LEVEL 5

Network Security and Cryptography

Student Guide

Modification History

Version	Date	Revision Description
V1.0	March 2024	For release

Published by: NCC Education Limited, Adamson House, Towers Business Park, Wilmslow Road, Didsbury, Manchester M20 2EZ, UK.

Tel: +44 (0) 161 438 6200 Fax: +44 (0) 161 438 6240 Email: info@nccedu.com
http://www.nccedu.com

CONTENTS

1. Unit Overview and Objectives

This unit introduces the fundamental concepts of network security and cryptography. It covers the principles, techniques, and best practices used to secure data and communication in modern computer networks. This unit will also introduce a range of well-known techniques and applications in network security, such as cryptography, hash functions, user authentication, access control, firewall, VPN, internet and wireless security, etc.

At the end of the unit, students should be able to:

1. Demonstrate a systematic and thorough understanding of the concept of Network Security and Cryptography.
2. Understand the vulnerabilities and systematically evaluate the security risks in networks.
3. Understand the analytical techniques and software tools to effectively secure networks.
4. Understand the security protocols in different domains such as web, internet, wireless.
5. Explain the concepts of Information Security and explain good practice in achieving security.

2. Learning Outcomes and Assessment Criteria

Learning Outcomes The Learner will:	**Assessment Criteria** The Learner can:
1. Demonstrate a systematic understanding of the concept of Network Security and Cryptography	1.1 Explain the concept of Network Security and Cryptography along with the relationship among two. 1.2 Explain the components and approaches of Network Security. 1.3 Understand the need and applications of network security and cryptography.
2 Critically evaluate the suitability of different Cryptographic Algorithms	2.1 Demonstrate the evolution of cryptographic algorithms and the need in modern networks. 2.2 Identify different types of cryptographic algorithms. 2.3 Demonstrate a systematic awareness of the theoretical foundations on cryptoanalysis.
3 Understand the vulnerabilities and systematically evaluate the security risks in networks	3.1 Understand the security risks in different components of networks. 3.2 Demonstrate a systematic awareness on different types of attack on the network systems.
4 Critically analyse appropriate tool and techniques for network security.	4.1 Understand and evaluate a range of modern security techniques and defence mechanisms. 4.2 Systematically evaluate the suitability of different network security techniques for different types of networks. 4.3 Make use of cutting-edge tools and technologies to provide network security.
5 Understand the wireless network security and associated protocols	5.1 Explain the vulnerabilities inherent in wireless networks. 5.2 Understand the wireless network infrastructure and the associated security protocols. 5.3 Evaluate and identify different types of wireless security methods and tools.

6 Explain the concepts of Information Security and explain good practice in achieving security	6.1 Critically analyse and prioritize information security risks. 6.2 Systematically identify countermeasures and review techniques appropriate to the management of information security risks. 6.3 Demonstrate a thorough understanding of the policy and technology trade-offs involved in developing information security systems of adequate quality. 6.4 Analyse and evaluate the significance of legal regulations and requirements on information security systems.

3. Syllabus

Syllabus			
Topic No	Title	Proportion	Content
1	Network Security and Cryptography Fundamentals	1/12 2 hours of lectures 3 hours of tutorials	• What is Network Security? • Principles of network Security • Model for Network Security • Approaches of Network Security • Introduction to Cryptography • Cryptography Fundamentals ***Learning Outcome: 1***
2	Cryptography Techniques	1/12 2 hours of lectures 3 hours of tutorials	• Classical Cryptography • Symmetric Key Cryptography ***Learning Outcome: 1,2***
3	Cryptography Techniques	1/12 2 hours of lectures 3 hours of lab	• Asymmetric Key Cryptography • Hash Function/digital signatures • Message Authentication Code ***Learning Outcome: 2,3***
4	Operating System Security and Vulnerabilities	1/12 2 hours of lectures 3 hours of lab	• Operating System Security basics • User Authentication • Unix Access Control ***Learning Outcome: 3***
5	Software Vulnerabilities and attacks	1/12 2 hours of lectures 3 hours of tutorials	• Software vulnerabilities: Input validation, Race conditions, Buffer overflows, etc. • Malwares • Worms ***Learning Outcome: 3***

6	Network Security and Defence	1/12 2 hours of lectures 3 hours of lab	• Why Network Security • Common Network Security Attacks • Internet Security ***Learning Outcome: 1,4***
7	Email and Web Security	1/12 2 hours of lectures 3 hours of tutorials	• Email Security, S/MIME • Web security considerations, • DNS security ***Learning Outcome: 4***
8	Firewalls	1/12 2 hours of lectures 3 hours of lab	• Why Firewall • Types of Firewalls • Bastion Host • Intrusion Detection and Prevention ***Learning Outcome: 4***
9	VLAN and VPN	1/12 2 hours of lectures 3 hours of tutorials	• Introduction to VLAN • VLAN Tagging • Introduction to VPN • Types of VPN • VPN protocols ***Learning Outcome: 4***
10	Wireless Security	1/12 2 hours of lectures 3 hours of tutorials	• Introduction to Wireless Networks • Wireless security (WEP, WPA, WPA2) ***Learning Outcome: 1,5***
11	Information Security Management	1/12 2 hours of lectures 3 hours of tutorials	• Information Security: Overview, culture, and governance • Legal Regulation and Compliance • Risk Management ***Learning Outcome: 6***
12	Unit Summary	1/12 3 hours of lectures 2 hours of tutorials	***Learning Outcome: ALL***

4. Related National Occupational Standards

The UK National Occupational Standards describe the skills that professionals are expected to demonstrate in their jobs in order to carry them out effectively. They are developed by employers and this information can be helpful in explaining the practical skills that students have covered in this unit.

Related National Occupational Standards (NOS)
Sector Subject Area: ICT Practitioners **Related NOS:** TECIS1201401, TECIS1201402, TECIS1201403, TECIS1201404, TECIS1201405, TECIS1201501

5. Resources

Lecturer Guide: This guide contains notes for lecturers on the organisation of each topic, and suggested use of the resources. It also contains all of the suggested exercises and model answers.

PowerPoint Slides: These are presented for each topic for use in the lectures. They contain many examples which can be used to explain the key concepts. Handout versions of the slides are also available; it is recommended that these are distributed to students for revision purposes as it is important that students learn to take their own notes during lectures.

Student Guide: This contains the topic overviews and all of the suggested exercises. Each student will need access to this and should bring it to all of the taught hours for the unit.

5.1 Additional Hardware and Software Requirements

Hardware: N/A

Software: Linux System, Cyber Ciege (free open source – education version), firewall visualization tool (free open source)

6. Pedagogic Approach

Suggested Learning Hours						
Guided Learning Hours				Assessment	Private Study	Total
Lecture	Tutorial	Seminar	Laboratory			
25	23	-	12	43	97	200

The teacher-led time for this unit is comprised of lectures, laboratory sessions and tutorials. The breakdown of the hours is also given at the start of each topic, with 5 hours of contact time per topic.

6.1 Lectures

Lectures are designed to introduce students to each topic; PowerPoint slides are presented for use during these sessions. Students should also be encouraged to be active during this time and to discuss and/or practice the concepts covered. Lecturers should encourage active participation and field questions wherever possible.

6.2 Tutorials

Tutorials provide tasks to involve group work, investigation and independent learning for certain topics. The details of these tasks are provided in this guide and also in the Student Guide. They are also designed to deal with the questions arising from the lectures, laboratory sessions and private study sessions.

6.3 Laboratory Sessions

During these sessions, students are required to work through practical tutorials and various exercises. The details of these are provided in this guide and also in the Student Guide. Some sessions will require more support than others as well as IT resources. More detail is given in this guide.

6.4 Private Study

In addition to the taught portion of the unit, students will also be expected to undertake private study. Exercises are provided in the Student Guide for students to complete during this time. Teachers will need to set deadlines for the completion of this work. These should ideally be before the tutorial session for each topic, when Private Study Exercises are usually reviewed.

7. Assessment

This unit will be assessed by means of an assignment worth 50% of the total mark and an examination worth 50%of the total mark These assessments will cover the learning outcomes and assessment criteria given above. Sample assessments are available through the NCC Education Virtual Learning Environment (http://vle.nccedu.com/login/index.php) for your reference.

8. Further Reading List

A selection of sources of further reading around the content of this unit must be available in your Accredited Partner Centre's library. The following list provides suggestions of some suitable sources:

- BSI, 2013. PAS555:2013 Cyber Security risk- Governance and Management Specification, London: BSI.
- CALDER, A. & WATKINS, S. 2015. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Ely: IT Governance.
- CHARLES J. B., Christopher G., Philip C., Donald S. 2018. Cybersecurity Essentials, John Wiley & Sons, Inc.
- CIAMPA, M. (2012). Security+ guide to network security fundamentals. Cengage Learning.
- HOFFMAN, A. 2020. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly.
- OZKAYA, E. 2019. Cybersecurity: The Beginner's Guide. Packet Publishing Ltd.
- QUINN, M. 2006. Ethics for the Information Age. Boston MA: Pearson.
- SILBERSCHATZ, A., PETER B. G. AND GAGNE, G. (2010). Operating system concepts. Hoboken: John Wiley & Sons.
- STALLINGS, W. 2022. Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition, Pearson.
- TANENBAUM, A. AND BOS, H. (2023). Modern Operating Systems, Global Edition. Pearson.

Topic 1: Network Security and Cryptography Fundamentals

1.1 Learning Objectives

This topic provides an overview of Network Security and Cryptography. The detailed introduction of network security, different network models and corresponding attacks will be discussed. The topic covers the fundamental concepts of cryptography as well.

On completion of the topic, students will be able to:

- Demonstrate a systematic understanding of the concept of network security and cryptography.
- Understand the principle and model of network security.
- Identify different approaches for network security.
- Understand the role of cryptography in network security.

1.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

1.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Tutorials:	3 hours

1.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- What is Network Security?
- Principles of Network Security
- Model for Network Security
- Approaches of Network Security
- Introduction to Cryptography
- Cryptography Fundamentals

1.5 Tutorial Sessions

The time allocation for this topic is 3 hours.

Look at below scenarios and identify the possible attack such as DoS, DDoS, MAC spoofing, DNS poisoning, session hijacking attack, SYN flood attack, phishing attack, ARP spoofing attack, SQL injection attack, XSS attack, IP spoofing, Code injection, Buffer overflow attack.

Scenario 1
While browsing the internet, a student keeps receiving annoying pop-up advertisements promoting suspicious software downloads.

Scenario 2
During a critical online exam, several students report that they cannot access the exam platform. The network team confirms that no maintenance or scheduled outage was planned.

Scenario 3
A student visits a local non-profit organization's website and finds that the homepage has been replaced with a message from hackers expressing their views.

