YORKSHIRE & HUMBER INSTITUTE OF TECHNOLOGY

Est. 1841 YORK ST JOHN UNIVERSITY

Teaching and Learning Cybersecurity courses with Virtualization Technology

Aminu Usman, PhD, HEA
Department of Computer Science
York St John

Presented at YHIoT Tech Seminar, 2021

Outline

- VT - Enabling students beyond the classroom
- Virtualization Technology ?
- Teaching With VT
- Examples - Environment Setup for the Experiments
- VT-Based Assessment Methods
- Samples of experiment
- VM Vs Containers
- Instructors and Students Observations/Feedback

Enabling students beyond the classroom

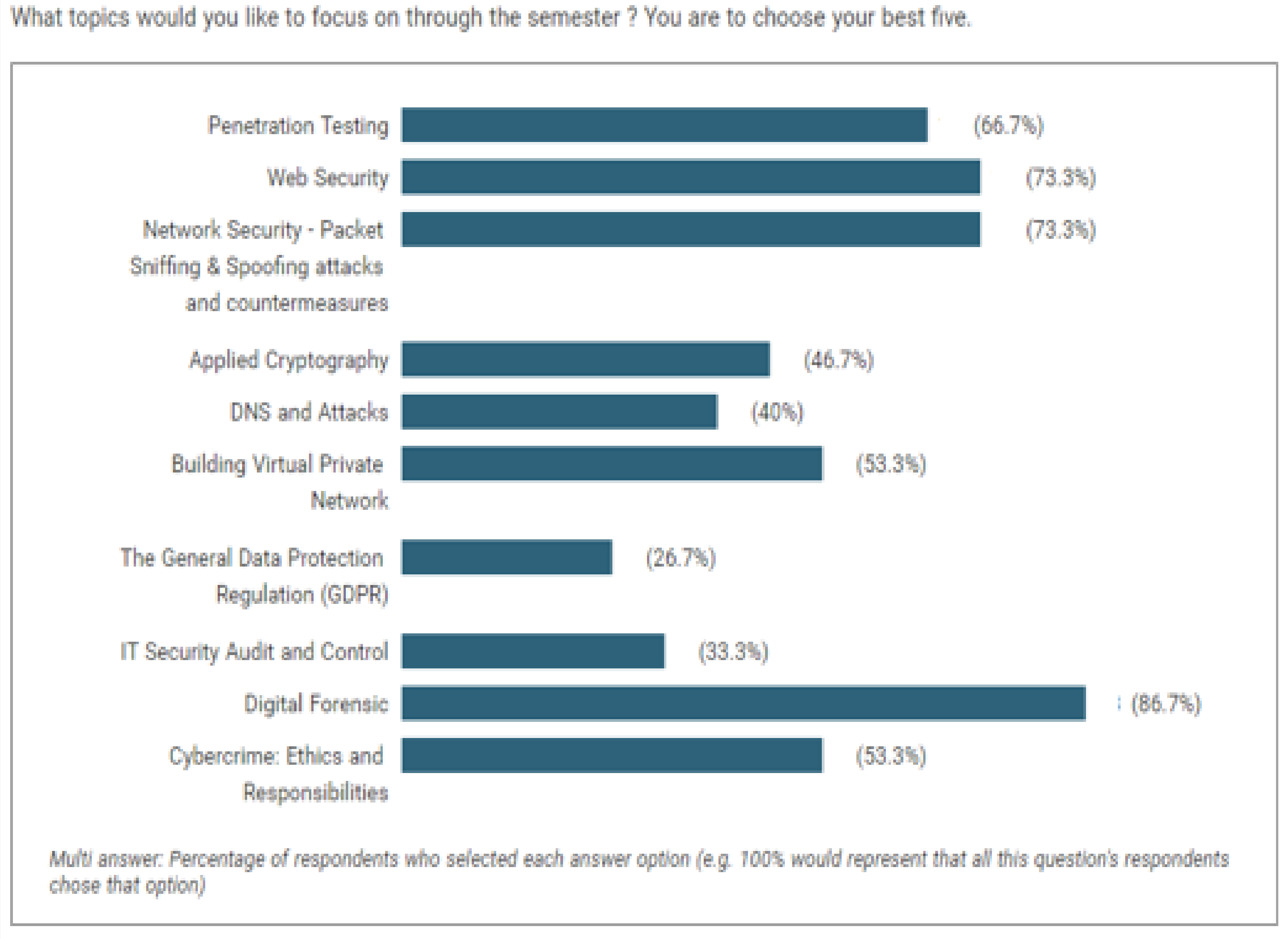
• Achieving accurate learning outcomes and assessments that reflect	• the practical elements of the courses learning objectives • students' expectations, • Industry’s changing requirements
• Time & Logistics	• How many hours do students have access to the laboratory infrastructures ?
• Safe Environment for Students Work	• Can the students have access to their practical learning platforms at their comfort and at any time? • Would the students be able to practice their learning in a safe environment with all the computer and network access privileges
• Scalability	• Would they be able to scale their work with adequate resources to enable them to demonstrate their learning from anywhere ?

Student-focused/expectations

- Students are looking for

- Job related topics

- Some topics are difficult to be taught theoretically
- Most of the subjects requires students to build a network



What topics would you like to focus on through the semester ? You are to choose your best five.

