Donda, Vinay Kumar Reddy dondavinayreddy@gmail.com

This document explains the procedure of how to use the security tools and their implementations in real time. All the commands concepts etc., are implemented by me in real time and got certifications on that.
Please do check my LinkedIn profile: https://www.linkedin.com/in/vinay-reddy-donda-36b10a20b/

This document will cover multiple concepts

1. **Managing Linux accounts:**
2. **Applying the encryption and hashing for secure communications.**
3. **Implementing the SDLC lifecycle**
4. **Performing Dynamic and static quality control testing:**
5. **Implementing Access Controls with Windows Active Directory**
6. **Using Access Control Lists to Modify File System Permissions on Windows System**
7. **Authenticating Security Communications with Digital Signatures**
8. **Configuring Linux File System Permissions**
9. **Analysing the traffic and protocols using wireshark**
10. **Using Wireshark and Netwitness Investigator to Analyze Wireless Traffic**
11. **Configuring a pfSense Firewall on the Server**
12. **Configuring a VPN Client for Secure File Transfers**
13. **Configuring a Virtual Private Network Server**
14. **Securing the Network with an Intrusion Detection System (IDS)**
15. **Recognizing Risks and Threats Associated with Emerging Technologies**
16. **Performing a Vulnerability Assessment**
17. **Analyzing Network Traffic to Create a Baseline Definition**
18. **Attacking a Vulnerable Web Application and Database**
19. **Exploiting Known Web Vulnerabilities on a Live Web Server**
20. **Investigating and Responding to Security Incidents**
21. **Conducting an Incident Response for a Suspicious Login**
22. **Investigating and Responding to Network Security Incidents**
23. **Performing a Post-Mortem Review of a Data Breach Incident**

Cyber security foundations:
Lab1:
Managing Linux accounts:
In this lab we will able to

- Create new users and groups
- Give administrate privileges to the users.
- Delete user accounts
- Understand different user account types and use of groups

Code used to add the users:

```
#yourname: Script to add users to Linux system
if [ $(id -u) -eq 0 ]; then
          read -p "Enter Full name : " comment
          read -p "Enter username : " username
          read -s -p "Enter password : " password
          egrep "^$username" /etc/passwd >/dev/null
          if [ $? -eq 0 ]; then
               echo "$username exists!"
               exit 1
          else
               pass=$(perl -e 'print crypt($ARGV[0], "password")' $password)
               useradd -m $username -p $pass -c "$comment"
               [ $? -eq 0 ] && echo "User has been added!" || echo "Failed to add a user!"
          fi
else
          echo "Only root may add a user to the system."
          exit 2
fi
```

Code used to view the added users
cat /etc/passwd
Code used to view the members of the group
grep “username” /etc/passwd
Code used to make the users as the administrators
usermod -aG root username
Code used to add the groups
groupadd groupname
Code used to add the users to group
usermod -aG groupname username
Code used to delete the user or group
deluser –remove-home username (or) deluser username
delgroup –remove-home groupname (or) delgroup groupname

Tools used in this lab : VI Editor, Terminal , Nano editor
Lab 2:
Applying the encryption and hashing for secure communications.

- Apply common cryptographic and hashing techniques on a message to ensure message confidentiality and integrity

- Verify the integrity of a message or file using hashing techniques to determine if it has been manipulated or modified

- Create an MD5 checksum and SHA-1 hash on a message or file and verify file integrity

- Explain the importance of checking the hash before executing or unzipping an unknown file

- Encrypt and decrypt a GnuPG encrypted message to ensure confidentiality between two parties

Most familiar hashing algorthims are MD5 and SHA1
MD5 uses 128 bit hash sum and
SHA1 uses 160 bit hash sum

Steps for hashing:
To create a hash sum for the file we use
Md5sum filename example : md5sum example.txt

In order to store the hash sum or hash string in .md5 file we use the command
Md5sum filename newfilename.md5 eg: md5sum example.txt example.txt.md5

To view the contents of the hash sum string
cat example.txt.md5

To check whether the hash sum is created for the example.txt
Md5sum -c example.txt.md5 it displays ok if it is correct.

Same process will be continued for the sha1

In order to know how the encryption is done check the lab manual

Adding the text to the file and will override it

echo data > filename

Adding the text to end of the file remaining data remains same and this data adds at the last

echo data >> filename

To generate the key command used is
gpg –gen-keys

Tools and softwares used: Gnu privacy guard, Vi editor, Key transfer, WinSCP

We use GNUPG to generate the key pairs and this GNUPG keys are used for encryption and decryption.

