatile data and disk images. Learned how to perform memory forensics to extract valuable information from a compromised system's RAM, including running processes and network connections. Understood how to examine network traffic logs, packet captures, and firewall logs to reconstruct the timeline of an incident and identify malicious activities. Developed the skills to create comprehensive forensic reports that document the incident, the evidence collected, and the analysis performed.

Three Lab exercise takeaways:

1. The importance of having an incident response plan and the ability to execute it.
2. Investigating security incidents and understanding the nature and scope of cyberattacks.
3. Legal and ethical considerations surrounding incident response and digital forensics, including privacy laws, chain of custody, and compliance requirements.


saint peters blackboard - Yahoo
Assignments and Labs – CY-511
saintpeters.blackboard.com/bb
Account details at Infosec Learn
Incident Response Procedures, F
lab.infoseclearning.com/course/OVFSIAOIVZ/lab/RJTZQBQTFG
Information Security Fundamentals
Incident Response Procedures, Forensics, and Forensic Analysis
□ Match case
○ Up ● Down
Topology
VM
00:37:49
Stop
Windows Server
192.168.1.10
Metasploitable
192.168.1.30
pfSense 192.168.1.254
(LAN Address)
pfSense 203.0.113.100
(External Address)
DNS www.campus.edu
alias: server.campus.edu
Windows 8.1 Attack Machine
External Address
175.45.176.200
(North Korea)
CHALLENGE #5
← PREVIOUS
NEXT →
68°F
Sunny
Search
9:59 AM
9/20/2023

```
04:09:
04:09:
04:09:
04:09:
04:09:55 175.45.176.200 [7]PASS - 530 1326
04:09:55 175.45.176.200 [6]PASS - 530 1326
04:09:55 175.45.176.200 [7]USER administrator 331 (
04:09:55 175.45.176.200 [9]PASS - 530 1326
04:09:55 175.45.176.200 [8]PASS - 530 1326
04:09:55 175.45.176.200 [6]USER administrator 331 (
04:09:55 175.45.176.200 [9]USER administrator 331 (
04:09:55 175.45.176.200 [7]PASS - 530 1326
04:09:55 175.45.176.200 [8]USER administrator 331 (
04:09:55 175.45.176.200 [10]PASS - 530 1326
04:09:55 175.45.176.200 [7]USER administrator 331 (
04:09:55 175.45.176.200 [10]USER administrator 331
04:09:55 175.45.176.200 [9]PASS - 530 1326
04:09:55 175.45.176.200 [6]PASS - 530 1326
04:09:55 175.45.176.200 [9]USER administrator 331 (
04:09:55 175.45.176.200 [6]USER administrator 331 (
04:09:55 175.45.176.200 [7]PASS - 530 1326
04:09:55 175.45.176.200 [10]PASS - 230 0
```

Note: Press the STOP button to complete the lab.

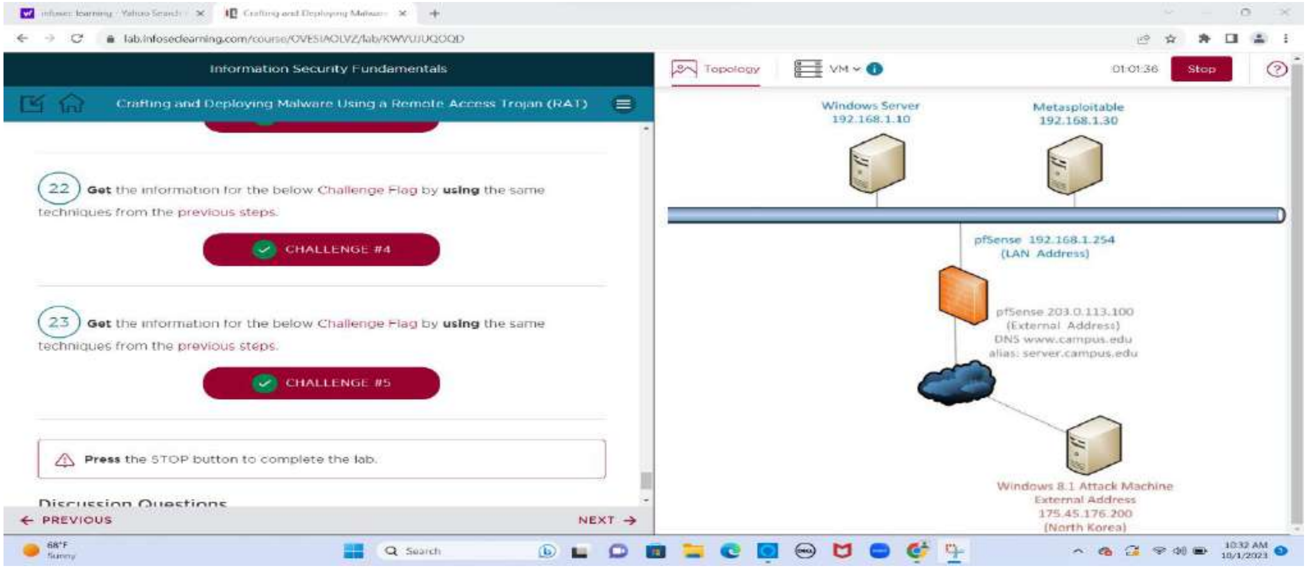
Discussion Questions

Lab 8: Crafting and Deploying Malware Using a Remote Access Trojan (RAT)