Scenario 4
A student attempts to log in to their university's online portal, but they receive an error message stating that their account is already logged in from a different location.

Scenario 5
A student accesses their favourite online shopping website, but the browser redirects them to an unfamiliar website promoting suspicious products.

Scenario 6
A student receives an email from a colleague with an attachment that claims to be an urgent report. However, the email address seems slightly different from the colleague's usual email address.

Scenario 7
A student notices unusually high network traffic on the organization's LAN during non-peak hours. The network seems sluggish, affecting both internet access and local file sharing.

1.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Activity: Individual Case- Study Report (700 words)
Look up the infographic in given link below and choose an information security incident that was in the news in the recent years, one that catches your attention. Study the incident. You may search the internet for further information about the incident. You may have to refer to lecture slides to understand the security terms.

Make sure to include the following elements in your report:

- What was the incident about?
- What was the cause of the incident?
- What was the impact of the incident?
- Don’t forget to discuss any vulnerabilities, threats, and risks that may have been involved.
- What were the actions that were taken in response to the incident?

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Topic 2: Cryptographic Techniques

2.1 Learning Objectives

This topic provides an overview of cryptographic techniques. The detailed introduction on symmetric cryptography including both classic and modern techniques will be discussed. The topic covers the role of secret key in symmetric cryptography and introduce different cryptographic algorithms such as Caesar cipher, block cipher, and stream ciphers.

On completion of the topic, students will be able to:

- Demonstrate a systematic understanding of the concept of cryptography.
- Understand different classic cryptographic techniques.
- Understand the modern symmetric key encryption principles.
- Understand in detail different symmetric cryptography algorithms.

2.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

2.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Tutorials:	3 hours

2.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Classical Symmetric Cryptography
- Modern Symmetric Cryptography

2.5 Tutorial Sessions

The time allocation for this topic is 3 hours.

Exercise 1: Caesar Ciphers

Caesar ciphers are among the simplest devised and rely solely on remapping characters to others in the alphabet using a constant shift modulo the size of the alphabet. The amount shifted is the key used to encipher, or decipher, the message. This remapping is usually restricted to letters, so that with a key of 3, `A' is replaced by `D', `B' by `E', ..., `X' by `A', `Y' by `B', and `Z' by `C'. Lower case letters are mapped in an identical way to give their upper lower-case replacements. Thus, here the key is an integer in the range 1 to 25 (note not 26 as there is no point replacing every `A' by an `A' etc.).

Task 1: Encrypt the following with key 3: “Caesar ciphers are simple”**.**

Task 2: Decrypt following cipher text: “M K O C K B M S Z R O B C K B O C S W Z V O**”.**

Exercise 2 – Symmetric Cyphers

Given the following alphabet:

A	00000	I	01000	Q	10000	Y	11000
B	00001	J	01001	R	10001	Z	11001
C	00010	K	01010	S	10010	Sp	11010
D	00011	L	01011	T	10011	,	11011
E	00100	M	01100	U	10100	.	11100
F	00101	N	01101	V	10101	-	11101
G	00110	O	01110	W	10110	!	11110
H	00111	P	01111	X	10111	$	11111

Task 1: Take the text “HI” and encrypt and decrypt it using the KeyStream “W”.

Task 2: Take the following text: HELLO
Encrypt and decrypt it – Using as a KeyStream the letter **V**:

Exercise 3
Task: Compare the features of Block and Stream Ciphers.

2.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Question 1:
What is symmetric cryptography? Explain the role of a secret key in symmetric encryption.

Question 2:
How is the secret key shared between two parties in symmetric cryptography? Discuss the challenges and best practices for secure key distribution and management. (Hint: Self-study the concept Pre-Shared Key (PSK), Key Distribution Centre (KDC), Diffie-Hellman Key Exchange, Public Key Infrastructure (PKI).

Question 3:
Discuss the importance of key length and entropy in ensuring security.

Question 4:
How does the avalanche effect contribute to the security of symmetric ciphers?

Question 5:
Describe various types of attacks on symmetric encryption, such as brute force, known-plaintext, and chosen-plaintext attacks.

Topic 3: Cryptographic Techniques

3.1 Learning Objectives

This topic provides an overview of cryptographic techniques. The detailed introduction on asymmetric cryptography will be discussed. The topic covers the role of hash functions and message authentication code as well in security.

On completion of the topic, students will be able to:

- Demonstrate a systematic understanding of the concept of cryptography.
- Understand the asymmetric key encryption principles.
- Understand in detail hash function and message authentication code.

3.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

3.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Laboratory:	3 hours

3.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Asymmetric Cryptography
- Hash Function/digital signatures
- Message Authentication Code

3.5 Laboratory Sessions

The time allocation for this topic is 3 hours.

In this practical we will do some exercises on symmetric and asymmetric encryption using OpenSSL and Linux (Preferably Kali Linux 2021). It is probably unlikely that students are familiar with Linux, and it would be useful to direct them to a basic tutorial at the start. It would also be useful to explain the purpose of Kali Linux and an overview of the tool categories. You can share the below resources if needed:

1. https://www.youtube.com/watch?v=psyDZ9ytlwc&ab_channel=Simplilearn
2. https://www.youtube.com/watch?v=sW0lQRl5nEE&ab_channel=Simplilearn

There is no need for answers to this lab. The step-by-step guide in included for the students. The lecturer is expected to help students if they get stuck at some point.

Lab 3: Cryptography with OpenSSL

In this practical we will do some exercises on symmetric and asymmetric encryption using OpenSSLand Linux (Preferably Kali Linux 2021).

Install OpenSSL in your Linux OS (either VM or not).

Please download the Kali Linux VirtualBox Image:

Official site: https://www.kali.org//get-kali/#kali-virtual-machines (scroll up a bit, and choose the VirtualBox VM on the right side)

The Password and Username of the Kali Linux downloaded from the web are both kali (default password: https://www.kali.org/docs/introduction/default-credentials/).

In Kali Linux 2021, OpenSSL has already been installed.

(Just in case you need installation in the future, you can give the command, but you don't need to do this for now: **sudo apt-get install openssl**)

Try some encryption/operations.

1. Create a file or download a file. E.g., creating new text file
   cat > test.txt
   Press Cntr +D when finish.

The commands below are working in the version 1.1.1 of OpenSSL. For the older commands: https://www.openssl.org/docs/man1.0.2/man1/openssl.html

2. Encrypt a file using triple DES in CBC mode using a prompted

   password: openssl des3 -salt -pbkdf2 -in test.txt -out test.des3

```
cat test.des3
```

3. Decrypt a file using triple DES in CBC mode using a prompted password:

   ```
   openssl des3 -d -salt -pbkdf2 -in test.des3 -out testdecrypteddes3
   ```

```
cat testdecrypteddes3
```

4. Encrypt some files with AES CBC mode:

   ```
   openssl aes-256-cbc -salt -pbkdf2 -in test.txt -out test.aes

   cat test.aes
   ```

5. Decrypt the files with AES CBC mode:

   ```
   openssl aes-256-cbc -d -salt -pbkdf2 -in test.aes -out testdecryptedaes
   ```

6. Encode a file in Base64 format:

   ```
   openssl base64 -in inputfile -out outputfile.b64
   cat outputfile.b64
   ```

   Decode

   ```
   openssl base64 -d -in outputfile.b64 -out decodedbase64

   cat decodedbase64
   ```

7. For RSA asymmetric encryption: Create a private key file (2048 bit length by default)

   ```
   openssl genrsa -out private.pem
   ```

8. Generate the public key file from the private key file

   ```
   openssl rsa -in private.pem -pubout -out public.pem
   ```

   You can share public.pem file with your mates or anyone who will then use that to encrypt a message for you.

9. *Encrypt a file using RSA public key*

   ```
   openssl rsautl -encrypt -inkey public.pem -pubin -in yourplaintextfile.txt -out encypted_file.txt
   ```

In the above command, you can add the option -oaep as well, which specifies the use of OAEP padding to increase security.

10. Decrypt with RSA private key

    openssl rsautl -decrypt -inkey private.pem -in encypted_file.txt -out clear_text_file.txt you may need to use -oaep option for decryption if you used that previously for encryption.

11. Try different algorithms (e.g., Blowfish, RC4-40 etc.). With openssl -help command you can see the full list of supported algorithms. Compare the chipertext file size of the different algorithms.

3.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Hash and Password Cracking

Note: The private study is divided into multiple parts that cover various aspects of hash and password cracking. Complete it in your private study time and ask tutor if you have any questions in the next session.

We will run Kali Linux 2021.3 in VirtualBox during this session.

The tool we use to crack the hashes:

We use the tool called **hashcat,** which is pre-installed in Kali linux**.**

Hashcat includes the following important features:

- multi-threaded
- supports several OSs based hashes (Linux, Windows and OSX)
- supports several algorithms (MD4, MD5, SHA1, DCC, NTLM, …)
- Dictionary and brute-force attack variants.

To check all the features and usage mode of the tool, provide the command:

hashcat -h

Dictionary attack

Kali linux by default contains several wordlists/dictionaries that we can use to perform cracking. You can navigate into the folder /usr/share/wordlists, and give the command **ls**
to list all the wordlists. Specifically:

```
cd /usr/share/wordlists

ls
```

Then, you can go inside the **dirb** folder, and give ls to find the **common.txt** dictionary file that we will use for cracking.

```
cd dirb

ls
```

To check the content of the common.txt file:

```
nano common.txt
```

To exit nano, Cntr + X.

Cracking MD5 password hashes

We will generate the MD5 hash for the password **apple** using the tool openssl. Then, the resulted password hash in stored inside the file passwordmd5.txt. Namely:
Open a new terminal and give this command.

```
echo -n apple | openssl md5 -binary | xxd -p > passwordmd5.txt
```

Command to crack the password hash:

```
sudo hashcat -m 0 -a 0 -o cracked.txt passwordmd5.txt /usr/share/wordlists/dirb/common.txt
```

Explanation:

-m 0 for choosing the type of hash we are cracking (MD5).

-a 0 is for choosing a dictionary attack. The following table summarise the modes:

```
 # | Mode
 ===+======
  0 | Straight
  1 | Combination
  3 | Brute-force
  6 | Hybrid Wordlist + Mask
  7 | Hybrid Mask + Wordlist
   ===+======
```

-o cracked.txt is the output file for the cracked passwords.

passwordmd5.txt is our input file of password MD5 hashes we want to crack.

/usr/share/wordlists/dirb/common.txt is the absolute path to the wordlist file we use for this dictionary attack. Note: In case of dictionary attack you can only crack the password if the password can be found in the wordlist file. Some tool supports a mode to combine the words and letters.

To read the cracked password, provide the command:

sudo cat cracked.txt

then provide the password **kali**.