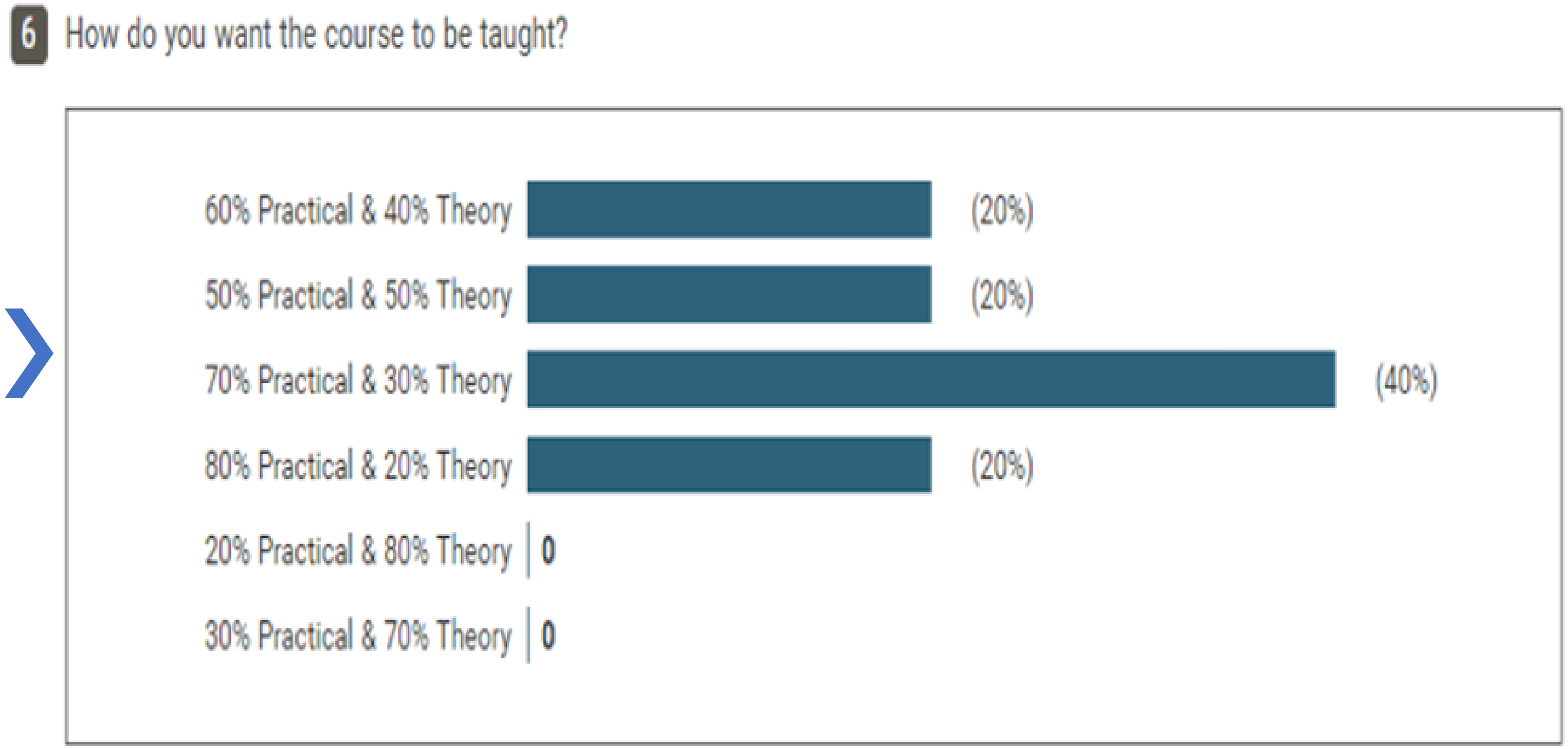
Multi answer: Percentage of respondents who selected each answer option (e.g. 100% would represent that all this question's respondents chose that option)

Cybersecurity Pre-course Survey

Student-focused/expectations (2)

- Students are looking for

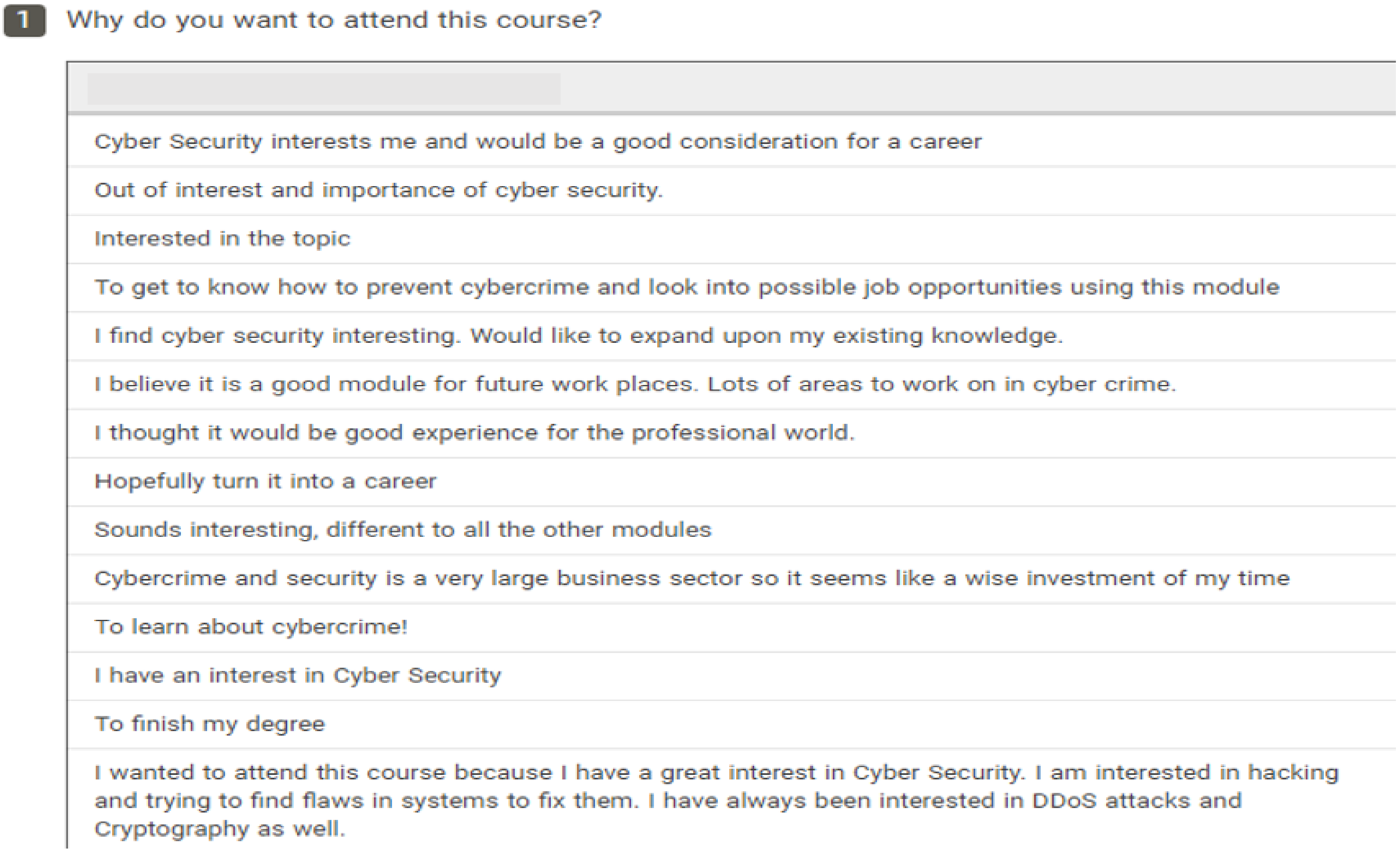
Hands on experiences/learning



6 How do you want the course to be taught?

Cybersecurity Pre-course Survey

Student-focused/expectations (3)



1 Why do you want to attend this course?

Cyber Security interests me and would be a good consideration for a career

Out of interest and importance of cyber security.