In this lab I have learned about the various components that make up a malware program, such as the payload, propagation methods, command and control (C2) servers, and evasion techniques, gained insights into how RATs work, including how they establish connections to compromised systems, capture data, control remote devices, and exfiltrate information. Understanding how RATs are deployed often involves exploring the vulnerabilities and exploiting techniques that attackers use to gain initial access to a target system. Gained insight into what attackers can do once they have control over a compromised system, such as data exfiltration, lateral movement, privilege escalation, and more. How malware is crafted and deployed, you can better appreciate the strategies and technologies used by cybersecurity professionals to defend against such threats. This includes intrusion detection systems, antivirus software, network monitoring, and security best practices.

Three lab takeaways:

1. Recognizing how malware is built, its functionality, and the techniques used by attackers to create and deploy it.
2. Aware of the tactics and techniques used by malicious actors to compromise systems and gain unauthorized access.
3. Regularly updating software and systems, implementing strong access controls, conducting regular security audits, and educating users about security risks.



22 **Get** the information for the below Challenge Flag by **using** the same techniques from the previous steps.

23 **Get** the information for the below Challenge Flag by **using** the same techniques from the previous steps.

Press the STOP button to complete the lab.

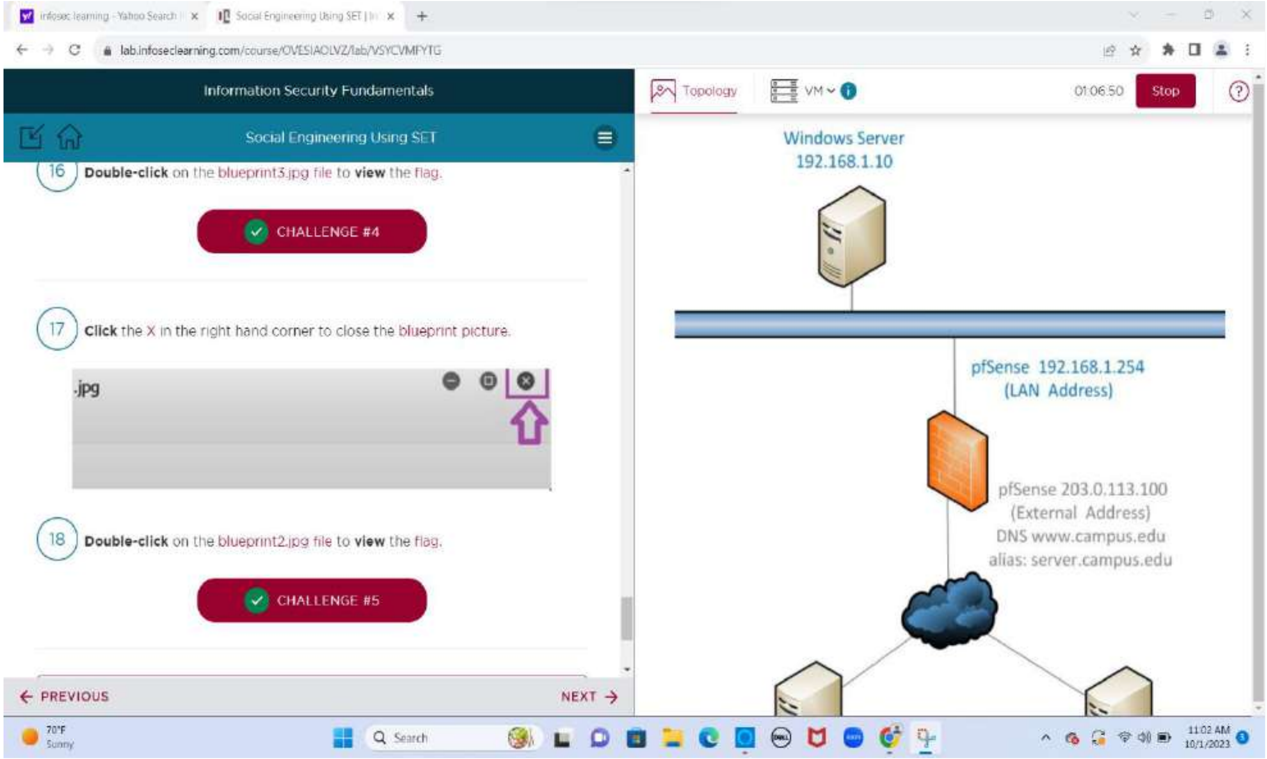
Discussion Questions

Lab 9: Social Engineering Using SET

In this lab I have learned about various social engineering tactics, such as pretexting, phishing, baiting, tailgating, and more. Understanding these techniques helps individuals recognize when they are being targeted and how to respond effectively. This lab introduced me to tools like the Social Engineering Toolkit, which is often used for penetration testing and security assessments. I have learned how attackers can use these tools to craft convincing social engineering attacks and how security professionals can use them to test and bolster defenses. Social engineering relies on manipulating human psychology and behavior. I have gained insights into the psychological principles that underlie social engineering attacks, including the use of authority, urgency, trust, and curiosity to deceive individuals. Understood the potential consequences of disclosing sensitive information or taking unauthorized actions based on manipulative requests. Studied real-world examples of social engineering attacks to understand how they work and the impact they can have on individuals and organizations.