Warning: If you receive an error saying, “no hashes loaded”, then this means that the password file contains a different format of hash compared to the cracking mode. E.g., if the password file contains SHA1 hash formats, but we want to crack for MD5. This error can also happen when the password files contain wrong hash format (due to characters such as space, hyphen, etc.)

Cracking SHA1 password hashes

Next, we will generate the SHA1 hash for the password **apple** using the tool openssl. Then, the resulted password hash in stored inside the file passwordsha1.txt. Namely:

echo -n **apple** | openssl sha1 -binary | xxd -p > passwordsha1.txt

We give the following command to crack (note that -m 100 is to choose cracking for the SHA1 algorithm).

sudo hashcat **-m 100 -a 0** -o crackedsha1.txt passwordsha1.txt /usr/share/wordlists/dirb/common.txt

To read the cracked password, provide the command:

sudo cat crackedsha1.txt

then provide the password **kali**.

Cracking SHA256 (SHA2-256) password hashes

echo -n apple | openssl sha256 > passwordsha256.txt
nano passwordsha256.txt
Then, delete the part “(stdin) = “ from the beginning of the row. Doing this, we want to only keep the hash.
Then, to save the file: Cntr + X and then Yes

To start cracking, provide the command (-m 1400 is to choose cracking for the SHA2-256 algorithm):

sudo hashcat **-m 1400** -a 0 -o crackedsha256.txt passwordsha256.txt /usr/share/wordlists/dirb/common.txt

To read the cracked password, provide the command:

sudo cat crackedsha256.txt

then provide the password kali.

Brute-force attack

We will generate the MD5 hash for the password **abcd** using the tool openssl. Then, the resulted password hash in stored inside the file passwordmd5brute.txt. Namely:

```
echo -n abcd | openssl md5 -binary | xxd -p > passwordmd5brute.txt
```

In case of brute force attack, we don’t have to provide the wordlist/dictionary we want to use to crack the password. In this case, all possible combinations will be checked, and it takes longer time and more computation overhead.

```
sudo hashcat -m 0 -a 3 -o crackedmd5brute.txt passwordmd5brute.txt
```

Topic 4: Operating System Security and Vulnerabilities

4.1 Learning Objectives

This topic provides an overview of OS Security and vulnerabilities. The detailed introduction on OS security basics will be covered. The topic covers the role of access Control and user authentication in OS security.

On completion of the topic, students will be able to:

- Understand the importance of securing the operating system.
- Explain the concept of user authentication and describe various authentication methods.
- Comprehend Unix file permissions (read, write, execute) for users, groups, and others.

4.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

4.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Laboratory:	3 hours

4.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Operating System Security basics
- User Authentication
- Unix Access Control

4.5 Laboratory Sessions

The time allocation for this topic is 3 hours.

In this practical we will do some exercises on Access Control using UNIX/Linux. They also require access to a suitable system, probably best as a VM. It is probably unlikely that students are familiar with Linux, and it would be useful to direct them to a basic tutorial at the start or give more explanation about the commands included in the lab. chmod and the coding of the access rights will need explaining.

There is no need for answers to this lab. The step-by-step guide in included for the students. The lecturer is expected to help students if they get stuck at some point.

Materials Needed:

- Unix-based operating system (e.g., Linux)
- Access to a terminal or command line interface
- Notepad or any text editor for documentation

Activity Steps:

1. User Authentication:

Task 1.1: Create User Accounts
Open the terminal and create two user accounts using the following commands:

```
sudo adduser user1
sudo adduser user2
```

Follow the prompts to set passwords for each user.

Task 1.2: Password Policies
Explore and set password policies for the created user accounts. Use the **passwd** command with appropriate options to enforce password complexity and expiration.

To view the current password policies for a user, you can use the **chage** command. For example, to check the password policies for "user1," run:

```
sudo chage -l user1
```

This command will display information about the password aging and expiration settings for the specified user.

Note the current settings.
Modify the password policies for user1**:** sudo **passwd --expire user1**
Check the password policies again: sudo **chage -l user1**

Explain what happened with the command sudo passwd --expire user1.

Task 1.3: Authentication Logs
View authentication logs to review login attempts:

```
sudo tail -n 20 /var/log/auth.log
```

Identify successful and failed login attempts.

Explain what happened with the above command.

2. Unix Access Control:

Task 2.1: File Permissions

Create a directory and a file inside it:

```
mkdir secure_data
touch secure_data/sensitive_file.txt
```

Set appropriate file permissions:

```
chmod 600 secure_data/sensitive_file.txt
```

Explain what happened with the command chmod

Task 2.2: User Groups

Create a new group and add user1 to that group:

```
sudo groupadd secure_group
sudo usermod -aG secure_group user1
```

Change the group ownership of the "secure_data" directory:

```
sudo chown :secure_group secure_data
```

Explain what happened with the above commands.

Task 2.3: Access Control Lists (ACL)

Enable ACL on the "secure_data" directory:

```
sudo setfacl -m u:user2:rw secure_data
```

Explain what happened with the above commands.

4.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Q1. What are the key components of an operating system, and how do they contribute to the system's functionality?

Q2. Describe two authentication techniques other than passwords. Explain their strengths and potential weaknesses.

Q3. What is password salting, and why is it crucial for password security? Provide a simple example.

Q4. Compare and contrast discretionary access control (DAC) and mandatory access control (MAC). Provide a practical example where each model might be suitable.

Q5. Explain what a dictionary attack is and how it differs from login spoofing. How can systems defend against these attacks?

Topic 5: Software Vulnerabilities and Attacks

5.1 Learning Objectives

This topic provides an overview of software security and vulnerabilities. The detailed introduction on software security vulnerabilities will be discussed. The topic covers the role of malware and worn in exploiting software vulnerabilities and present counter prevention measures.

On completion of the topic, students will be able to:

- Understand the importance of securing the software's.
- Explain the software vulnerabilities such as Input validation, Race conditions, Buffer overflows, etc.
- Understand the impact of Malware and Worms.
- Differentiate between different types of malwares and worms and understand prevention measures.

5.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

5.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Tutorials:	3 hours

5.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Software vulnerabilities
- Malwares
- Worms

5.5 Tutorial Sessions

The time allocation for this topic is 3 hours.

Q1. Why is input validation crucial for preventing security vulnerabilities?

Q2. How can buffer overflows lead to security vulnerabilities?

Q3. What are the risks associated with improper handling of format strings?

Q4. What is the role of penetration testing in security testing, and how does it complement other testing methods?

Q5. What is the purpose of locks or semaphores in concurrent programming, and how do they prevent race conditions?

Q6. What are the Risks Associated with Malware?

Q7. Describe how malware can cause system crashes and execute malicious code.

5.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Question 1:
In a web application, there is a form that takes user input for a search query. The application uses this input directly in a database query without proper validation. An attacker exploits this by entering a malicious SQL query.

Explain the potential security risks in this scenario and propose a mitigation strategy.

Question 2:
A legacy C application processes user input without proper bounds checking, leading to a buffer overflow vulnerability.

Describe the consequences of a buffer overflow in this scenario and suggest measures to address the vulnerability.

Question 3:
An application accepts a format string from a user to display log messages. The format string is not properly sanitized.

Explain the security risks associated with improper handling of the format string and propose a solution.

Question 4:
A financial application performs arithmetic operations on user account balances without proper checks for integer overflows.

Identify potential security risks associated with integer overflows in this context and suggest preventive measures.

Question 5:
A multi-threaded application processes transactions on a shared resource without proper synchronization mechanisms.

Describe the potential issues that may arise due to race conditions in this scenario and propose a solution.

Question 6:
In a ransomware attack scenario, describe the potential impact on a user's data and suggest preventive measures.

Question 7:
If a user's computer is infected with spyware, what sensitive information is at risk, and how can the user detect and remove the spyware?

Question 8:
A computer on a university network is infected with a self-replicating worm. Describe the potential consequences for the university network and suggest measures to contain and prevent the worm's spread.

Question 9:
A user receives an email with an attachment claiming to be a software update. The user unknowingly opens the attachment, leading to malware infection. Describe the potential impact on the user's computer and suggest steps for remediation and prevention.

Topic 6: Network Security and Defence

6.1 Learning Objectives

This topic provides an overview of network security. The detailed introduction on network security and attacks will be discussed. The topic covers the internet security protocols such as SSL and IPsec.

On completion of the topic, students will be able to:

- Understand the importance of network security.
- Identify common network security attacks.
- Understand the basic of internet security and the corresponding protocols.
- Discuss key concepts and best practices for securing the internet and networks.

6.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

6.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Laboratory:	3 hours

6.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Why Network Security
- Common Network Security Attacks
- Internet Security

6.5 Laboratory Session

The time allowance for tutorials in this topic is 3 hours.

In this practical we will do some exercises on network security.

There is no need for answers to this lab. The step-by-step guide is included for the students. The lecturer is expected to help students if they get stuck at some point. The exercise is based on CyberCIEGE, which is a useful introductory game. The web site states that ‘CyberCIEGE is available at no cost for educational institutions. To obtain a copy, send a request to: cyberciege@nps.edu. Student can download free as well.

REFER TO THE TOPIC 6 LAB EXERCISE GUIDE PROVIDED

6.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

The private study exercise is based on further enhancing students’ skills in Linux and how an attack plan and gather network parameters to foster attack. All the steps required to perform the exercise are included in the study manual.

The private study is divided into multiple parts that cover various aspects of network port scanning. There is no need for answers to this lab. The step-by-step guide in included for the students. The lecturer is expected to help students if they get stuck at some point in the next session.

Network Scanning/Reconnaissance

We will run Kali Linux 2021.3 in VirtualBox during this exercise.

In this exercise, we will do some reconnaissance exercises through network scanning. We will use the following two machines:

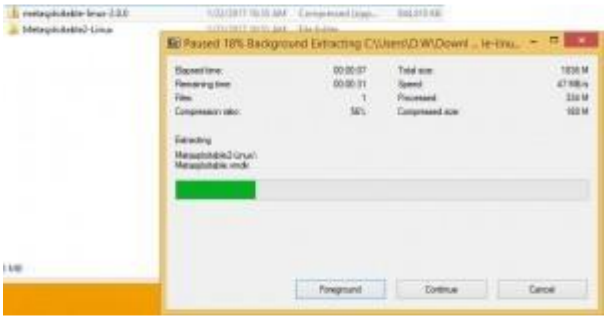
1. Kali Linux (our attacker machine) as done is topic 3,
2. (our victim/target machine), which is an intentionally vulnerable Linux OS designed for education purposes.

(You can also download Metasploitablev2 from https://sourceforge.net/projects/metasploitable/)

To launch Metasploitable v2 in VirtualBox, following the guideline below (ref: https://www.wikigain.com/download-install-metasploitable-in-virtualbox/):

Download and unzip it.