Lab 3:
Implementing the SDLC lifecycle

- Describe the Microsoft Security Development Lifecycle Plan (SDL)
- Build a threat model for a simple web application
- Create and compare an attack surface baseline for analysis
- Test Regular Expressions for a Regular Expression denial of service (ReDoS) vulnerability
- Test a dynamic link library (DLL) for possible security issues

Tools used:

- Attack Surface Analyzer
- BinScope Binary Analyzer
- Damn Vulnerable Web Application (DVWA)
- Microsoft Threat Modeling Tool
- OpenSSL
- PuTTY
- SDL Regex Fuzzer

Attack surface analyser to used to run the scan before and after installing the application.

SDL regex fuzzer is used to check whether the regex is passing or not

Threat modelling tool is used to design the model

Binscope is used to test the Dynamic link library.

Lab 4:

Performing Dynamic and static quality control testing:

- Identify tools and techniques commonly used for website and Web application software code testing
- Use various techniques and tools to help provide the most comprehensive testing for software code and Web applications
- Dynamically test software for vulnerabilities in the code and understand the concepts and benefits of manual code reviews using the open source tool skipfish
- Perform static analysis testing on software source code and evaluate the advantages and disadvantages of various testing methods
- Compare and analyze the Web application source code using skipfish and RATS to help identify vulnerabilities and insecure coding tactics

Tools used:

- Damn Vulnerable Web Application (DVWA)
- PuTTY
- RATS
- skipfish
- vi Editor

In this lab, you will use skipfish, a dynamic testing tool, to identify vulnerabilities in the Damn Vulnerable Web Application (DVWA). The DVWA is a Web application that is made purposefully vulnerable. It is installed on a local Web server to allow security analysts a safe place to test the security of their applications. You also will use RATS (Rough Auditing Tool for Security) to perform static analysis testing on the DVWA. You will use the vi Editor to review the source code for a part of the DVWA to identify exactly where the software code is most vulnerable. Finally, you will compare the results of both skipfish and RATS reports.

DIFFERENCE BETWEEN STATIC AND DYNAMIC ANALYSIS.

Static analysis is performed on the source code itself while dynamic analysis is commonly called testing, and is performed on input and output of the executable.

DIFFERENCE BETWEEN STATIC AND DYNAMIC TESTING.

Static testing is a system of White Box **testing** where developers verify or check code to find fault. This type of **testing** is completed without executing the

applications that are currently developed. **Dynamic Testing** is completed by walking the real application with valid entries to verify the expected results.

Lab 5:

Implementing Access Controls with Windows Active Directory

- Create new global security groups using Microsoft Windows Active Directory
- Create new domain users using Microsoft Windows Active Directory
- Assign domain users to global security groups using Microsoft Windows Active Directory
- Create a simple folder system to match an organization's departmental structure
- Configure departmental group folders with unique access rights per defined access control requirements
- Remotely access a Windows Server machine using different user accounts and test access rights for your organization's folder system

Icacls command:

The icacls utility can be used to explicitly grant or remove permissions for groups and users of a specified file or directory. The icacls utility is a command-line tool that requires you to use the following syntax.

To remove permissions:

The **`remove`** command combined with **`:g`** removes any explicitly granted permissions. The **`remove`** command combined with **`:d`** removes any explicitly denied permissions.

- **`icacls.exe <directory path> /remove:g <user name or group>`**
- **`icacls.exe <directory path> /remove:d <user name or group>`**

To add (grant) permissions:

The **grant** command has two variations: The first option, shown in the first example without the appended **:r**, will add the specified permissions to any previously granted permissions. The second option, **grant:r**, replaces any previously granted explicit permissions.

- **icacls.exe <full directory path> /grant <user name or group>:<permission>**
- **icacls.exe <full directory path> /grant:r <user name or group>:<permission>**

To grant NTFS permissions to a user name or group, you must use one of the following forms:

(D) – delete access	**(F)** – full access
(M) – modify access	**(R)** – read-only access
(RX) – read and execute access	**(W)** – write-only access

For example, to grant read-only to the CoreFiles directory to a group titled Students, you would use the following command:

- **icacls.exe C:\CoreFiles /grant Students:(R)**

Tools used:

Microsoft Active Directory, icacls.exe

Lab 6:

Using Access Control Lists to Modify File System Permissions on Windows System

1. Control a registered user's ability to access resources in Microsoft Windows
2. Identify existing access control list definitions for protected objects
3. Modify access control list definitions
4. Validate access control list definitions
5. Create a script to add new users and new groups, modify permissions, and create new directories

To know the existing file permissions

```
icacls.exe filepath
```

```
example: icacls.exe C:\LabDocuments\SFfiles
```

Note: If at any point you cannot remember the syntax for a given command, **type** `icacls /?` and **press Enter** to open the icacls help manual.