Three Lab takeaways:

1. Importance of educating users and employees about social engineering threats.
2. To recognize various social engineering tactics and manipulation techniques employed by attackers.
3. Emphasis on ethical and responsible use of social engineering knowledge.



lab.infoseclearning.com/course/OVESIAOLVZ/lab/VSYCVMFYTG

Information Security Fundamentals

Social Engineering Using SET

16 **Double-click** on the blueprint3.jpg file to **view** the flag.

17 **Click** the X in the right hand corner to close the blueprint picture.

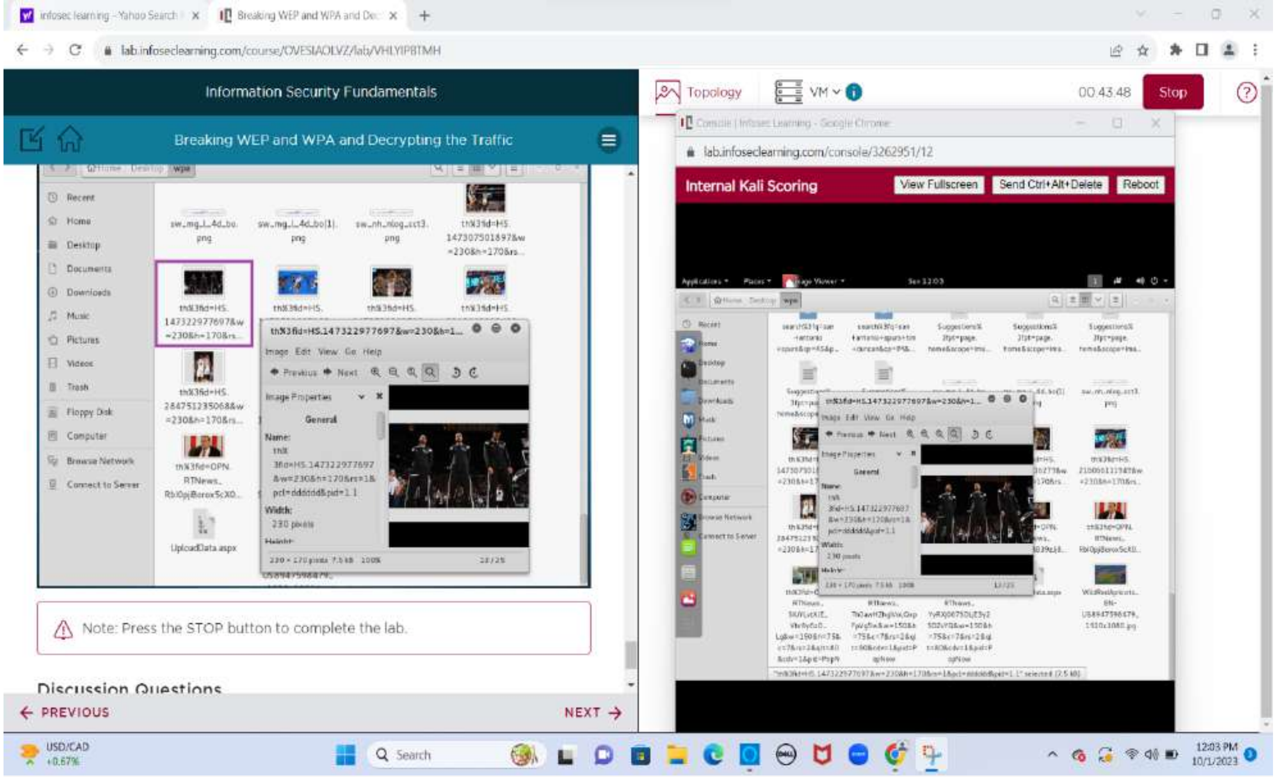
18 **Double-click** on the blueprint2.jpg file to **view** the flag.

Lab 10: <u>Breaking WEP and WPA and Decrypting the Traffic</u>

In this lab I have learned about the basics of wireless security protocols, particularly WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). Understood the strengths and weaknesses of these protocols and why they have been susceptible to attacks, common vulnerabilities, and weaknesses in WEP and WPA, such as weak encryption keys, weak initialization vectors (IVs), and flawed key management and how tools like Aircrack-ng, Reaver, or similar software can be used to capture network traffic and recover encryption keys. Gained knowledge of how captured network packets can be analyzed to recover encryption keys, making it possible to decrypt network traffic and how decrypted traffic can be inspected, revealing potentially sensitive information. Learned about legal and regulatory requirements regarding wireless network security. Compliance with laws such as the Computer Fraud and Abuse Act (CFAA) and ethical hacking guidelines is crucial.