1. Extract the Metasploitable file.



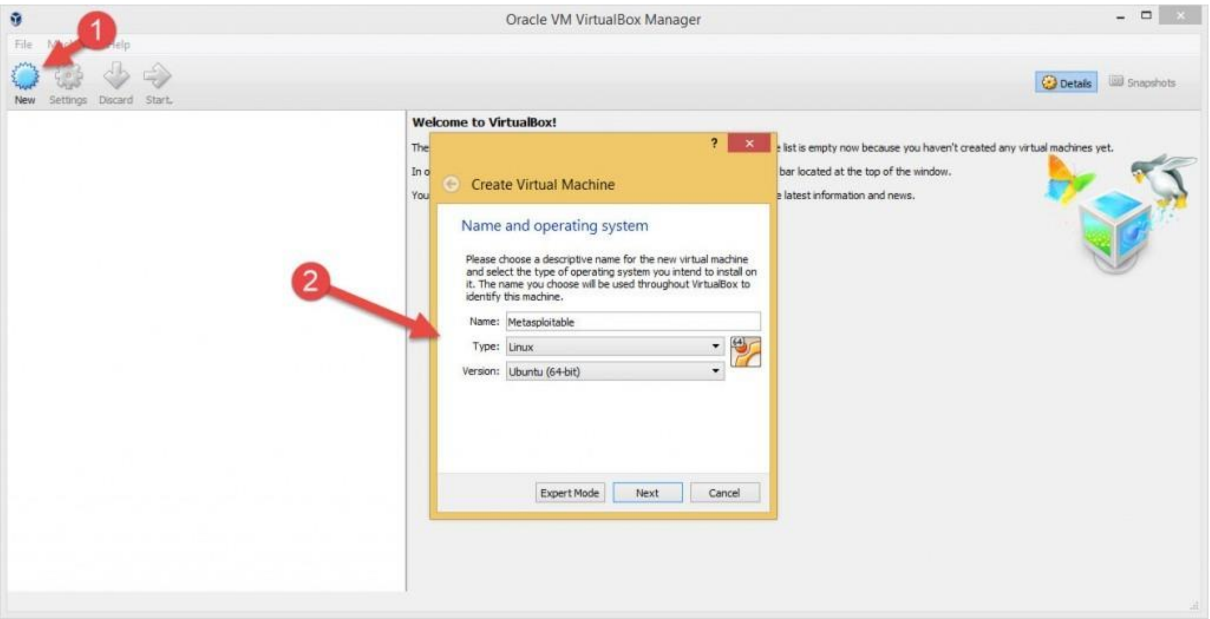
Paused 18% Background Extracting C:\Users\D.W\Downl ... le-linu...

Elapsed time: 00:00:07 Total size: 1836 M
Remaining time: 00:00:31 Speed: 47 MB/s
Files: 1 Processed: 334 M
Compression ratio: 56% Compressed size: 183 M

Extracting
Metasploitable2-Linux\Metasploitable.vmdk

Extract The File

2. Open the Virtual Box and click the new button on the top right side of your Virtual Box. On the first option, write Metasploitable and select Kali Linux in the second option and click Next and go forward.



Welcome to VirtualBox!

The … list is empty now because you haven't created any virtual machines yet.

In o… bar located at the top of the window.

You… latest information and news.

Create Virtual Machine

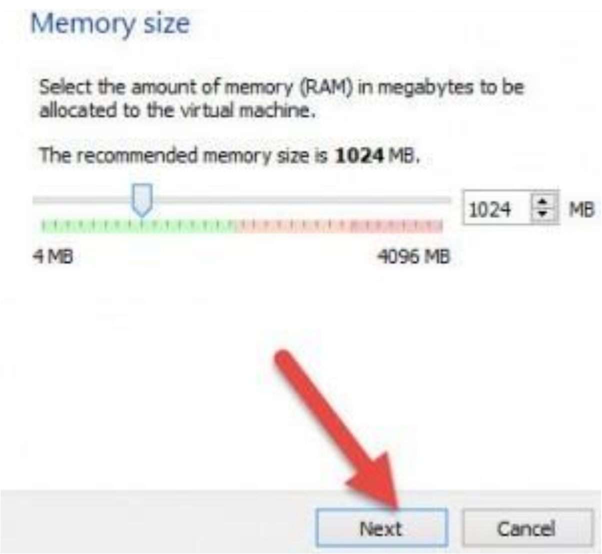
Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Metasploitable
Type: Linux
Version: Ubuntu (64-bit)

Click on a new button

3. After step 5, you will select the memory size (RAM). You can use it as default or give some extra and click on next then Create button.



Memory size

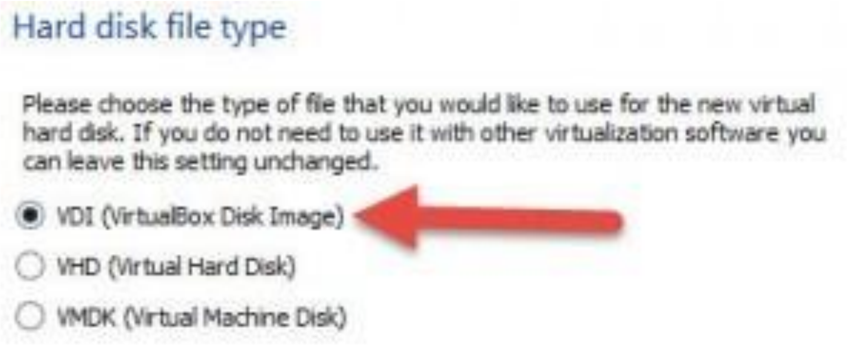
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

1024 MB

RAM Size

4. This step, you will select the type of your Hard disk, and it is VDI (Virtualbox Disk Image). After that, click on Next button and again click Next button.



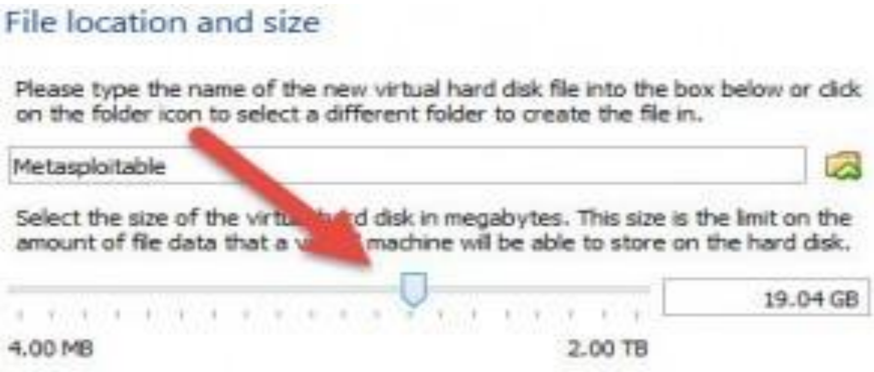
Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)

Select Hard disk type

5. Now you will select the Size and location of your Virtual machine.



File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

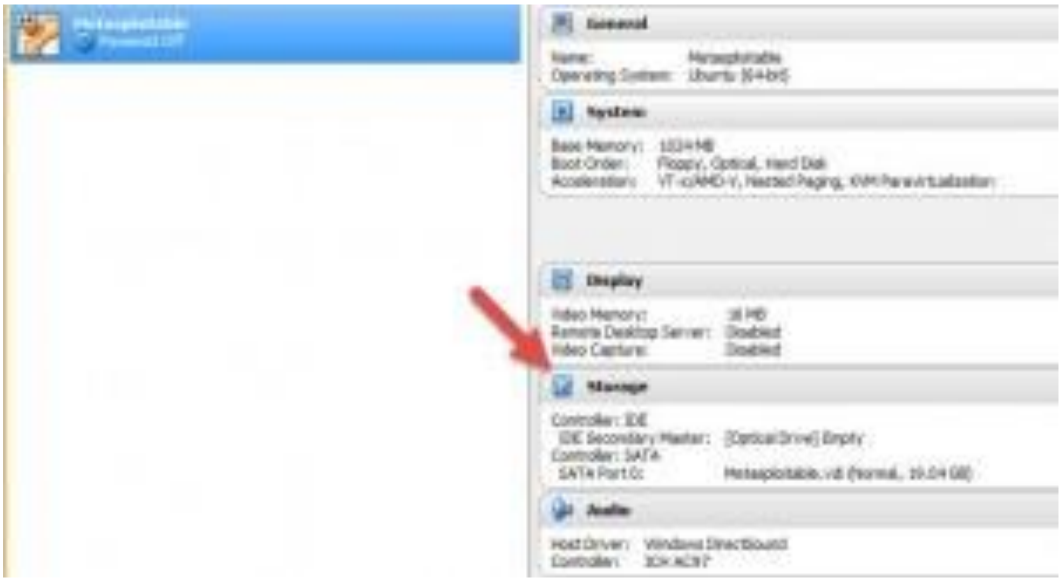
Metasploitable

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

19.04 GB

File Size and location

6. Now the settings are fixed up, and we have to select our downloaded OS, and for that, we must click on the Storage button as the picture below.