Interested in the topic

To get to know how to prevent cybercrime and look into possible job opportunities using this module

I find cyber security interesting. Would like to expand upon my existing knowledge.

I believe it is a good module for future work places. Lots of areas to work on in cyber crime.

I thought it would be good experience for the professional world.

Hopefully turn it into a career

Sounds interesting, different to all the other modules

Cybercrime and security is a very large business sector so it seems like a wise investment of my time

To learn about cybercrime!

I have an interest in Cyber Security

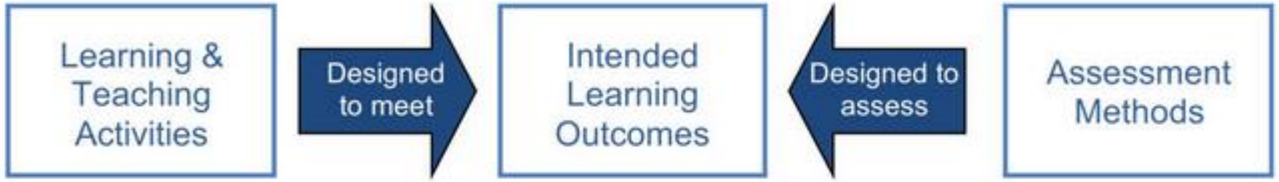
To finish my degree

I wanted to attend this course because I have a great interest in Cyber Security. I am interested in hacking and trying to find flaws in systems to fix them. I have always been interested in DDoS attacks and Cryptography as well.

- Career, Interest, work placement, experience, to finish a degree

ILOs and constructive alignment with L&T and Assessment Method

- At the heart of curriculum design are three key processes:
  - establishing appropriate ILOs;
  - designing appropriate learning and teaching activities that enable learners to meet those outcomes;
  - designing appropriate assessment methods through which learners can demonstrate that they have met the outcomes.



Teaching Cybersecurity courses

Theory – lectures

Explain/describe ideas and the meanings of terms

Case studies

Evaluate/discuss/ the strength and weaknesses of security systems

Simulators/Emulators/Model Checkers

Illustrate events/incidences with limitations & approximations

Mathematics

Demonstrate ideas with approximations. NOT the actual events

Virtualization Technology

Practice

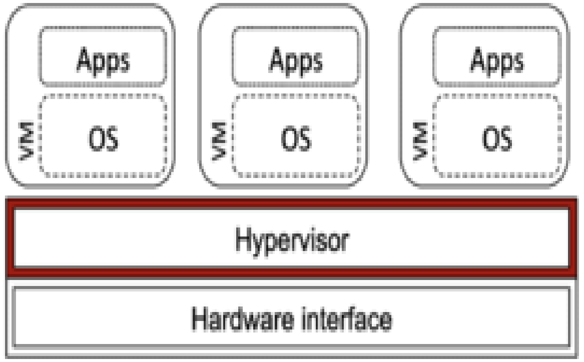
Virtualization Technology ?

Virtualization

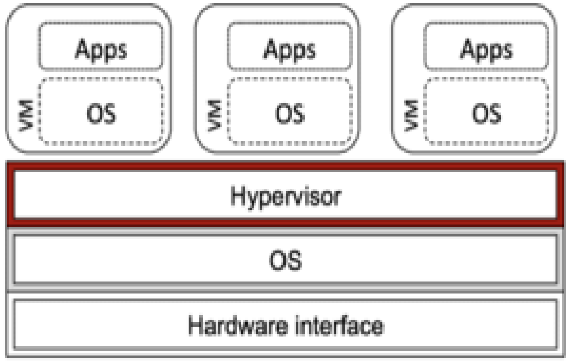
- Virtualization is the creation of a virtual version computer, including virtual computer hardware platforms, storage devices, etc.
- A VM is a software implementation of a computer that executes programs like a physical machine.
- Hypervisors (VMM) - a software program that manages multiple OSes
- Types
  - Application Server Virtualization
  - Application Virtualization
  - Network Virtualization
  - Storage Virtualization
  - Desktop Virtualization
  - Full Virtualization

- Virtualization Concepts

- Bare-Metal Hypervisor (Type 1)
  - Vmware vSphere/ESXi
  - Microsoft Hyper-V
  - Citrix XenServer



- Hosted Hypervisor (Type 2)
  - Vmware Worksstaion/Fusion
  - Oracle VirtualBox
  - Parallels (Mac)



Teaching With VT

Students can create more virtual hosts than the number of physical computers available in the laboratory

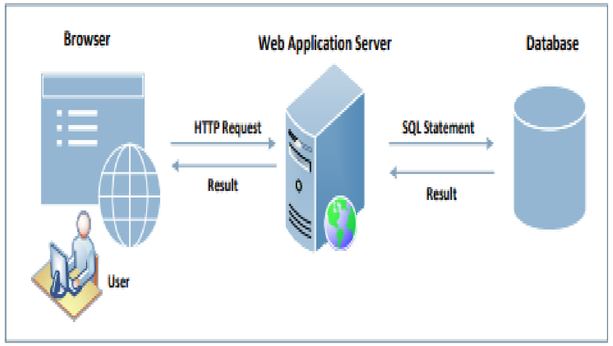
Student can create complex scenarios involving several hosts