Three lab takeaways:

1. Understanding the vulnerabilities and weaknesses in wireless security protocols like WEP and WPA.
2. How attacks are executed, including capturing network traffic, and decrypting it.
3. Techniques should only be applied in controlled and authorized environments, such as security testing or research, and never for malicious purposes.



Note: Press the STOP button to complete the lab.

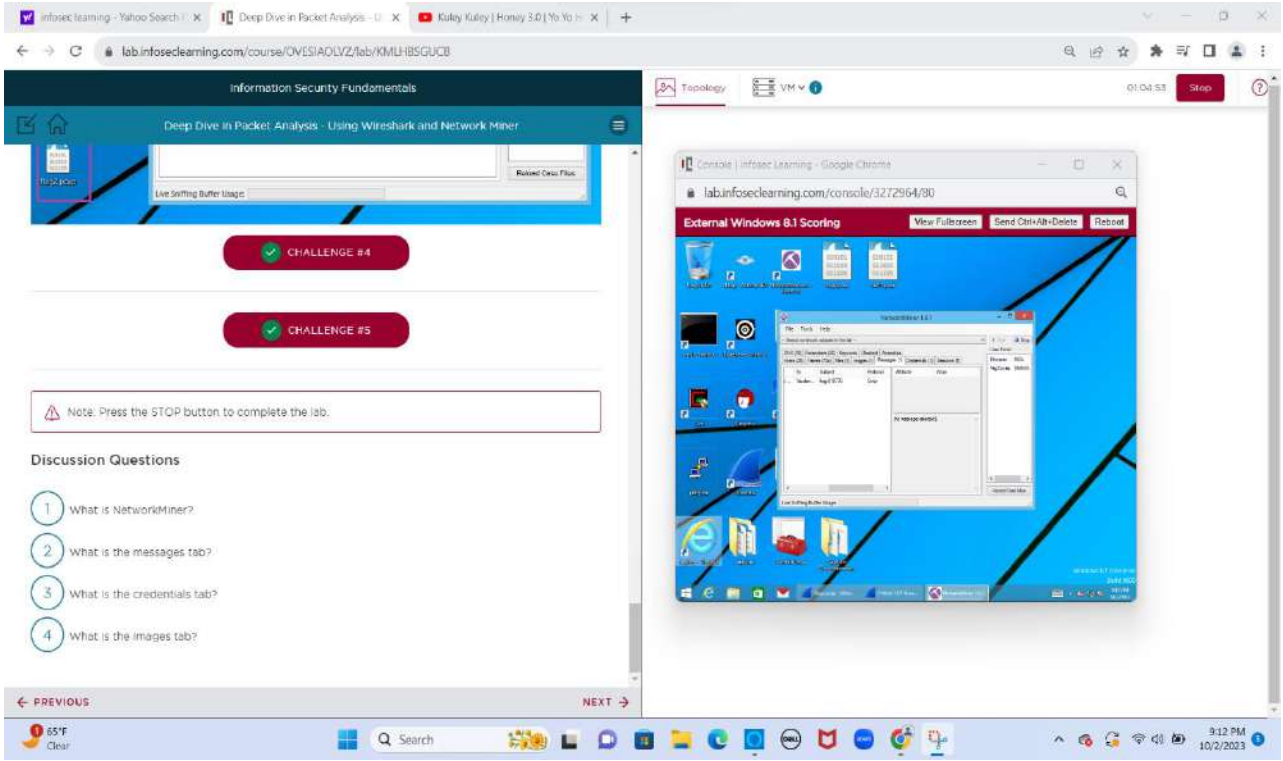
Discussion Questions

Lab 11: <u>Deep Dive in Packet Analysis - Using Wireshark and Network Miner</u>

In this lab I have learned the basics of packet capture, including how network packets are captured and stored for analysis. Understood the capture process is essential for acquiring network data effectively. The lab introduced me to the Wireshark and Network Miner tools, which are widely used for packet analysis. Gained skills in inspecting individual network packets. This includes understanding packet headers, payload data, and various network protocols. Learned to identify network anomalies, potential security threats, and performance issues by examining packet details and to identify specific signatures or patterns associated with network attacks or suspicious behavior. Gained insights into understanding typical traffic patterns and behaviors within a network. Learned how to use packet analysis to investigate security incidents, such as malware infections, network intrusions, or data breaches and capturing network traffic without authorization may violate privacy laws and ethical standards.

Three lab takeaways:

1. Develop proficiency in capturing, inspecting, and analyzing network packets using tools like Wireshark and Network Miner.
2. Identifying signs of network intrusions, malware infections, or data breaches by analyzing network traffic patterns and identifying unusual or suspicious behavior.
3. visualize their findings and communicate them effectively through reporting.


infosec learning - Yahoo Search
Deep Dive in Packet Analysis - U
Kuley Kuley | Honey 3.0 | Yo Yo H
lab.infoseclearning.com/course/OVESIAOLVZ/lab/KMLHBSGUCB
Information Security Fundamentals
Deep Dive in Packet Analysis - Using Wireshark and Network Miner
Reload Case Files
Live Sniffing Buffer Usage
CHALLENGE #4
CHALLENGE #5
Topology
VM
01:04:53
Stop
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3272964/80
External Windows 8.1 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
NetworkMiner 1.6.1
← PREVIOUS
NEXT →
65°F
Clear
Search
9:12 PM
10/2/2023

Note: Press the STOP button to complete the lab.