Metasploitable
Powered Off

General
Name: Metasploitable
Operating System: Ubuntu (64-bit)

System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

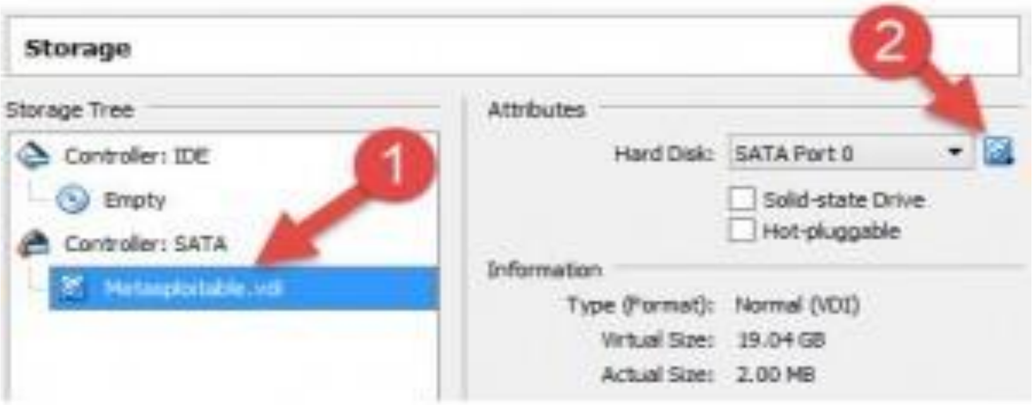
Display
Video Memory: 16 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vdi (Normal, 19.04 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

Click on the Storge

7. Click on the small hard disk on the top right of the dialogue box as the picture.



Storage

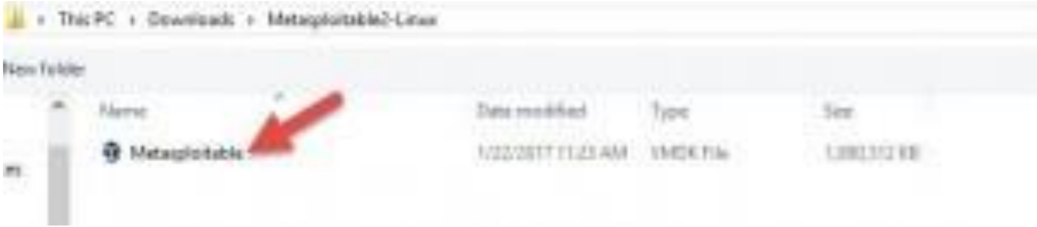
Storage Tree
- Controller: IDE
  - Empty
- Controller: SATA
  - Metasploitable.vdi

Attributes
Hard Disk: SATA Port 0
□ Solid-state Drive
□ Hot-pluggable

Information
Type (Format): Normal (VDI)
Virtual Size: 19.04 GB
Actual Size: 2.00 MB

Select Metasploitable

8. Now go the directory that Metasploitable is downloaded and select that.



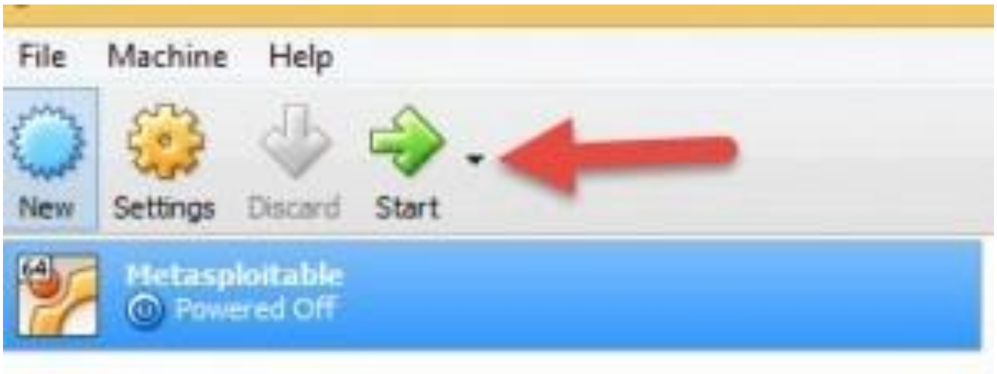
This PC › Downloads › Metasploitable2-Linux

New folder

Name | Date modified | Type | Size
Metasploitable | 1/22/2017 11:23 AM | VMDK File | [illegible] KB

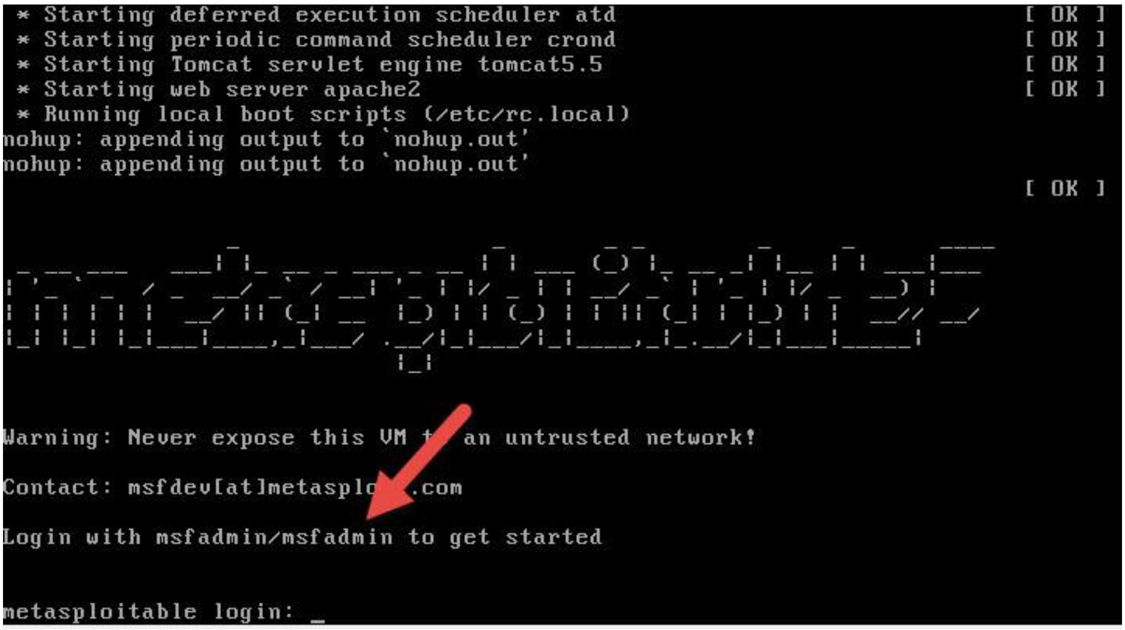
Select Metasploitable

9. It is finished, and you are ready to open.
10. Before you start the VM, go to Settings (yellow icon) and change the Network adapter 1 from NAT **to Host-only**. To do this, click on the “Network” option => Adapter1 tab => select **Host-only** (instead of the default NAT) => OK/Save.
11. To start the VM click the start button on the top right of the Virtualbox.



Click on the Start button

Note: – The password and the Username of the OS are msfadmin. And you can shut down it by writing power off and if you got any question or problem, do not hesitate to share with us. Install Metasploitable in VirtualBox.



```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

Login with the account/password = msfadmin/msfadmin

After starting the Metasploitable VM, you can now set the Network Adapter 1 of Kali Linux to Host-only (to put it in the same subnet like the Metaspolitable VM to communicate).

To do this, Under Settings in the Kali Linux VM, click on the “Network” option => Adapter1 tab => select **Host-only** (instead of the default NAT) => OK/Save.

Part I. Attacks

In the Metasploitable machine, provide the command.

ifconfig

Then, note down the IP address of this machine.

In the Kali Linux machine, open the terminal.

1. Ping the Metasploitable machine using the command.

   ping <IPaddress>   (replace <IPaddress> with the IP address of Metasploitable)

   See if you get any response (let tutor know if not).

By default, the firewall in the Metasploitable machine is disabled, so any scan attempt should be successful.

Let’s carry out some service/port scan with the tool called **nmap**:

1. Ping sweep: with this you will be able ping several devices at the same time in an automated way.

   sudo nmap -sP <Range of IP address> (replace <Range of IPaddresses> with the IP address range that contains the address of Metasploitable. E.g. if the address of Metasploit is 192.168.54.118, then the range can be 192.168.54.**1-255**, which defines the 255 IP addresses between 192.168.54.**1-**192.168.54.**255**)

2. Basic port/service scan. Give the command.

   sudo nmap <IPaddress> (replace <IPaddress> with the IP address of Metasploitable)

Observe and search on the web for the meaning of each open port. Create a table in MS Word where you note down all the open port as a result of this command. Follow the 3 column table format below:

Time	Command	Open ports/services/Results
9am-9:05am	**sudo nmap <IPaddress**>	…

3. Now we also want to scan for operating system/OS information:

   sudo nmap -O <IPaddress>

Again, add a new row to your logbook/table and complete the details (MAC address and OS info)

4. Now let’s do a scan on a particular port or port-range only:

   sudo nmap -p22 <IPaddress> (check if port 22/ssh service is open)

   sudo nmap -p1-100 <IPaddress> (check if ports between port 1 port 100 are open)

5. If you would like to see the details of the scan, you can give the command:
   Nmap **-d `--packet-trace` `-p22`** < **IPaddress** >

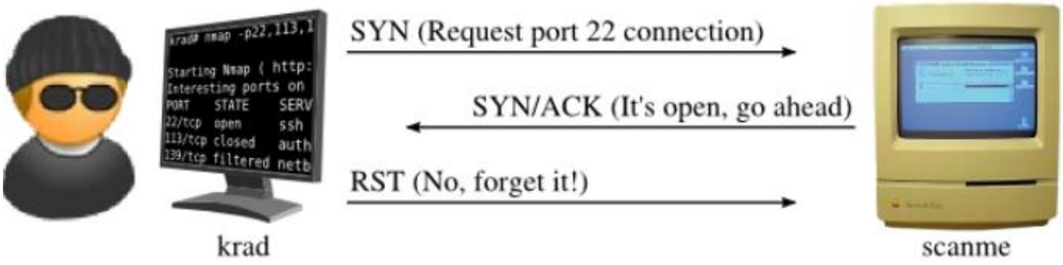
   Again, note down the results and observation in the table.

6. TCP SYN Stealth scan, by carry out the stealth scan, we want to avoid that the scan attempts are being logged at the victim’s side.

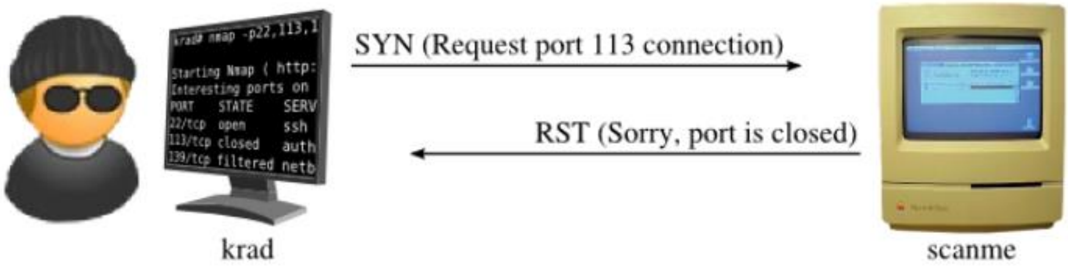
   nmap **-sS** <IPaddress> (Stealth, SYN scan)

   SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections.

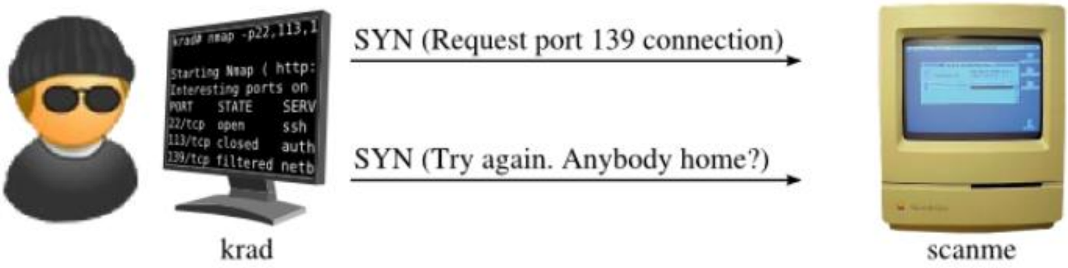
   Scan to discover open port 22:



   Scan to discover closed port 113:



   Scan to discover filtered (blocked by Firewall) port 139:

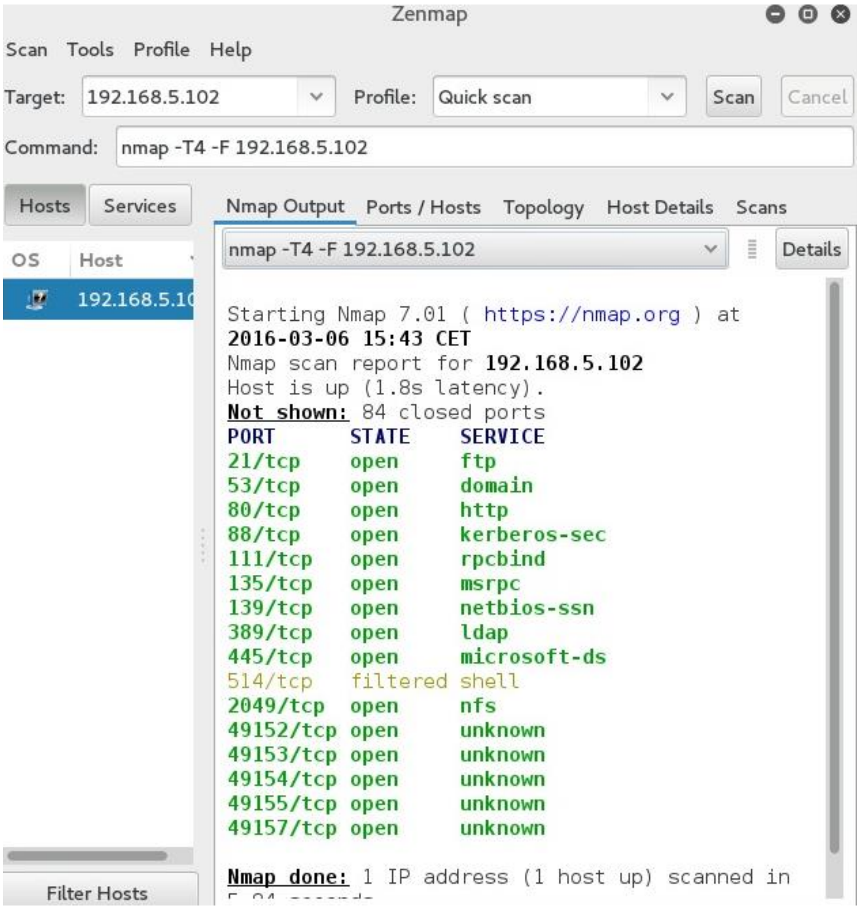

SYN (Request port 139 connection)
SYN (Try again. Anybody home?)
krad
scanme

Summary:

Probe Response	Assigned State
TCP SYN/ACK response	`open`
TCP RST response	`closed`
No response received (even after retransmissions)	`filtered`
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	`filtered`

Note: There is a graphical tool called Zenmap in Kali Linux that you can try to perform scan and get the result in a graphical window, instead of in command line.

You can open the search bar on Kali Linux (top left corner) and type Zenmap, the double click on the icon.



Target: 192.168.5.102

Profile: Quick scan

Command: nmap -T4 -F 192.168.5.102