No restrictions of the number of network interfaces in each host

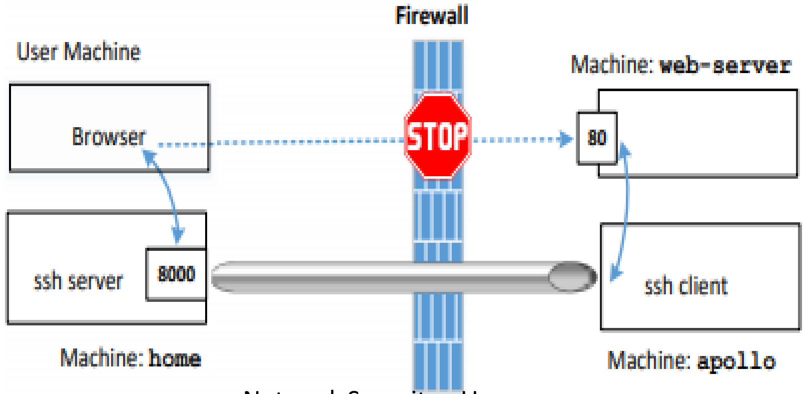
Student are the administrators of their virtual hosts

Students can reproduce the experiments at home

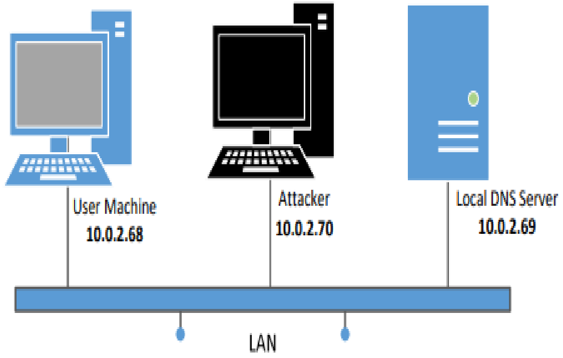
Examples - Environment Setup for the Experiments



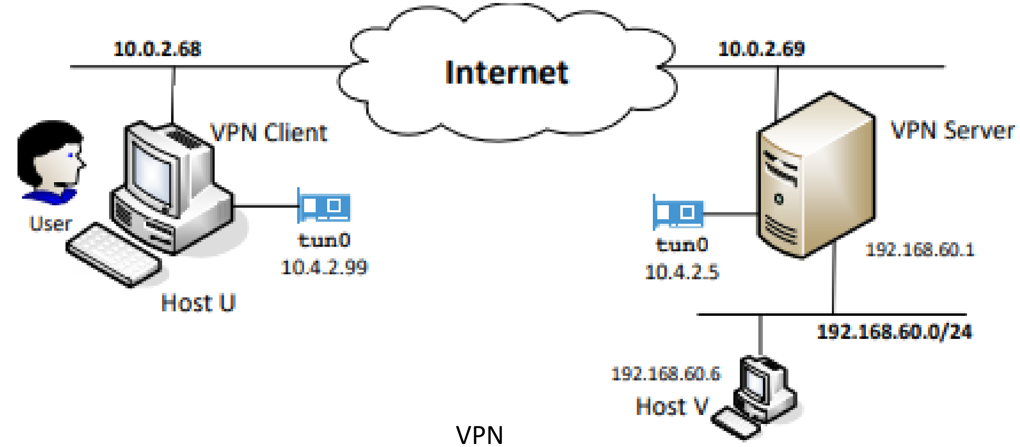
Web security - SQL Injection Attacks & countermeasures



Network Security - Use reverse SSH tunnelling to access an internal web server



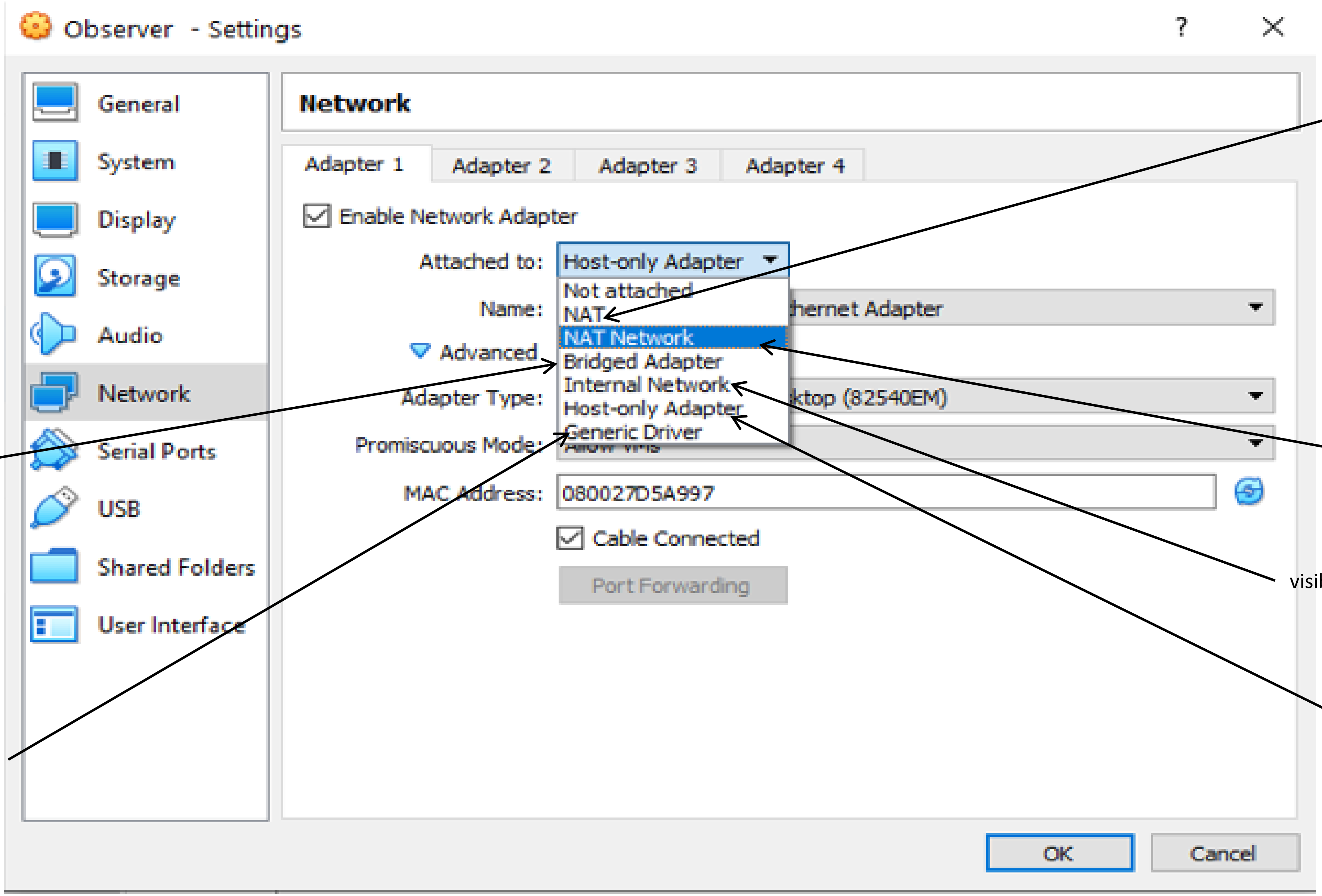
Network Security - DNS Attacks & countermeasures