`New-ADUser` – A PowerShell cmdlet that creates an Active Directory user.
`-Name` – Specifies the username.
`-SamAccountName` – Specifies the logon name used to support Windows clients and servers.
`-GivenName` – Specifies the first name for the user account.
`-Surname` – Specifies the last name for the user account.

Set-ADAccountPassword – A PowerShell cmdlet that specifies the user account's password.
-Identity – Specifies the Active Directory user object (e.g., username).

ConvertTo-SecureString -AsPlainText "*password*" -Force – A PowerShell cmdlet that converts a plain text password, such as P@ssw0rd!, into a secure string.

Enable-ADAccount – The PowerShell cmdlet that brings an account active.

New-ADGroup – A PowerShell cmdlet to create a new group.
-Name – Specifies the name of the group you want to create.
-SamAccountName – Specifies the resource name (same as New-ADGroup).
-GroupScope – Specifies the scope of the group as either Global or Universal.
-GroupCategory – Specifies the type of group as Security or Distribution.

Add-ADGroupMember – A PowerShell cmdlet to add an Active Directory user to a group.
-Identity – Specifies the Active Directory group object.
-Members – Specifies the Active Directory user object to be added to the group.

New-Item – A PowerShell cmdlet to create a new file or directory.
-type – Specifies *file* or *directory*
-path – Specifies the full path to the new file or directory.

DirPermissions – A PowerShell cmdlet to assign permissions to a file or directory.
-Location – Specifies the full path to the file or directory.
-User – Specifies the user account or group for which permissions will be assigned.
-Permission - Specifies the level of permission this user will be granted.
-Inherit – Specifies the permissions that this file or directory will inherit from the parent object.

Tools and softwares:

- icacls.exe
- Notepad++
- PowerShell

Lab 7:

Authenticating Security Communications with Digital Signatures

1. Create a digitally signed message.
2. Verify a digital signature.
3. Understand the purpose of digital signatures.
4. Understand the use of digital signatures.

At the command prompt, **type** `gpg --list-keys` and **press Enter** to list the public keys that are in Roger's GPG keyring. You should see only Roger's own public key that you just created.

At the command prompt, **type** `gpg --list-secret-keys` and **press Enter** to list the private keys that are in Roger's GPG keyring. You should see only Roger's own private key that you just created.

Tools and softwares:

- GNU Privacy Guard (GPG)
- Mousepad
- GPG4Win/Kleopatra
- rng/tools
- WinSCP

rng-tools, a random number generator (rng), will run continuously in the background to generate enough entropy for GPG to generate its key set in seconds instead of minutes.

GPG4Win/Kleopatra first it generates the key pair and we need to import the key which is shared from another user and we need to verify that key which is digitally signed and last step is to view the message by verifying or decrypting the message.

Lab 8.

Configuring Linux File System Permissions

1. Create basic Linux directories.
2. Assign Linux file permissions to individual users and groups.
3. Change the ownership of a directory.
4. Change the directory permissions and directory group permissions.
5. Change the group owner of a directory.
6. In the next steps, you will use the **`chmod`** (change mode) command to change the access permissions of a file. Absolute (full path) and relative paths are both taken; however, you must be in the directory the file is located to use a relative path. In this lab, you will change the permissions using an alphabetic symbol to represent the roles and permissions assigned to each role, which are:
7.

Role	Symbol	Permission	Symbol
Users	u	Read	r
Group	g	Write	w
All other users	o	Execute	x

8.
9. The symbol to grant permissions is **+** and the symbol to remove permissions is **-**. For example, to give a group permission to read, write, and execute on the /usr/coursework/StudentWorkspace/BetsyAfiles directory, run the following command: **`chmod g+rw /usr/coursework/StudentWorkspace/BetsyAfiles`**.

Tools and softwares.

- AWK

- YAD
- **BASH** is a command processor that runs in a text or terminal window.
- **AWK** is a data-drive scripting language that takes action with data streams and textual data.
- **YAD** (Yet Another Dialog) is a versatile lightweight GUI (Graphical User interface) interaction shell.

Lab 9:

Enabling Windows Active Directory and User Access Controlss

1. Understand how Microsoft's Active Directory Domain Services can help implement an access control framework

2. Use Active Directory to create new user accounts and security groups

3. Implement a Windows file folder structure with custom permission rights

4. Augment an existing Group Policy to facilitate remote access

5. Create and verify access control lists to protect objects and folders from unauthorized access

Tools and softwares:

- Active Directory Domain Services
- Group Policy Object Editor
- PowerShell

ENTERPRISE SECURITY

Lab 1:
Analysing the traffic and protocols using wireshark

1. Use basic features of the Wireshark packet capture and analysis software.
2. Apply appropriate filters to view only the traffic subset of interest.
3. Be able to reliably and consistently place probes to capture packet traffic.
4. Determine whether timing and clocking is synchronized for better reliability and repeatability.
5. Guarantee that all traffic is being captured and that the interface rate and capture rate are compatible.
6. Capture and analyze basic Internet Protocol transactions and determine basic configuration information about the IP hosts from which traffic is captured.