Discussion Questions

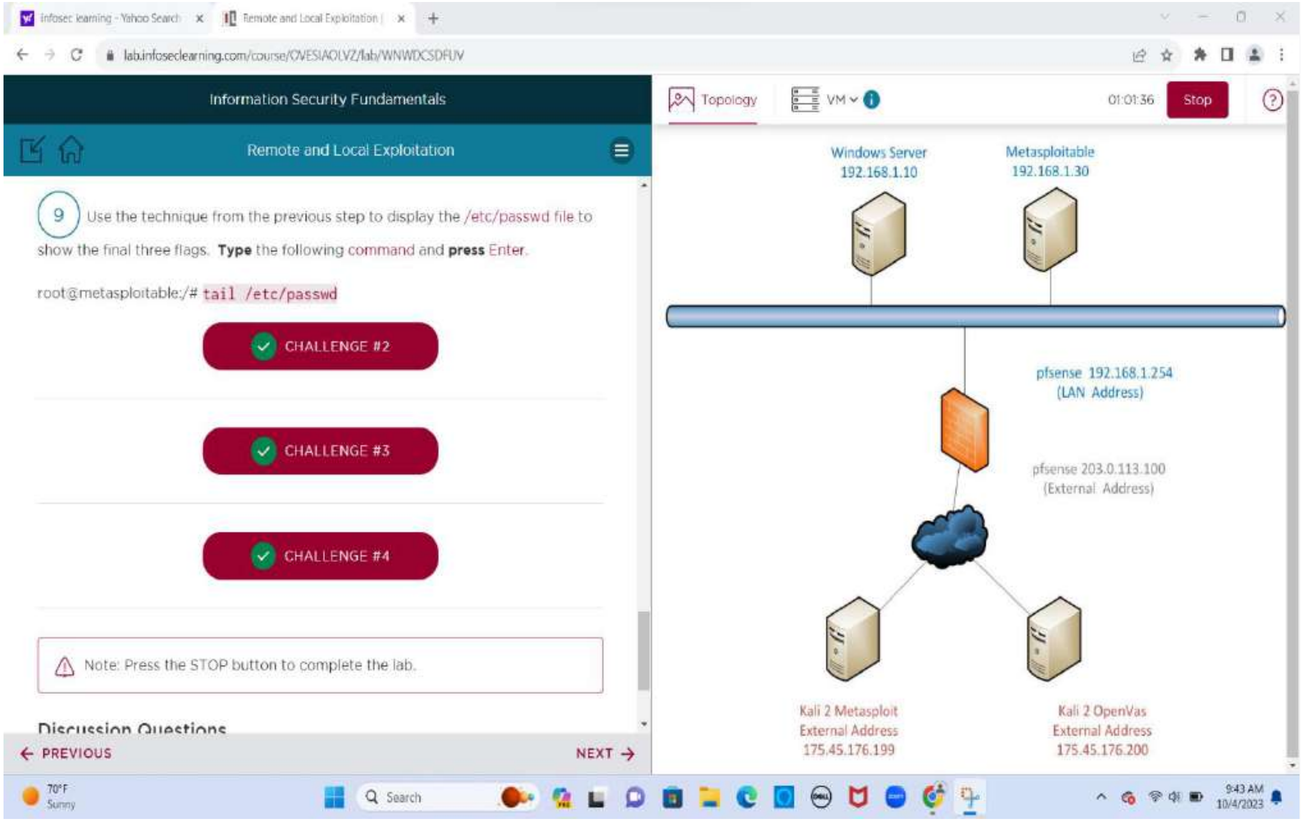
1. What is NetworkMiner?
2. What is the messages tab?
3. What is the credentials tab?
4. What is the images tab?

Lab 12: <u>Remote and Local Exploitation</u>

In this lab I have learned how to identify and assess vulnerabilities in software, operating systems, and network configurations and techniques for exploiting vulnerabilities in remote systems over a network, such as using remote code execution vulnerabilities or exploiting weak authentication mechanisms and about local privilege escalation vulnerabilities and how attackers can escalate their privileges from a low-privileged user to gain administrator or root access. Understood post-exploitation activities is essential for both offensive and defensive cybersecurity strategies. Learned how to implement mitigation strategies to defend against exploitation attempts and about legal and regulatory requirements related to cybersecurity and ethical hacking. This lab provides valuable insights into identifying and exploiting vulnerabilities in computer systems and networks. It also emphasizes ethical considerations, encourages proactive security measures, and teaches individuals how to defend against exploitation attempts.