VPN

Digital Forensics

VMs Network settings



Observer - Settings

Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: ...hernet Adapter

▽ Advanced

Adapter Type: ...ktop (82540EM)

Promiscuous Mode: Allow VMs

MAC Address: 080027D5A997

☑ Cable Connected

If all you want is to use the VM to browse the Web

For more advanced networking needs, such as network simulations and running servers in a guest

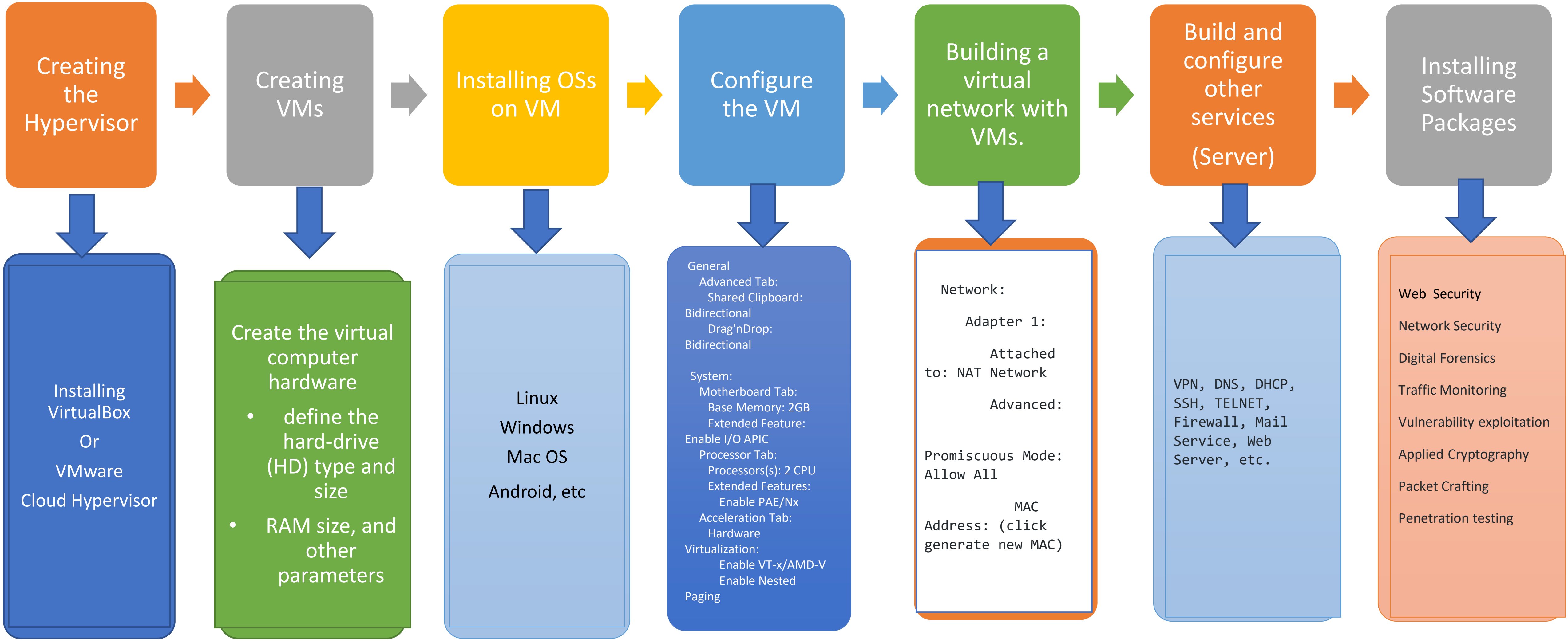
Internal network that allows outbound connections

visible to selected virtual machines

This can be used to create a network containing the host and a set of virtual machines

Rarely used modes which share the same generic network interface

Building the Lab Environment



Creating the Hypervisor

Installing VirtualBox
Or
VMware
Cloud Hypervisor

Creating VMs

Create the virtual computer hardware

- define the hard-drive (HD) type and size
- RAM size, and other parameters

Installing OSs on VM

Linux
Windows
Mac OS
Android, etc

Configure the VM

```
General
   Advanced Tab:
     Shared Clipboard:
Bidirectional
     Drag'nDrop:
Bidirectional

 System:
   Motherboard Tab:
     Base Memory: 2GB
     Extended Feature:
Enable I/O APIC
   Processor Tab:
     Processors(s): 2 CPU
     Extended Features:
        Enable PAE/Nx
   Acceleration Tab:
     Hardware
Virtualization:
        Enable VT-x/AMD-V
        Enable Nested
Paging
```

Building a virtual network with VMs.

```
 Network:

     Adapter 1:

          Attached
to: NAT Network

          Advanced:


Promiscuous Mode:
Allow All

               MAC
Address: (click
generate new MAC)
```