Tools and softwares:
Wireshark

Using wireshark we can find
Source and destination address
Frame number
Data transferred through the website
Internet protocol version
Source port and destination port

Lab2:
Using Wireshark and Netwitness Investigator to Analyze Wireless Traffic

1. Analyze the wireless-specific portion of network traffic using Wireshark.
2. Identify the portions of network traffic that remain the same regardless of whether the packets traverse wires or fly through the air wirelessly.

3. Use features of the NetWitness Investigator tool to analyze traffic with wireless content.

4. Determine which tool, Wireshark or NetWitness Investigator, is the preferred tool for a given task.

5. Utilize both Wireshark and NetWitness Investigator together to provide a complete picture of the interactions being investigated.

6. Be able to generalize your new knowledge of Wi-Fi traffic to other types of wireless traffic analyzed by using the Wireshark analyzer.

7. Differentiate between the more generalized capabilities of Wireshark and the more specialized cybersecurity analysis-focused uses of NetWitness Investigator.

NetWitness Investigator, on the other hand, requires the purchase of a license for use, so it is often used only by more skilled security analysts for specific types of analysis. Often, investigators, or even clients, with little training can capture needed information with the no-cost Wireshark while a more in-depth security-focused analysis is later done with NetWitness Investigator.

While you will not find any of the low-level wireless information in NetWitness Investigator that you found in Wireshark, such as command and control, you will find that the kind of sophisticated analysis that requires some work to accomplish within Wireshark is automated by NetWitness Investigator. For instance, the Layer 2 MAC addresses, which in this case are Ethernet, and the Layer 3 IP addresses are available in both Wireshark and NetWitness, but you will not find the transmitter and receiver addresses in NetWitness. What you will find easily in NetWitness is information about the geographic location of the transmitter and receiver which, when plotted on Google Earth, can aid an investigation.

Using netwitness investigator we can find.

NetWitness Investigator Collection Categories	
SECTION TITLE	**DESCRIPTION**
Service Type	Types of traffic seen on the network.
Source IP Address	Who sent traffic?
Destination IP Address	Who received traffic?
Action Event	Commands seen in the traffic flow.
User Account	User names seen on the network.

Extension	Types of files seen on the network.
Filename	Names of files seen on the network. **Click [open]** to view.
TCP Destination Port	TCP Ports accessed.
UDP Target Port	UDP Ports accessed.
Password	Clear text passwords seen on the network. **Click [open]** to view.

Tools and softwares used:

Wireshark and Netwitness Investigator

Lab 3:
Configuring a pfSense Firewall on the Server

1. Configure the physical connectivity of a firewall that protects a server.
2. Understand how Network Address Translation (NAT) allows access from the public to the private network.
3. Configure NAT using a pfSense firewall.
4. Configure WAN-side firewall rules to expose an internal (private) server.

Tools and softwares:

- pfSense Firewall

for natting we need to create the
virtual ip address first
the nat the existing ip wit the virtual ip
then add the rules according with the new virtual ip.

Lab 4:
Configuring a VPN Client for Secure File Transfers

1. Recognize and explain the differences between secure and non-secure file transfers.

2. Determine the password and content of non-secure file transfers.

3. Configure a Windows VPN client to work with a L2TP\IPsec server on a pfSense appliance.

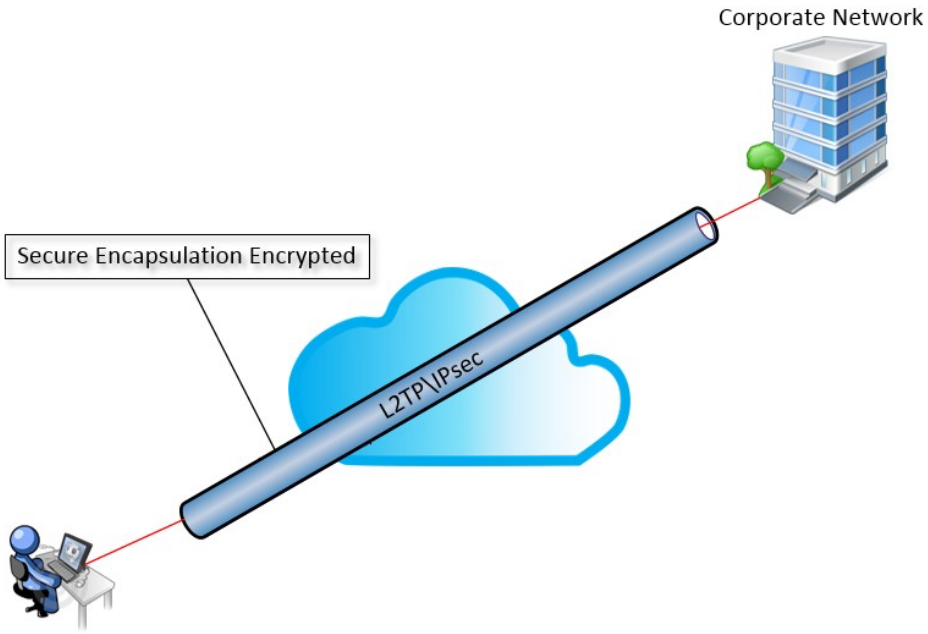
4. Describe the differences between non-tunneled and tunneled connections.