Three lab takeaways:

1. Awareness of potential vulnerabilities in computer systems and networks.
2. Understanding of how attackers can exploit vulnerabilities, both remotely and locally.
3. Emphasis on ethical and legal considerations.



9 Use the technique from the previous step to display the /etc/passwd file to show the final three flags. **Type** the following command and **press** Enter.

```
root@metasploitable:/# tail /etc/passwd
```

✓ CHALLENGE #2

✓ CHALLENGE #3

✓ CHALLENGE #4

Note: Press the STOP button to complete the lab.

Discussion Questions

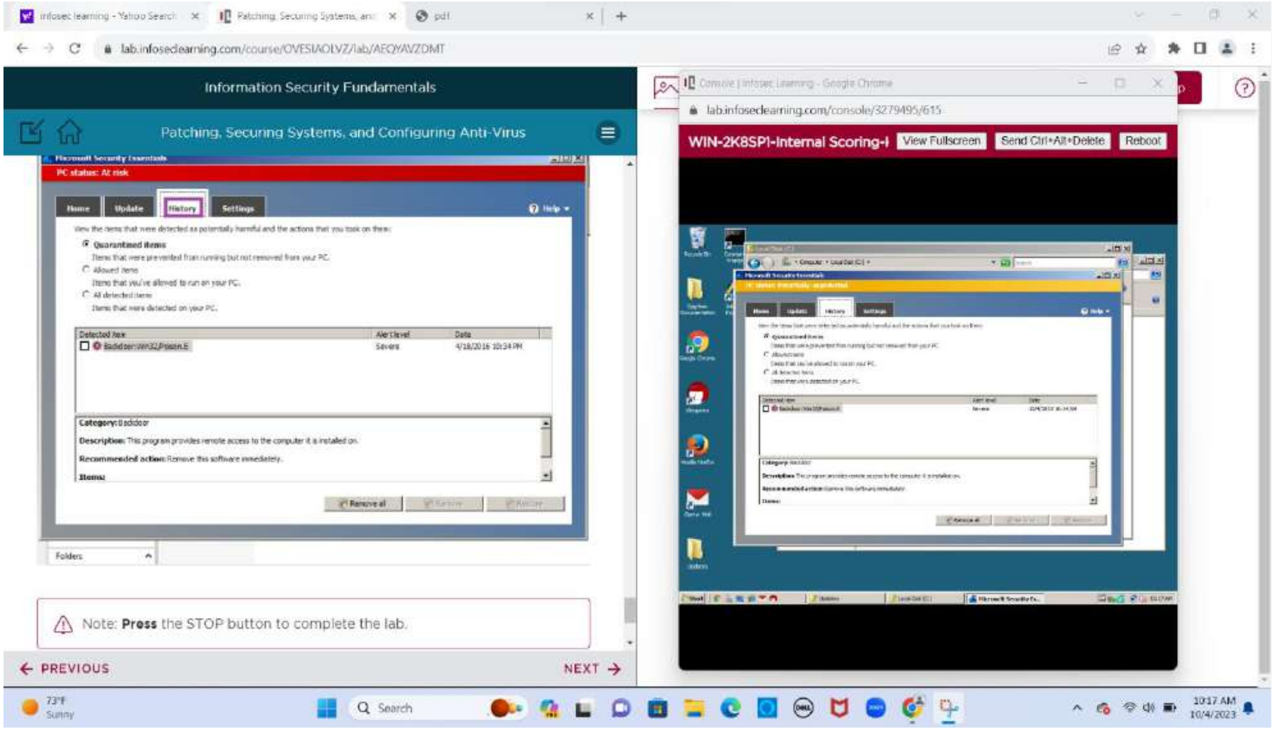
← PREVIOUS NEXT →

Lab 13: Patching, Securing Systems, and Configuring Anti-Virus

In this lab I have learned the importance of keeping operating systems and software up to date with security patches and updates and how vulnerabilities can be exploited by attackers when systems are not properly patched and the consequences of neglecting patch management. The lab covers best practices for securing system configurations and how to harden system configurations to reduce the risk of unauthorized access and attacks. Learned how to properly configure and use antivirus software to protect against malware, including viruses, Trojans, and ransomware. Understood the importance of regular antivirus updates and how to schedule and configure scans and how to conduct vulnerability assessments and security audits on systems to identify weaknesses that could be exploited, how to respond to security incidents effectively, contain threats, and mitigate potential damage. Gained an understanding of developing and implementing security policies and procedures within an organization. Learned about industry-specific compliance requirements and regulations related to cybersecurity, such as GDPR, HIPAA, or PCI DSS.

Three lab takeaways:

1. Proactive security measures, such as regular patching, system hardening, and configuring antivirus software, are crucial for safeguarding computer systems against cybersecurity threats.
2. Significance of security awareness and user training.
3. Importance of compliance with industry-specific regulations and standards.



infosec learning - Yahoo Search
Patching, Securing Systems, an
pdf
lab.infoseclearning.com/course/OVESIAOLVZ/lab/AEQYAVZDMT
Information Security Fundamentals
Patching, Securing Systems, and Configuring Anti-Virus
Microsoft Security Essentials
Home
Update
History
Settings
Help
Remove all
Remove
Restore
Folders
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3279495/615
WIN-2K8SP1-Internal Scoring-I
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
73°F
Sunny
Search
10:17 AM
10/4/2023

PC status: At risk

View the items that were detected as potentially harmful and the actions that you took on them:

● Quarantined items
Items that were prevented from running but not removed from your PC.