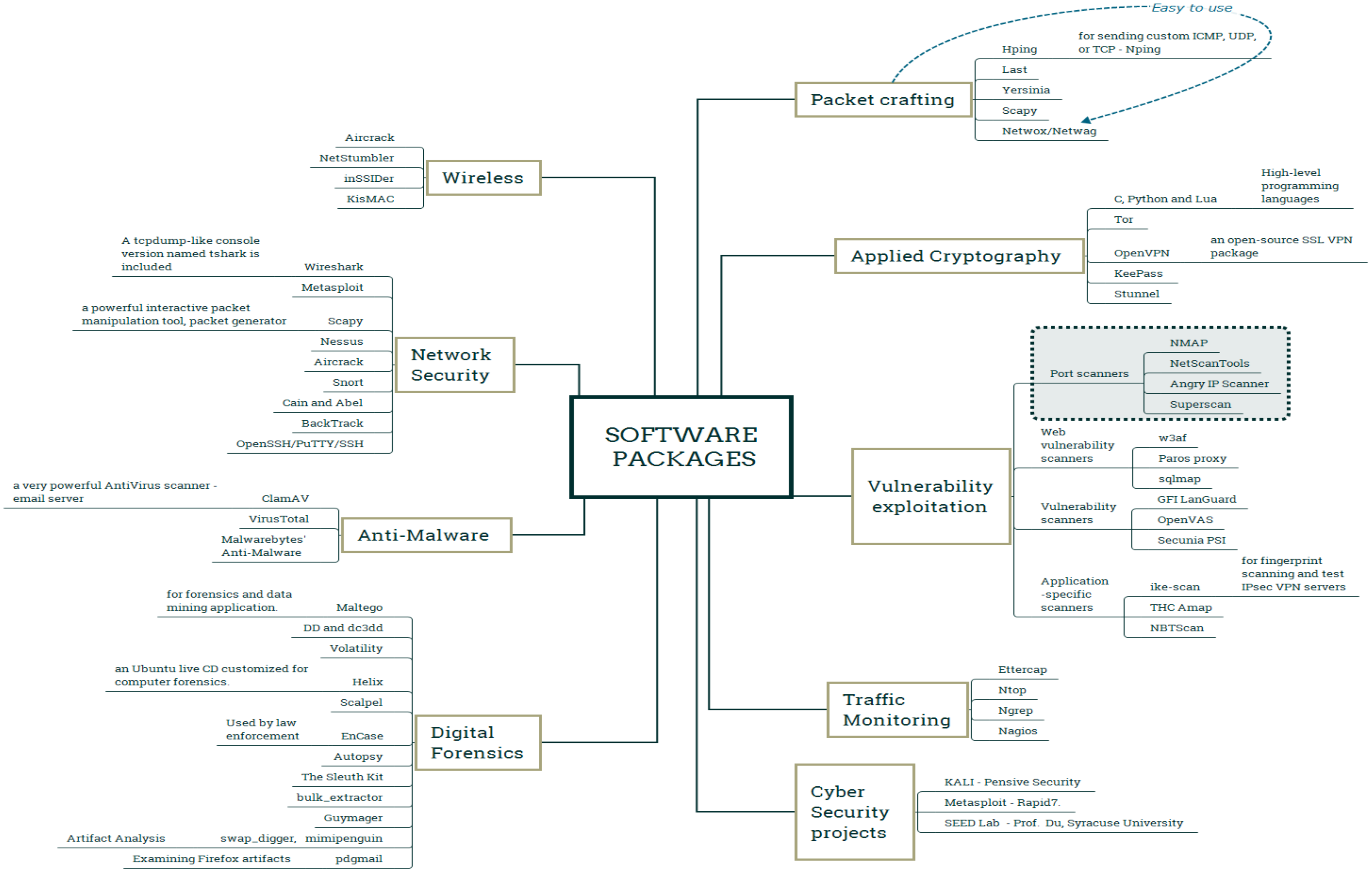
Build and configure other services

(Server)

VPN, DNS, DHCP, SSH, TELNET, Firewall, Mail Service, Web Server, etc.

Installing Software Packages

Web Security
Network Security
Digital Forensics
Traffic Monitoring
Vulnerability exploitation
Applied Cryptography
Packet Crafting
Penetration testing



SOFTWARE PACKAGES

- Packet crafting
  - Hping – for sending custom ICMP, UDP, or TCP - Nping
  - Last
  - Yersinia
  - Scapy
  - Netwox/Netwag – *Easy to use*
- Applied Cryptography
  - C, Python and Lua – High-level programming languages
  - Tor
  - OpenVPN – an open-source SSL VPN package
  - KeePass
  - Stunnel
- Vulnerability exploitation
  - Port scanners
    - NMAP
    - NetScanTools
    - Angry IP Scanner
    - Superscan
  - Web vulnerability scanners
    - w3af
    - Paros proxy
    - sqlmap
  - Vulnerability scanners
    - GFI LanGuard
    - OpenVAS
    - Secunia PSI
  - Application -specific scanners
    - ike-scan – for fingerprint scanning and test IPsec VPN servers
    - THC Amap
    - NBTScan
- Traffic Monitoring
  - Ettercap
  - Ntop
  - Ngrep
  - Nagios
- Cyber Security projects
  - KALI - Pensive Security
  - Metasploit - Rapid7.
  - SEED Lab - Prof. Du, Syracuse University
- Wireless
  - Aircrack
  - NetStumbler
  - inSSIDer
  - KisMAC
- Network Security
  - Wireshark – A tcpdump-like console version named tshark is included
  - Metasploit
  - Scapy – a powerful interactive packet manipulation tool, packet generator
  - Nessus
  - Aircrack
  - Snort
  - Cain and Abel
  - BackTrack
  - OpenSSH/PuTTY/SSH
- Anti-Malware
  - ClamAV – a very powerful AntiVirus scanner - email server
  - VirusTotal
  - Malwarebytes' Anti-Malware
- Digital Forensics
  - Maltego – for forensics and data mining application.
  - DD and dc3dd
  - Volatility
  - Helix – an Ubuntu live CD customized for computer forensics.
  - Scalpel
  - EnCase – Used by law enforcement
  - Autopsy
  - The Sleuth Kit
  - bulk_extractor
  - Guymager
  - swap_digger, mimipenguin – Artifact Analysis
  - pdgmail – Examining Firefox artifacts

Kali Linux – Advance Penetration Testing tool

- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing
  - Hundreds of penetration tools..
  - Kali Linux can run on laptops, desktops or servers
  - Open source availability
  - Azure Penetration Testing
  - Building a customized Kali ISO is easy, fun, and rewarding
  - You can run Kali "Live" from a USB drive on standard Windows and Apple PCs

SEED Lab – A Hands-on Labs for Security Education

- A hands-on laboratory exercises (called SEED labs) for computer and information security education
  - Software Security Labs
  - Network Security Labs
  - Web Security Labs
  - System Security Labs
  - Cryptography Labs
  - Mobile Security Labs

The SEED project is now fully open sourced: https://github.com/seed-labs.