5. Discuss the roles and functions of encryption, authentication, and different elements of the IPSec protocol, such as ESP and AH.

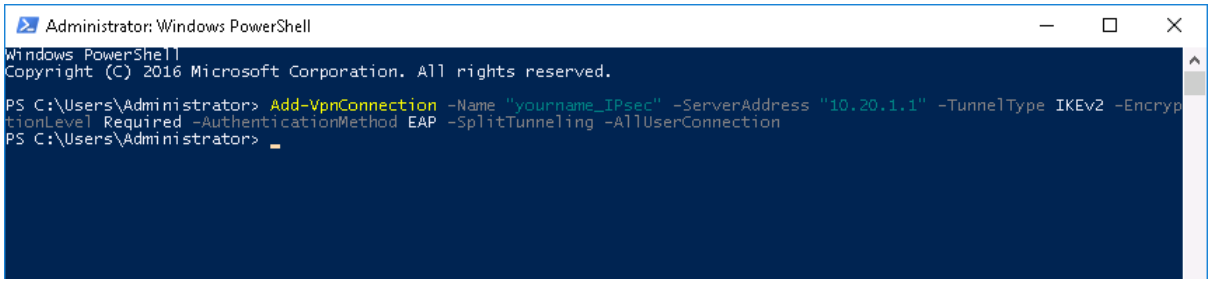
6. Explain different phases and modes of operation of the IPSec protocol.

In Part 1 of this lab, you will configure a VPN client on a Windows Server 2016 machine using IPsec to create a secure tunnel to a L2TP\IPsec server on a pfSense appliance. It is important to understand that L2TP (Layer 2 Tunneling Protocol) does not perform any encryption; it is strictly a tunneling protocol that will work on both an IP network and a non-IP network. IPsec and its policies provide the encryption that makes this tunnel secure. Remember, even though VPN tunnels are secure, they are not 100% secure or safe over the Internet. Your system is still vulnerable to inline attacks.

Because the client system may use a VPN to explore web sites on the Internet, the IP address of the VPN is visible to the target web site, while masking the actual client IP address. An inline attack is a code snippet that, when run, can reveal the actual location of the IP address of the client system. The following code snippet is an example of this type of attack.



For vpn encryption is not done just the tunnel is created
Who ever the user is need to install the certificate and there by user can connect to the vpn . always place the certificates in the trusted root directory.
At the command prompt, **execute** **`Add-VpnConnection -Name "yourname_IPsec" -ServerAddress "10.20.1.1" -TunnelType IKEv2 -EncryptionLevel Required -AuthenticationMethod EAP -SplitTunneling -AllUserConnection`**, replacing *yourname* with your own name, to add a VPN connection to the connection manager with specified parameters.



Tools and softwares:

- pfSense Firewall

Lab 5:

Configuring a Virtual Private Network Server

1. Configure the server side of a VPN.
2. Describe the advantages and disadvantages of different VPN configuration options.
3. Discuss how to prevent attacks against data in transit using a properly configured VPN.

Field Name	**Default values**
Generate TLS Key	This option will automatically generate the shared TLS authentication key.
TLS Shared Key	This field remains blank because the key is auto-generated in the previous field. If you chose to manually create a key, that key would be entered in this box and the Generate TLS Key would be left un-checked.
DH Parameters Length	The Diffie Hellman key exchange is used for establishing a secure communication channel. Originally conceptualize by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. The default value is 2048 bit.
Encryption Algorithm	The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side. The default value is AES-246-CBC (256-bit).
Auth Digest Algorithm	This method is used to authenticate traffic between endpoints. This setting must match on the client and server side. The default value is SHA1 (160-bit).
Hardware Crypto	The hardware cryptographic accelerator is used for the VPN connections. The default value is No Hardware Crypto Acceleration.