○ Allowed items
Items that you've allowed to run on your PC.

○ All detected items
Items that were detected on your PC.

Detected item	Alert level	Date
□ Backdoor:Win32/Poison.E	Severe	4/18/2016 10:34 PM

Category: Backdoor

Description: This program provides remote access to the computer it is installed on.

Recommended action: Remove this software immediately.

Items:

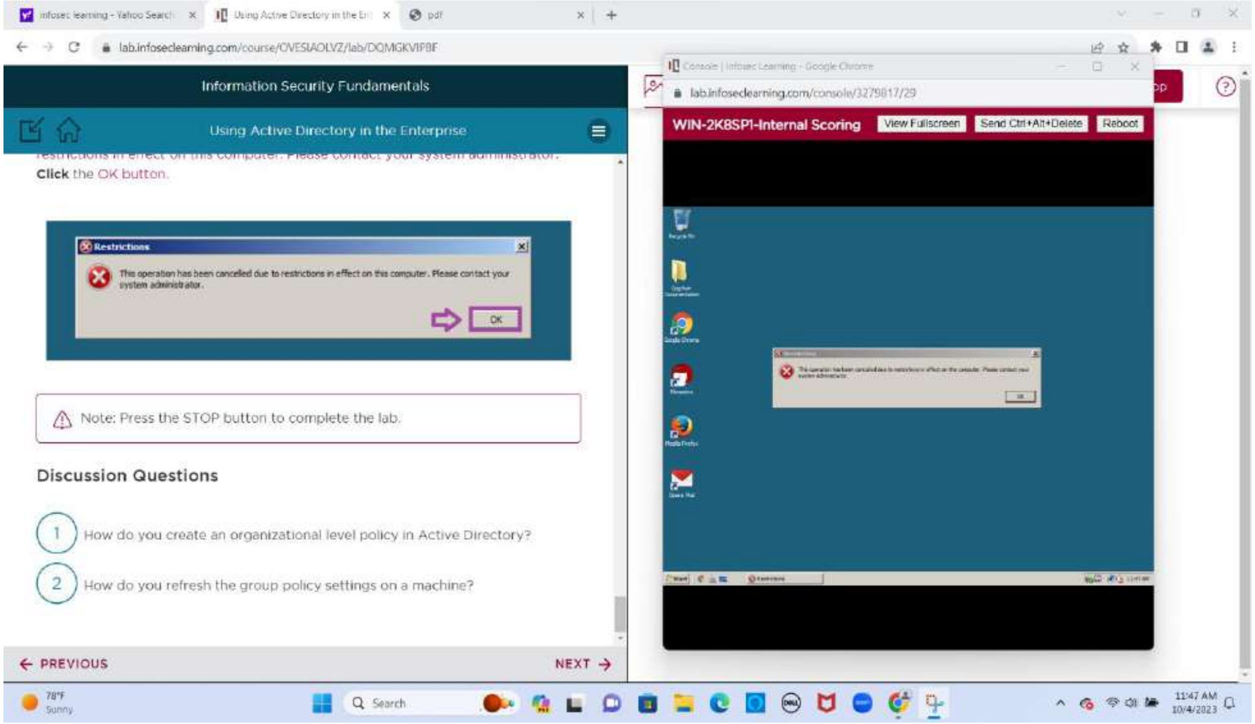
⚠ Note: **Press** the STOP button to complete the lab.

Lab 14: <u>Using Active Directory in the Enterprise</u>

In this lab I have learned the fundamentals of Active Directory, including its purpose, components, and architecture. You'll understand how AD serves as a centralized directory service for managing users, computers, groups, and resources in a networked environment. Gained knowledge of how to manage network resources, such as printers, shared folders, and networked devices, within an Active Directory environment. This includes assigning permissions and access control. Learned about strategies for ensuring high availability and disaster recovery within an Active Directory environment. Gained skills in troubleshooting common Active Directory issues, such as user account lockouts, DNS problems, and replication errors. This lab provides me with a comprehensive understanding of Active Directory and its practical applications in managing users, resources, and security in an enterprise network.

Three lab takeaways:

1. Significance of Active Directory as a centralized directory service for managing users, computers, and resources in an enterprise network.
2. The role of Active Directory in enforcing security measures, such as authentication, access control, and Group Policy management.
3. Insights into strategies for scaling Active Directory to meet the needs of large and complex enterprise environments.


infosec learning - Yahoo Search
Using Active Directory in the En
pdf
lab.infosecleaming.com/course/OVESIAOLVZ/lab/DQMGKVIPBF
Information Security Fundamentals
Using Active Directory in the Enterprise
Console | Infosec Learning - Google Chrome
lab.infosecleaming.com/console/3279817/29
WIN-2K8SP1-Internal Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
78°F
Sunny
Search
11:47 AM
10/4/2023

restrictions in effect on this computer. Please contact your system administrator.