- Cloud-ready: You can now create a SEED VM on the cloud

Virtual Labs Environment

- Among the popular virtual security labs
  - DeterLab (cyber DEfense Technology Experimental Researc) – Terry Benzel, University of Southern California.
  - Tele-Lab IT – a web-based training system, University of Trier, Germany
  - NETinVM – Comprises several computers and networks, in a single virtual machine using nested virtualization
- These virtual labs can facilitate cybersecurity experiments, whereby students can configure a number of networked virtual machines and embark on security offense and defense exercises

VT-Based Assessment Methods (1)

Example Screenshots (still pictures)

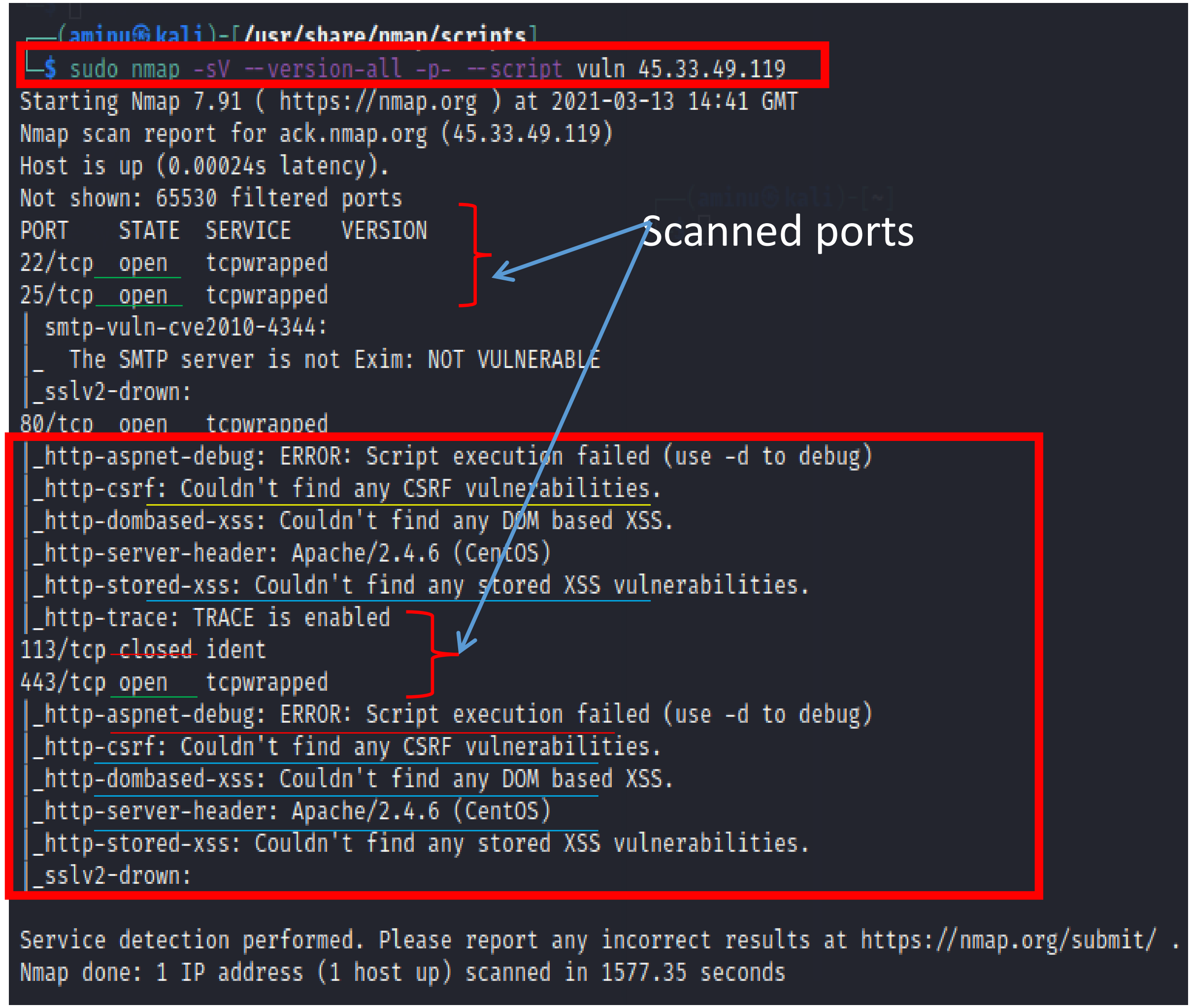
Settings, configurations, parameters, static outcomes, policies, codes or scripts

Example

Question – Detecting Cross-Site Scripting vulnerabilities in web applications.

Cross Site Scripting vulnerabilities allow attackers to spoof content, steal user cookies, and even execute malicious code on the user's browser. Many Web pen testers use the Nmap scripting engine to discover these vulnerabilities in web servers

Your task is to use either Nmap scripts or any methods of your choice to scan a web server looking for file vulnerabilities to Cross-Site Scripting (XSS). You are required to use a free scan web server or develop your own.



```
┌──(aminu㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV --version-all -p- --script vuln 45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-13 14:41 GMT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.00024s latency).
Not shown: 65530 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   tcpwrapped
25/tcp   open   tcpwrapped
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
80/tcp   open   tcpwrapped
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
113/tcp  closed ident
443/tcp  open   tcpwrapped
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1577.35 seconds
```