Tools and softwares:

- pfSense Firewall

Lab 6:
Securing the Network with an Intrusion Detection System (IDS)

1. Configure an open source intrusion prevention and detection system (IPS/IDS), Snort, on the TargetIDS virtual machine to detect a network-based attack

2. Configure an IDS monitoring tool, Snorby, to view alerting events on a running IDS system

3. Recognize IDS signatures and understand how scans appear as events in the IDS

4. Use scanning tools to attack the IDS virtual machine to trigger an alert

5. Document and describe the attacks detected and be able to identify false positives or remediation actions

Snorby is a web-based front-end to other applications, such as Snort. When Snort captures and examines IP packets, it does not save every IP packet. Rather, it is looking for specific IP packet traffic patterns and abnormal traffic attempting to enter a network. The IDS maintains logs and alerts and alarms when certain IP packet traffic patterns are identified inbound to the organization's network. Alerts or alarms can be automated to send information to a network or security operations help desk. Should you receive an IDS alert about a port scan detected from the same IP on a subnet, this is one of the first signs of a possibly compromised machine. An attacker may have remote access to a workstation and enabled a vulnerability assessment scan from within your organization. The results of his scan will be sent back to the attacker, unnoticed by your organization.

Nessus is a framework of several services and tools offering vulnerability scanning and management solutions. It is used to run tests against client computers using a database of known exploits and weaknesses.

There will be three severities medium, high and low

Tools and softwares:

- Nessus
- Snort
- Snorby
- vi Editor

Lab 7:

Recognizing Risks and Threats Associated with Emerging Technologies

1. Recognize the risks that social networking and peer-to-peer sites could introduce into an organization, and recommend hardening techniques to minimize exposure

2. Evaluate the risks associated with using mobile devices in an organization by analyzing all possible vectors and using best practices to mitigate the risk

3. Evaluate and recognize the security advantages and disadvantages of cloud and grid computing

4. Apply industry-specific best practices provided by the Cloud Security Alliance (CSA) and European Network and Information Security Agency (ENISA) to recognize and evaluate risk in cloud and grid computing

5. Provide a written analysis and report regarding hot security topics in emerging technologies, and create a strategy to maintain situational awareness of new security risks

Today's information security professionals face a daunting task. Not only do you need to understand how to secure a complex, diverse, and rapidly changing IT environment, but you also need to be aware of the risks and threats to come. Few of today's technologies were even in use 30 years ago. The fast pace of development means that faster, more innovative technologies spring up every day.Three emerging technologies that have gained prominence in recent years are cloud computing, social networking, and mobile applications. Cloud computing involves moving computing resources out to the Internet. Those resources are then shared by multiple applications. Mobile computing – from smartphones to tablets and beyond – extends office resources, including confidential or proprietary materials, into the field. Social networking websites are online communities designed for people with similar interests, or people pretending to have similar interests.

In this lab, you will explore risks, threats, and vulnerabilities inherent with cloud computing, social networking, and mobile computing. You will read the National Institute of Standards and Technology's (NIST) Definition of Cloud Computing and review the best practices put forth by the Cloud Security Alliance (CSA) and European Network and Information Security Agency (ENISA). You also will use your research to identify the security risks and recommended mitigations for each.

Tools and softwares: Oracle VM VirtualBox

VM labs: Vulnerability management

Lab 1:

Performing a Vulnerability Assessment

1. Identify risks, threats, and vulnerabilities in an IP network infrastructure using Zenmap to perform an IP host, port, and services scan

2. Perform a vulnerability assessment scan on a targeted IP subnetwork using Nessus

3. Compare the results of the Zenmap scan with a Nessus vulnerability assessment scan

4. Assess the findings of the vulnerability assessment scan and identify critical vulnerabilities

5. Make recommendations for mitigating the identified risks, threats, and vulnerabilities as described on the CVE database listing

Nmap, and its graphical user interface Zenmap, is the most popular tool used to perform an initial IP host discovery as well as port/services scan for the first part of the scanning and vulnerability assessment step of the hacking process. Nessus performs the second part of this hacking step, the vulnerability assessment. Nessus can assess Linux, Windows, and network infrastructures, and can perform a network discovery of devices, operating systems, applications, databases, and services running on those devices. Any known vulnerabilities or bugs will be flagged and identified by Nessus. These two tools work together to complete the scanning and vulnerability assessment phase of the ethical hacking process and lay the groundwork for the third phase (enumeration).

In this lab, you will use Nmap commands within the Zenmap application to scan the virtual network and identify the devices on the network and the operating systems and services running on them. You will also use Nessus to conduct a vulnerability assessment and record the high risk vulnerabilities identified by the tool. Finally, you will use the information you gathered from the report to discover mitigations for those risks and make mitigation recommendations based on your findings.

```
nmap -sn 172.30.0.0/24
```

This command will manually execute a Ping scan (-sn) on all hosts on the 172.30.0.0/24 subnet. The scan should find three hosts on the 172.30.0.0/24 subnet.