Click the OK button.

Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

OK

Note: Press the STOP button to complete the lab.

Discussion Questions

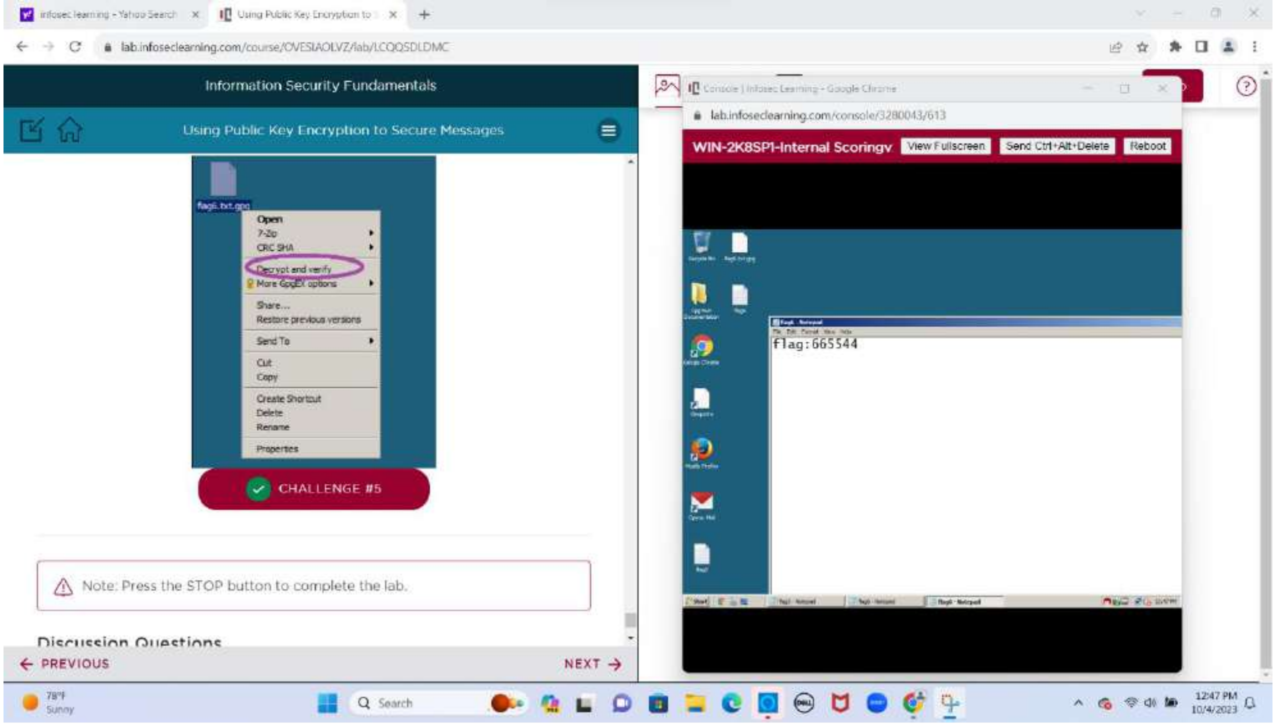
1. How do you create an organizational level policy in Active Directory?
2. How do you refresh the group policy settings on a machine?

Lab 15: <u>Using Public Key Encryption to Secure Messages</u>

In this lab I have learned the basics of public key cryptography, which involves the use of two related keys, a public key and a private key, for encrypting and decrypting messages. Gained an understanding of how asymmetric encryption works and its advantages in securing communication. Learned how to create and manage key pairs, which is essential for secure communication and how to use public keys to encrypt messages and private keys to decrypt them. Gained practical experience in encrypting and decrypting messages using public key encryption algorithms like RSA or ECC (Elliptic Curve Cryptography). Understood how digital signatures enhance message authentication and non-repudiation and how to use public key encryption to establish secure and confidential communication channels, ensuring that sensitive information is protected during transmission. Explored real-world applications of public key encryption, such as email encryption (e.g., PGP or S/MIME), secure web browsing, and secure file transfers.

Three lab takeaways:

1. Fundamental understanding of public key cryptography, including how it works, the concept of key pairs, and the asymmetric encryption process.
2. Experience in encrypting and decrypting messages using public key encryption techniques.
3. Security best practices for managing keys, protecting private keys, and ensuring the security of encrypted communication.


infosec learning - Yahoo Search
Using Public Key Encryption to
lab.infoseclearning.com/course/OVESIAOLVZ/lab/LCQQSDLDMC
Information Security Fundamentals
Using Public Key Encryption to Secure Messages
flag6.txt.gpg
Open
7-Zip
CRC SHA
Decrypt and verify
More GpgEX options
Share...
Restore previous versions
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties
CHALLENGE #5
Discussion Questions
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3280043/613
WIN-2K8SP1-Internal Scoringv
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
78°F
Sunny
Search
12:47 PM
10/4/2023

Note: Press the STOP button to complete the lab.

```
flag:665544
```