```
nmap -T4 -F 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at
2016-03-06 15:43 CET
Nmap scan report for 192.168.5.102
Host is up (1.8s latency).
Not shown: 84 closed ports
PORT       STATE    SERVICE
21/tcp     open     ftp
53/tcp     open     domain
80/tcp     open     http
88/tcp     open     kerberos-sec
111/tcp    open     rpcbind
135/tcp    open     msrpc
139/tcp    open     netbios-ssn
389/tcp    open     ldap
445/tcp    open     microsoft-ds
514/tcp    filtered shell
2049/tcp   open     nfs
49152/tcp  open     unknown
49153/tcp  open     unknown
49154/tcp  open     unknown
49155/tcp  open     unknown
49157/tcp  open     unknown

Nmap done: 1 IP address (1 host up) scanned in
```

Part II. Defence:

As mentioned above, by default, the firewall in the Metasploitable machine is disabled, so any scan attempt was successful. Now, it's time to enable the firewall in the Metasploitable machine and see what happens if you carry out the above scans.

To enable to firewall, in Metaploitable, provide the command:

sudo ufw enable

Now, carry out some of the scans from the attack section above to see the differences.

Note down all observation for each command in the Table in the MS Word document that you created before. You should not be able to see open ports like before as the firewall blocks your scan attempts.

Part III. Bypassing Firewall Defence:

We will continue with the settings/configuration from the last part, with Kali Linux and Metasploitable. Make sure that you enable the firewall in Metasplotable VM using the command: **sudo ufw enable**

Nmap offers three approaches to bypass some firewall traffic filtering, and you will be able to see potential open ports behind the firewall.

1. FIN scan (-sF)

   How this works?

   1. An adversary sends TCP packets with the FIN flag but not associated with an existing connection to target ports.
   2. An adversary uses the response from the target to determine the port's state. If no response is received the port is open. If an RST packet is received, then the port is closed.

   The RFC 793 expected behaviour is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response.

   Commands:

   sudo nmap -sF -Pn -p80 IPaddress of target (check if the port 80 is open)

   sudo nmap -sF -Pn IPaddress of target (check which ports are open)

   Note down all observation for each command in the Table in the MS Word document that you created before. You should now see open ports despite the firewall is enabled at the victim.

2. NULL scan (-sN)

   This case, we do not set any bits (TCP flag header is 0) in the TCP header of the packets.

   sudo nmap -sN -Pn IPaddress of target

3. Xmas scan (-sX)

   This case, we set the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

   sudo nmap -sX -T4 IPaddress of target

4. If you want to allow ftp and ssh inbound traffic in the firewall ruleset, give the commands:

   sudo ufw allow **22/tcp** (or *sudo ufw allow* ssh)

   sudo ufw allow **21/tcp** (or *sudo ufw allow* ftp)

   sudo ufw allow **80/tcp** (or *sudo ufw allow* http)

   Once you allow these in the firewall ruleset, you can give the normal nmap command to see the open ports.

   sudo nmap IPaddressOFtarget.

Topic 7: Email and Web Security

7.1 Learning Objectives

This topic provides an overview of email and web security. The topic covers the different email and web security protocols. The role of DNS and the corresponding threats and preventions will be also covered.

On completion of the topic, students will be able to:

- Understand the importance of email security.
- Identify common web security consideration.
- Understand the basic of DNS security and corresponding protocols.
- Discuss key concepts and best practices for securing the internet and networks.

7.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

7.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Laboratory	3 hours

7.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Email security
- Web security
- Domain Name Server (DNS) security

7.5 Tutorial Sessions

The laboratory time allocation for this topic is 3 hours.

Q1. Explain why mail servers are often targeted by attackers.

Q2. What functionalities does PGP offer in terms of email security?

Q3. How does S/MIME contribute to email security?

Q4. What is DKIM, and how does it authenticate emails?

Q5. Name and briefly explain two common web threats and their potential impacts.

Q6. List three DNS security threats and briefly describe their potential impact.

Q7. Name three security measures to enhance DNS security and briefly explain each.

Q8. Outline three best practices for securing web applications against Cross-Site Scripting (XSS) attacks. Provide details on each practice.

7.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Q1. Explain the concept of key management in PGP. How does PGP handle issues relate to key distribution and revocation?

Q2. Compare and contrast the security features of S/MIME and PGP. In what scenarios would one be more suitable than the other?

Q3. Outline potential challenges in implementing DKIM on a large-scale email infrastructure. How can organizations overcome these challenges?

Q4. Provide advanced best practices for securing mail servers against sophisticated attacks. How can organizations defend against advanced persistent threats targeting email infrastructure?

Q5. If a user wants to send a confidential email using PGP, describe the steps they would take, including key generation and encryption.

Q6. A company receives an email claiming to be from a trusted partner. How can DKIM help verify the authenticity of this email, and what steps should the company take?

Q7. An organization falls victim to a DNS amplification attack, causing service disruptions. Explain how implementing DNS Response Rate Limiting (RRL) can mitigate this attack.

Q8. A web application has implemented input validation to prevent SQL injection attacks. Describe an advanced evasion technique that attackers might use to bypass input validation measures and suggest additional countermeasures.

Topic 8: Firewalls

8.1 Learning Objectives

This topic provides an overview of firewalls. The topic covers the different types of firewalls and characteristics of these firewalls. The role of bastion host and intrusion detection and prevention systems will be also covered.

On completion of the topic, students will be able to:

- Understand the importance of firewalls.
- Identify common firewall design consideration.
- Understand the basic of bastion host and corresponding methods such as honey pot etc.
- Discuss key concepts and best practices for securing the internet including intrusion detection and prevention measures.

8.2 Pedagogic Approach

Information will be transmitted to the students during the lecture. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

8.3 Timings

Lecture:	2 hours
Private Study:	8 hours
Laboratory:	3 hours

8.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Why Firewall
- Types of Firewalls
- Bastion Host
- Intrusion Detection and Prevention

8.5 Laboratory Sessions

The laboratory time allocation for this topic is 3 hours.

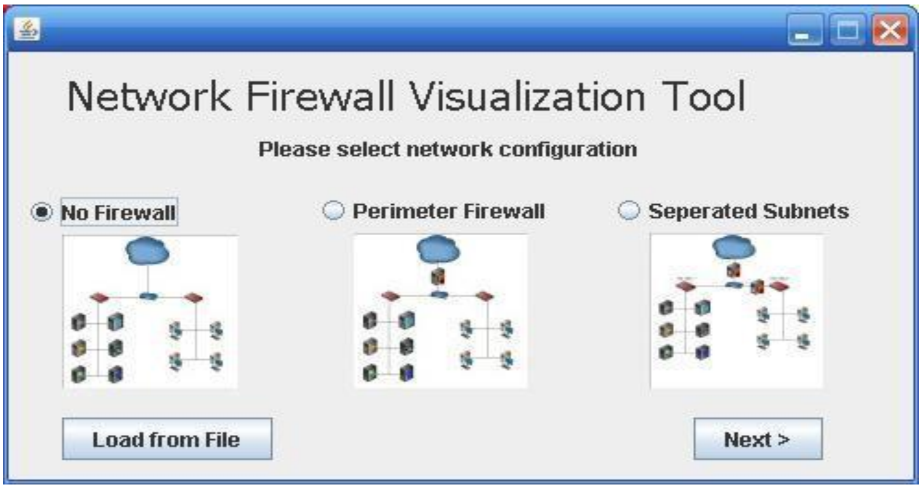
There is no need for answers to this lab. The step-by-step guide in included for the students. The lecturer is expected to help students if they get stuck at some point. Lab requires installation of a firewall visualization tool (written in Java) downloaded from KevinCurran's website (prof at University of Ulster). This requires java. His site contains many other useful and relevant resources and it would be beneficial to include them in the references.

Firewall Virtualization Tool Introduction

1. Start the Firewall program by downloading the visual tool.

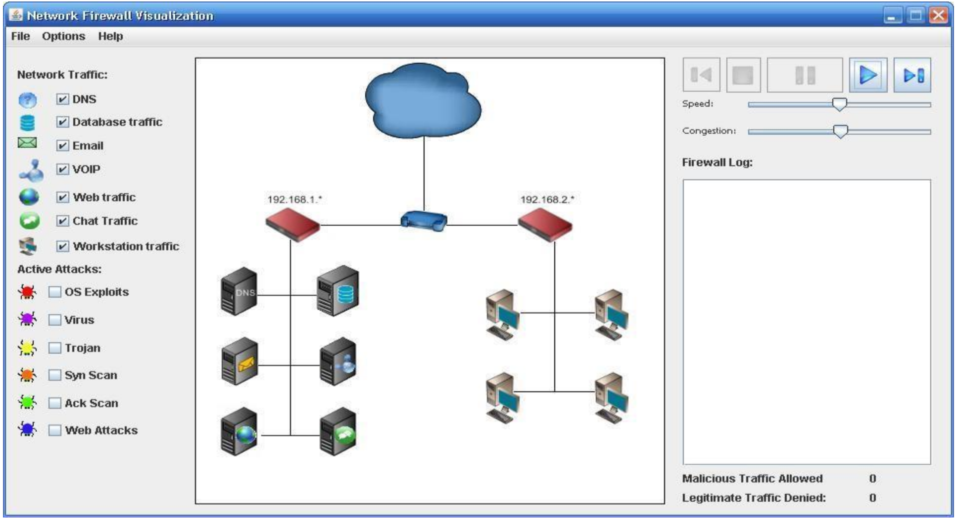
- https://kevincurran.org/com320/labs/Firewall/FirewallVisualizationTool.jar
- https://kevincurran.org/com320/labs/Firewall/FirewallWorkstationDataFile.dat

2. You should see a screen similar to the one below:


Network Firewall Visualization Tool
Please select network configuration
Load from File
Next >

● No Firewall ○ Perimeter Firewall ○ Seperated Subnets

Choose "**no firewall**" and click next. The following screen will appear:



Network Traffic:
☑ DNS
☑ Database traffic
☑ Email
☑ VOIP
☑ Web traffic
☑ Chat Traffic
☑ Workstation traffic

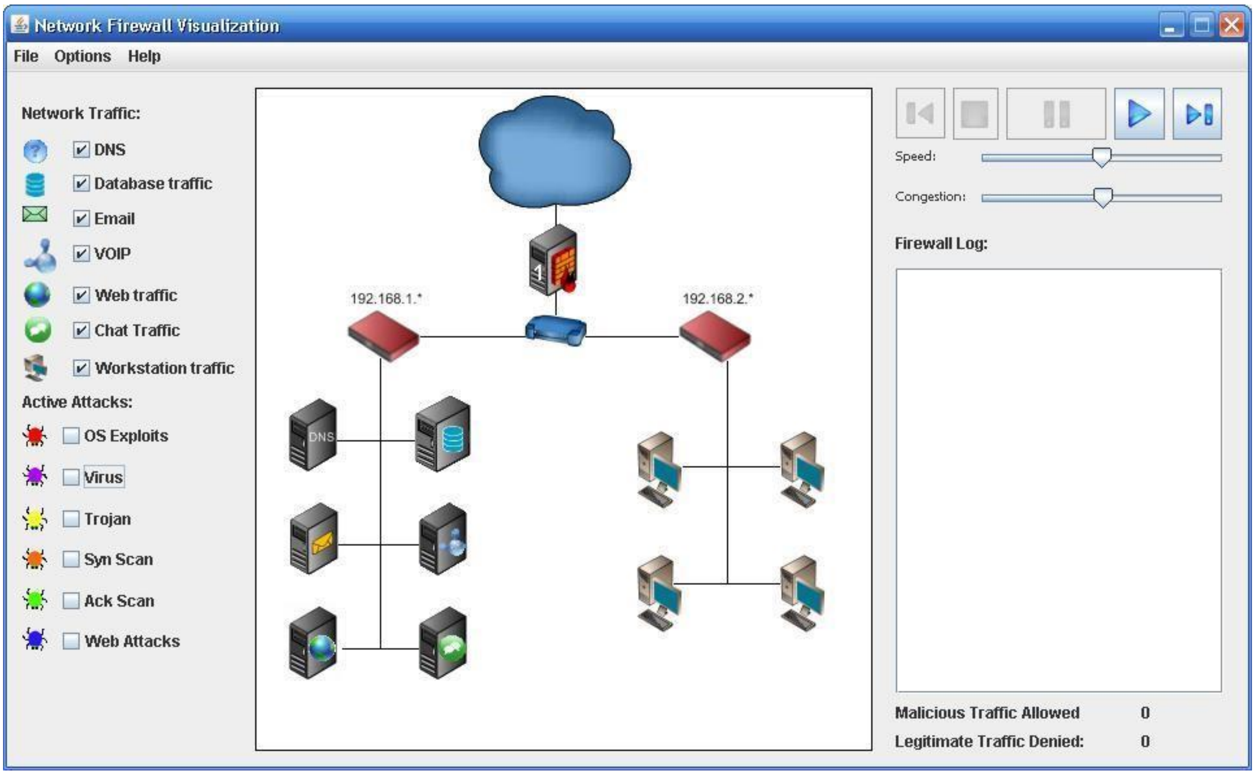
Active Attacks:
☐ OS Exploits
☐ Virus
☐ Trojan
☐ Syn Scan
☐ Ack Scan
☐ Web Attacks

Malicious Traffic Allowed 0
Legitimate Traffic Denied: 0

Click the ▷ button. Note that the traffic flows both from the "cloud" or internet to the client machines. By default, there is no malicious traffic flowing to the machines. Click on the *OS Exploit* option. Eventually, you'll see a similar red coloured bug flow from the internet into the local area network and land on a machine, infecting the machine. Once a machine is infected, it is marked as such with the "international No" emblem. Let us see how configuring a firewall will help prevent such infections.