The Ping scan confirms that the machine is available, but can't identify ports, operating systems, or services. The host icon in the Host Details tab matches the

one in the OS column of the left pane. These icons indicate that the scan was unable to determine the operating system (OS) of the host.

`nmap -sS 172.30.0.0/24`

The SYN scan is a form of TCP scanning that is less intrusive to the target host. The scanner, Zenmap, can identify open ports without completing a TCP handshake, which might be noticed by network administrators.

Notice that the SYN scan can identify the services (e.g. FTP, HTTP, SSH, etc.), but not the versions of these applications. You will discover that information in a later step.

`nmap -O 172.30.0.0/24 Os scan`

to begin an OS fingerprinting scan and determine which operating systems (OS) are running on the network hosts.

`nmap -sV 172.30.0.0/24 Service Scan`

In the SYN scan from earlier in the lab, Zenmap identified the services running on the machines, but not the versions. This scan will discover the versions of the software on open TCP ports and will make a guess at the OS based on the services. As a result, the Service (–sV) scan can detect OS types better than the -O option and will take a little longer to run than the previous scans.

execute **`nmap -sT 172.30.0.0/24`** to run a TCP connect scan (-sT) on all hosts on the 172.30.0.0/24 subnet.

This scan will take several minutes to complete. A TCP connection scan takes longer to run because a connection is established with the target and can be run when a user does not have permission to use raw packets. Once complete, the scan should find three hosts on the 172.30.0.0/24 subnet.

Tools and softwares: Nessus Zenmap

Lab 2:
Analyzing Network Traffic to Create a Baseline Definition

1. Capture live network traffic with Wireshark and TCPdump
2. Analyze packet capture data in NetWitness Investigator
3. Use Wireshark statistics to identify baseline definitions
4. Identify common network protocols, such as HTTP, Telnet, FTP, TFTP, and SSH protocols, in a packet capture file
5. Discuss how network baseline definitions are created

Tools and softwares:

- Damn Vulnerable Web Application (DVWA)
- FileZilla
- NetWitness Investigator
- PuTTY
- TCPdump
- Tftpd64
- Wireshark

We will use TCPdump, a command line utility, to capture network traffic on the DVWA virtual server. You will generate that traffic by exploiting a cross-site scripting (XSS) vulnerability in the Damn Vulnerable Web Application (DVWA) tool.

type `tcpdump -i eth0 -n -w tcpdumpcapturefile` and **press Enter** to start the data capture.

type `tcpdump -n -r tcpdumpcapturefile | less` and **press Enter** to display the contents of the tcpdumpcapturefile file.

The pipe less command (| less) enables the user to use the arrow keys to cycle through the tcpdumpcapturefile log in smaller sections, one line at a time. To generate a pipe (|) character, press shift + backslash (\).

We can also simply used the grep command and find whatever we needed.

We can Transfer Files using Tftpd64 and FileZilla

Lab 3:

Penetration Testing a pfSense Firewall

1. Describe the steps of a penetration test.
2. Perform a penetration test against a system protected by a pfSense firewall.
3. Discuss measures that can be taken to harden a target against attacks while balancing system access and usability needs.

Penetration testing tests the strengths and weaknesses of an organization's IT security, as well as the readiness of the facility and/or employees to respond to an attack. Pen testing, as it is often called, can be as much of an art as it is a science. It can be done by security professionals who are part of the organization being tested, or it can be done by professionals hired by that organization to assure that its IT defenses are sound (at least as sound as reasonably possible) and consistent with policy, or it can be done by black-hat hackers (the bad guys) as a part of their targeting rituals. In many cases, pen testing is done by those clueless beginners—known as script kiddies—in their search for a great story to tell.

In this lab, you will examine the inbound (WAN) and outbound (LAN) firewall rules for a Windows network. You will use a popular automated tool, Nessus, to scan for threats that might expedite the beginning of the hacking process, and identify the logic and strategy behind the attack or attacks. You will modify the firewall rules to reduce or eliminate those vulnerabilities, and you will rescan the network to confirm that in closing those threats, you did not open others.

Every penetration tester has their own set of steps, but these all fall into the same general categories: network scanning, port scanning, vulnerability analysis, exploitation, and so on. For defenders, there is also a remediation step during which vulnerabilities are fixed and then the steps are repeated to ensure the attack can't occur again. For attackers, the last step is often an attempt to cover their tracks by destroying or modifying log files or other bits of forensic information that will prove that they were there.