Firewall Configuration.

1. Start a new session by clicking **File -> New** in the upper window of the tool. This time, choose the **Perimeter firewall**. The window that comes up will look like this:



Network Traffic:

- ☑ DNS
- ☑ Database traffic
- ☑ Email
- ☑ VOIP
- ☑ Web traffic
- ☑ Chat Traffic
- ☑ Workstation traffic

Active Attacks:

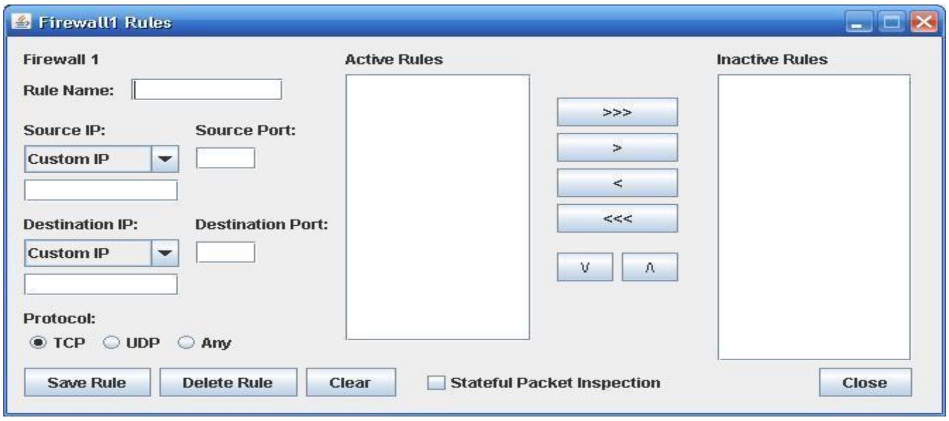
- □ OS Exploits
- □ Virus
- □ Trojan
- □ Syn Scan
- □ Ack Scan
- □ Web Attacks

Malicious Traffic Allowed	0
Legitimate Traffic Denied:	0

You now have a firewall between the internet (represented by a cloud) and your network router. Click the play ▷ button and watch what happens. **Do you see traffic flowing from the internet into your system or from your network to the internet? Explain why or why not:**

2. Add some active attacks by clicking on several different options.

3. Configure your firewall to allow traffic to flow in and out of your network. Do this by choosing the 'options' tab at the top of tool & define firewall rules. You should see a screen like below:



Source IP: Custom IP

Destination IP: Custom IP

Protocol: ● TCP ○ UDP ○ Any

Name your firewall rule (typically with a name that focuses on a given subject or attack). The "Source IP" option and port refer to how you want the firewall to recognize a given source IP/Port combination and respond. The Destination is similar but focusing on a destination rule. The goal of any good firewall configuration is to identify legitimate traffic while restricting malicious traffic. Try setting the following firewall rule:

Rule Name: DNS Rule
Source IP: DNS, Source Port: 53
Destination IP: Any, Destination port *
Protocol: Any.

Click "**Save Rule**". You should now see the rule in your Active Rules box. Click "close" and you should be back to your Network Firewall Visualization Tool window. Click the play button and watch what happens. You may need to move the speed bar to the right for a higher speed of traffic. Add some active attacks and watch if they flow through the firewall.

4. Download the **WorkstationDatabase** scenario from the above. It is called **FirewallWorkstationDataFile.dat**[1] and save it to your desktop. Choose **File -> new** to restart the program and click "**load from file**" button, pointing the program to the file you downloaded.

   https://kevincurran.org/com320/labs/Firewall/FirewallWorkstationDataFile.dat

   This scenario was configured so that workstations can pass through *firewall2* and gain access to the database. *Firewall1* has an ***allow all*** traffic rule set so all information is passed through to the network and from the network to the servers. Write rules to prevent active attacks from passing through *firewall 1* and attacking the database.
5. Would you claim your rule is now sufficient to allow traffic to flow for a typical network? Why or why not?
6. Do any of the active attacks now work against machines behind the firewall?
7. Create a rule to permit Email traffic to enter the network and check which of the active attack now work against machines behind the firewall?

8.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Firewall and IDS

Activity 1:

1. Is the firewall software or hardware? Could it be a combination of both?
2. What data does the firewall monitor?
3. John has 5 PCs at home, and he wants to protect them all, what type of firewall should be used?
4. John has a laptop and uses it in different locations such as work, hotels, and home. What type of firewall should be used?
5. In a home network environment where you have 3 PCs, IPads and IPhones and a router. Which of the following is the best option to install a firewall (PC, router, switch) to protect the network?
6. In the lab, one of the computers has been infected by malware as an employee brought by using his infected USB, do you think firewall can protect the PCs?

Activity 2

1. What does packet filtering firewall examine in a packet?
2. What does stateless firewall mean?
3. Does packet filter examine the payload of a packet?
4. A company has network-based firewall and they authorized port #80, because they want to tell the world about the company's activity, but the company administrator wasn't aware that they were using an old version of webserver which has a Buffer Overflow bug. Can the firewall protect a hacker from the internet to exploit this bug?
5. Write a rule to allow inbound mail (SMTP, port25) but only to our email server with IP address 192.168.0.25.
6. Write a rule to block all traffic from the site TIMEWASTE.

7. Write a rule that any inside host can visit all secure webservers (note: The port number for secure web server is 443).

Activity 3

1. Discuss the advantages and disadvantages of application-level proxy compared with packet filtering firewall.

2. What is the purpose of honeypots?

3. Explain why bastion host needs to be highly secured by system administrators compared to other computers in the private networks.

Activity 4

1. Explain the difference between a host-based intrusion detection system (HIDS) and a network-based intrusion detection system (NIDS). Provide a scenario where each type would be more suitable.

2. Describe the concept of signature-based intrusion detection and anomaly-based intrusion detection. What are the advantages and disadvantages of each approach?

Topic 9: VLAN and VPN

9.1 Learning Objectives

This topic provides an overview of VLAN and VPN. The topic covers the different types of VLAN and VPN. The concept of VLAN tagging and various VPN protocols will be also covered.

On completion of the topic, students will be able to:

- Understand the concept of VLANs and their benefits for network segmentation.
- Explore basic VLAN configuration steps and communication principles.
- Define Virtual Private Networks (VPNs) and their applications.
- Differentiate between Remote Access, Site-to-Site, Extranet, and Intranet VPNs

9.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

9.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Tutorials:	3 hours

9.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Introduction to VLAN
- VLAN Tagging
- Introduction to VPN
- Types of VPN
- VPN protocols

9.5 Tutorial Sessions

The laboratory time allocation for this topic is 3 hours.

Q1. What does VLAN stand for, and what is its primary purpose in networking?

Q2. Explain the concept of VLAN tagging and its significance in network communication.

Q3. Define VPN and briefly explain why organizations implement VPNs.

Q4. Name two primary types of VPNs and provide a brief description of each.

Q5. Company ABC wants to segment its network to enhance security and optimize traffic. Describe how VLANs could be implemented in this scenario.

Q6. Company ABC is planning to implement a VoIP system. How can VLANs be utilized to optimize network performance for VoIP traffic, and what considerations should be considered?

Q7. The sales team of Company XYZ frequently works from various locations. How can a Remote Access VPN benefit the sales team, and which VPN protocol might be suitable for this scenario?

9.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours

Q1. Mention two common VPN protocols and highlight a key difference between them.

Q2. Explain the concept of VLAN pruning and provide a scenario where VLAN pruning would be advantageous in a network with multiple interconnected switches.

Q3. Compare and contrast the use of GRE (Generic Routing Encapsulation) tunnels and IPsec tunnels in the context of VPNs. In what scenarios might one be preferred over the other?

Q4. Discuss the concept of "Double VLAN Tagging" or "Q-in-Q" and describe a situation where it might be beneficial in a network architecture.

Q5. Describe the security considerations and potential vulnerabilities associated with VLAN hopping. How can network administrators mitigate the risks of VLAN hopping attacks?

Q6. Discuss the advantages and disadvantages of using Layer 3 switches for inter-VLAN routing compared to a dedicated router. In what scenarios would one approach be preferred over the other?

Q7. Explain the concept of Private VLANs (PVLANs) and provide a real-world scenario where PVLANs could be beneficial for network design.

Topic 10: Wireless Security

10.1 Learning Objectives

This topic provides an overview of wireless network along with corresponding threats to wireless network. The topic covers the different types of wireless security protocols and mobile device security aspects.

On completion of the topic, students will be able to:

- Understand the importance of wireless security.
- Identify common security threats in wireless networks.
- Understand the basic of security protocols in wireless networks.
- Discuss key concepts and best practices for securing the wireless networks.

10.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

10.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Tutorials:	3 hours

10.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Introduction to Wireless Networks
- Wireless security (WEP, WPA, WPA2)
- 802.11i Robust Security Network (RSN)
- Wireless Application Protocol

10.5 Tutorial Sessions

The laboratory time allocation for this topic is 3 hours

Q1. Explain what RSN is and why it is an improvement over previous wireless security protocol.

Q2. Describe the concept of Wireless LAN for Trusted Systems (WLTS) and its applications.

Q3. What is a Wireless Access Point (WAP), and how does it contribute to a wireless network?

Q4. Implementing strong wireless security is essential to protect against unauthorized access and data breaches. List three best practices for securing a wireless network.

Q5. In what scenarios is Wireless Application Protocol particularly beneficial, and what limitations might users encounter when accessing web content through WAP?

Q6. Describe the purpose and implementation of Wireless Intrusion Prevention Systems (WIPS) in securing wireless networks. Provide a scenario where WIPS would be crucial.

10.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Q1. Discuss the advantages and disadvantages of using the 2.4 GHz and 5 GHz frequency bands in wireless networks. In what scenarios would each band be more suitable?

Q2. Explain the concept of a Rogue Access Point in wireless security. How can organizations detect and mitigate the risks associated with Rogue Access Points?

Q3. Elaborate on the concept of a Virtual Private Network (VPN) in the context of wireless networks. How can the integration of VPN enhance the security of wireless communications, especially in public Wi-Fi scenarios?

Q4. Differentiate between WAP and standard web browsing. What challenges does WAP address in the context of mobile devices?

Q5. Contrast the security features and vulnerabilities of WEP, WPA, and WPA2. Provide recommendations for migrating from WEP to more secure protocols.

Q6. Imagine a scenario where a bank is developing a mobile banking application using WAP. How can WAP's architecture facilitate secure and efficient communication between a user's mobile device and the bank's servers? Highlight the role of WTLS in this context.

Q7. Consider a scenario where a smart home uses various IoT devices such as smart thermostats and security cameras. Discuss the security risks associated with IoT devices and propose measures homeowners can take to enhance the security of their smart home networks.

Topic 11: Information Security Management

11.1 Learning Objectives

This topic provides an overview of information security management along with cultural and governance aspect. The topic covers the different types of legalization and standard compliance issue related to information security. The topic will also provide students with risk management strategies related to information security management.

On completion of the topic, students will be able to:

- Understand the importance of information security management.
- Identify countermeasures and review techniques appropriate to the management of information security risks.
- Understand the significance of legal regulations and requirements on information security systems.

11.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

11.3 Timings

Lectures:	2 hours
Private Study:	8 hours
Tutorials:	3 hours

11.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Information Security: Overview, culture, and governance
- Legal Regulation and Compliance
- Risk Management

11.5 Tutorial Sessions

The laboratory time allocation for this topic is 3 hours.

Q1. Explain the importance of establishing a strong information security culture within an organization. What role does leadership play in fostering this culture?

Q2. Define information security governance and outline its key components. How does effective governance contribute to the overall security posture of an organization?

Q3. Discuss the significance of legal regulations and compliance in the field of information security. Provide an example of a relevant regulation and explain its impact on organizations.

Q4. Explain the concept of risk management in the context of information security. Outline the steps involved in the risk management process.

Q5. Discuss the differences between qualitative and quantitative risk assessments in information security. In what scenarios might one approach be preferred over the other?

Q6. Explain the concept of a risk appetite and risk tolerance in the context of risk management. How do these concepts guide decision-making in addressing information security risks?

Q7. In a scenario where a company is implementing a phishing awareness training program, outline the key elements that should be included in the training, and explain how such training contributes to the organization's information security.

Q8. In a scenario where an organization is migrating its infrastructure to the cloud, discuss the security considerations and challenges associated with cloud adoption. How can the organization address these challenges to ensure a secure cloud environment?

11.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Q1. In a corporate environment allowing employees to bring their own devices, discuss the security challenges associated with BYOD. Propose strategies and technologies that organizations can implement to enhance the security of BYOD policies.

Q2. Imagine a scenario where a company detects a security incident involving a potential data breach. Discuss the steps the organization should take to activate and implement its incident response plan. Highlight the importance of a well-prepared incident response strategy.

Q3. Discuss the ethical considerations and challenges associated with penetration testing. How can organizations ensure responsible and ethical testing practices?

Q4. In a scenario where an organization is adopting a zero-trust security model, discuss the fundamental principles of zero-trust and how they differ from traditional security models. Provide examples of security measures that align with a zero-trust approach.

Q5. Explain the purpose and significance of ISO 27001 in the context of information security management.

Q6. In a scenario where an organization is seeking ISO 27001 certification, describe the steps the organization needs to take to achieve and maintain certification. Highlight the ongoing commitment required for compliance.

Q7. In a complex scenario where an organization heavily relies on third-party vendors for critical services and information processing, discuss the challenges and strategies related to managing and ensuring the security of information handled by these vendors in alignment with ISO 27001.

Topic 12: Unit Summary

12.1 Learning Objectives

This topic provides an overview of complete unit and highlight the important aspect and provide students with the complete overview of topics covered in the unit.

On completion of the topic, students will be able to:

- Demonstrate a systematic understanding of the concept of Network Security and Cryptography.
- Critically evaluate the suitability of different Cryptographic Algorithms.
- Understand the vulnerabilities and systematically evaluate the security risks in networks.
- Critically analyse appropriate tool and techniques for network security.
- Understand the wireless network security and associated protocols.
- Explain the concepts of Information Security and explain good practice in achieving security.

12.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

12.3 Timings

Lectures:	3 hours
Tutorials:	2 hours
Private Study:	9 hours

12.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Introduction to Network Security and Cryptography
- Cryptography Techniques
- Operating System Security and Vulnerabilities
- Software Vulnerabilities and Attacks
- Network Security and Defence
- Email and Web Security
- Firewalls
- VLAN and VPN
- Wireless Security
- Information Security Management

12.5 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

This session is for support to student to address any questions related to lab or tutorial session, and can also introduce assessment or provide some guidance on exam.

12.6 Private Study

The time allocation for private study in this topic is expected to be 9 hours.

The private study time is used for the preparation of exams or to complete any lab or tutorial session.