Tools and softwares:

- pfSense Firewall
- Nessus
- Zenmap

Lab 4:

Attacking a Vulnerable Web Application and Database

1. Identify web application and web server backend database vulnerabilities as viable attack vectors

2. Develop an attack plan to compromise and exploit a website using cross-site scripting (XSS) against sample vulnerable web applications

3. Perform a manual cross-site scripting (XSS) attack against sample vulnerable web applications

4. Perform SQL injection attacks against sample vulnerable web applications with e-commerce data entry fields

Tools and softwares:

- Damn Vulnerable Web Application (DVWA)
- MySQL

Lab 5:

Exploiting Known Web Vulnerabilities on a Live Web Server

1. Evaluate the most common web vulnerabilities using the OWASP Top 10 and make recommendations based on best practices

2. Execute an HTML form brute force attack, and exploit a web application by issuing arbitrary commands through an HTML input form

3. Exploit a web application using cross-site request forgery (CSRF) and cross-site scripting (XSS) victimizing logged-in users to a web application in order to gain an understanding of how attackers exploit vulnerability and what countermeasures can be implemented

4. Compromise an SQL database for confidential data using an SQL injection and extract PII from a vulnerable backend

5. Obtain administrator access on a web application using file path injection and CSRF to understand the risks associated with allowing file uploads and dynamic file inclusion

6. the results of the SQL injection attempt;
7. the results of the command execution attempt;
8. the results of the file inclusion attempt;
9. the results of the successful file upload;
10. the results of the successful stored XSS attack;

Tools and softwares:

- Damn Vulnerable Web Application (DVWA)

Lab 6:
Investigating and Responding to Security Incidents

1. Use applications and tools to scan a Windows workstation for malware

2. Identify malware that has compromised the workstation
3. Isolate and quarantine the Windows workstation for incident response
4. Perform a security incident response on the Windows workstations and document, identify, isolate, and eradicate
5. Draft a security incident response report capturing your date/timestamps, findings, the steps taken, and the solutions for preventing a recurrence

Tools and softwares:

- AVG AntiVirus Business Edition

Lab 7:

Conducting an Incident Response for a Suspicious Login

1. Identify suspect login credentials from an FTP packet trace

2. Evaluate information that would be useful to an attacker who has infiltrated the network

3. Analyze the digital portion of a forensic investigation and link the two pieces of evidence together to solidify your case

4. Bookmark and export suspect data

5. Create a report detailing findings based on automated reporting of evidence related to a suspect's email communications, identified email attachments, and the protocol capture of the FTP session

The Service Type report includes information about each attempt. Notice that only one attempt included a successful file transfer. A lower rate of attempts followed by a successful logon usually means the user has the password for the account. Several attempts could point toward a brute force attack.s

Tools and softwares:

- NetWitness Investigator
- Paraben's E3

NetWitness Investigator can analyze the file name, size, the user name and password of the sender, the sender's IP address, and more. Passwords are visible in the FTP data because FTP traffic travels in cleartext, which makes it easy to capture by using a packet sniffer. More secure options include SFTP (Secure FTP) which uses the SSH (Secure Shell) protocol to transfer files in an encrypted fashion.

Lab 8:

Investigating and Responding to Network Security Incidents

1. Use system administration tools to gather information.

2. Scan a computer system for vulnerabilities using automated tools.

3. Explain the use of automated tools to gather information as part of an incident response process.

Tools and softwares:

- Windows Task Manager
- Windows Computer Management
- Microsoft Baseline Security Analyzer

Lab 9:

Performing a Post-Mortem Review of a Data Breach Incident

1. Analyze web traffic in real time using tcpdump to capture traffic as it happens on the network, and identify attack traffic

2. Identify potentially malicious activity and Brute Force attempts in Apache web logs to determine if an attack was successful on a given target

3. Dissect the header information in a HTTP request to determine whether a particular request is undesirable or a normal and expected HTTP session

4. Analyze web traffic using a web analytics tool (Webalizer) to identify website visitors and other statistics gathered from a web log file

5. Use and leverage Internet-based tools and research commercial web analysis tools to identify which is most appropriate for different business needs

Tools and softwares:

- Damn Vulnerable Web Application (DVWA)
- Live HTTP headers
- PuTTY
- Tcpdump
- Webalizer
- Webtrends Infinity Analytics
- Wireshark

type `ifconfig eth1 promisc` and **press Enter** to set the eth1 interface card to promiscuous mode, which will allow packet capturing.In the next steps, you will review the web server logs using Webalizer, a web-based tool that parses the log files to easily extract information about a variety of usage statistics. You will also review the server logs from the command line and compare the results from the two methods.

type `webalizer` and **press Enter** to process the most recent web traffic logs with the Webalizer tool.When the Webalizer script is executed, web server log files are processed into the Webalizer database. These log files can now be interpreted in easy-to-read HTML format. The data is summarized as the web site to which the stats are applicable, the summary period, and the time last processed.