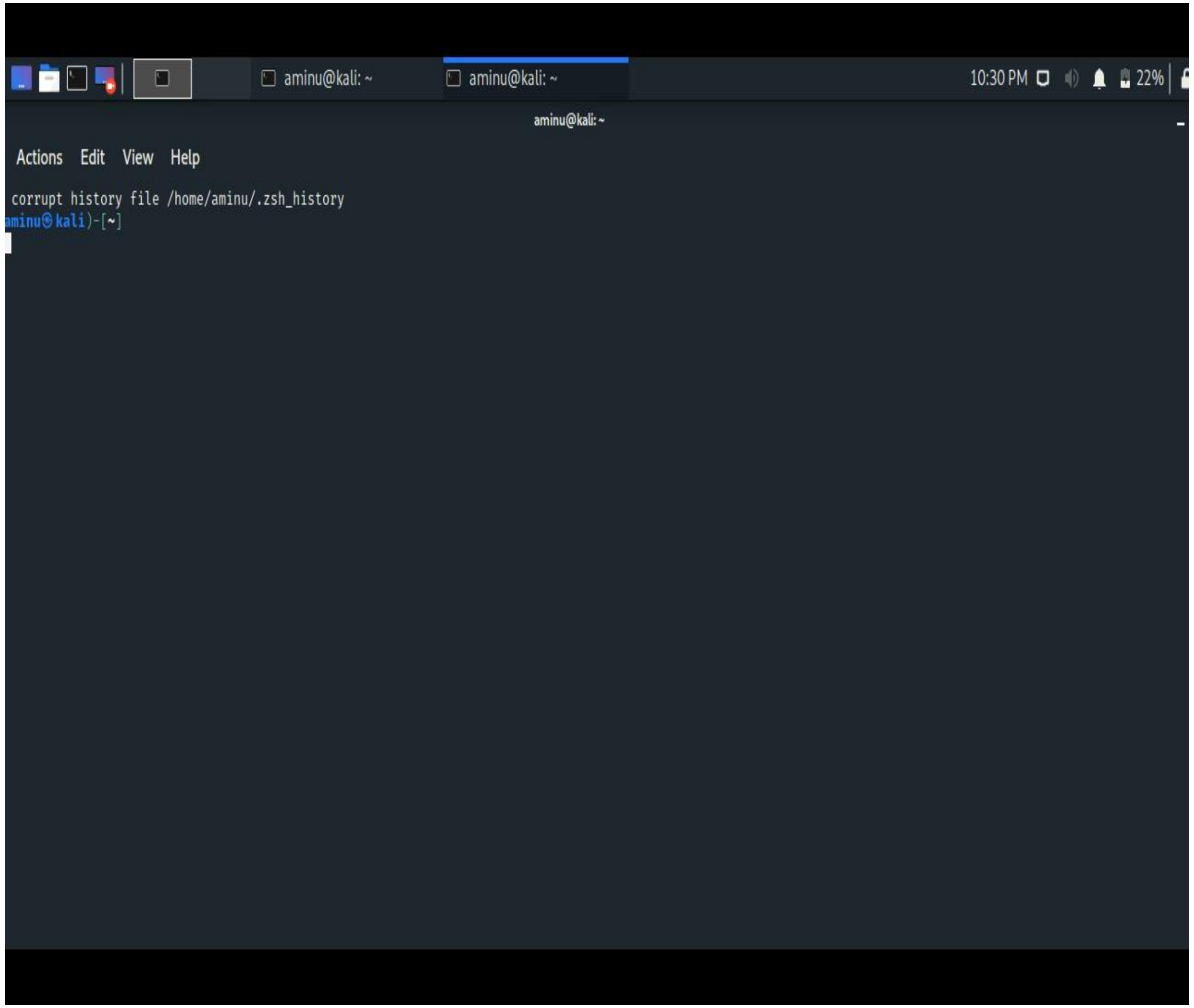
Scanned ports

Example- Assessment with Screenshots (still pictures)

VT-Based Assessment Methods (2)

- Assessment With Screen Capture Video
  - VT comes with a built-in screen video capturing function
  - Time in grading is reduced significantly
  - Short procedures, interactive outcomes

- Virtual Hard Disk Files and Virtual Appliances
  - the entire virtual hard disk file can be submitted for assessment
  - Using Save State - VM clears its memory when it is shut down

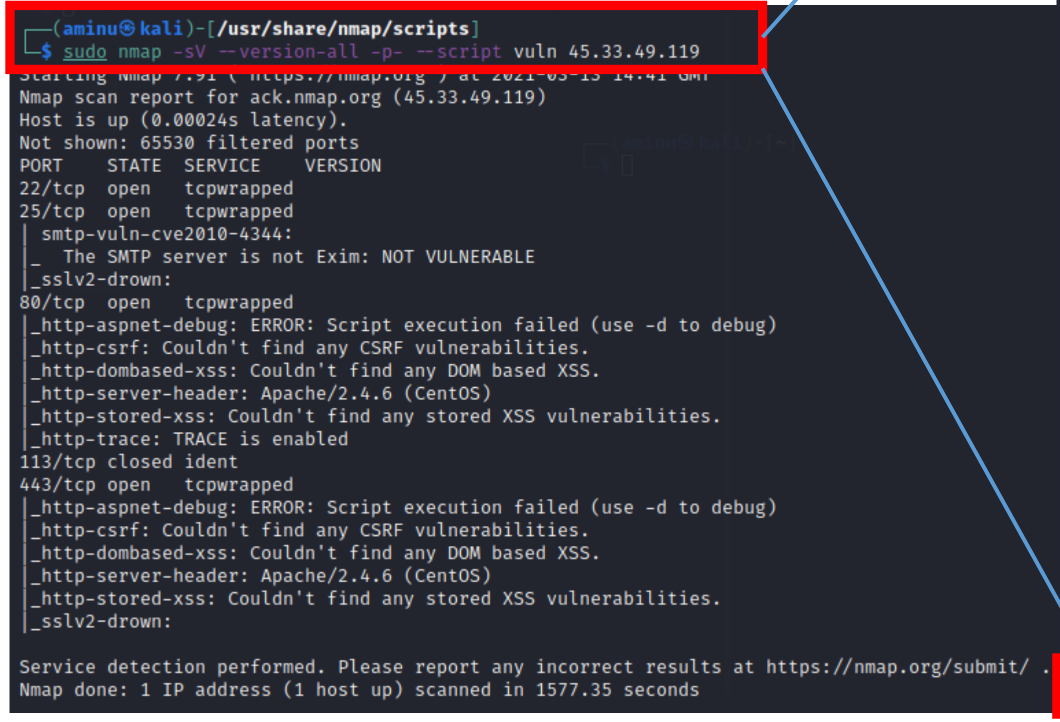


```
corrupt history file /home/aminu/.zsh_history
aminu㉿kali)-[~]
```

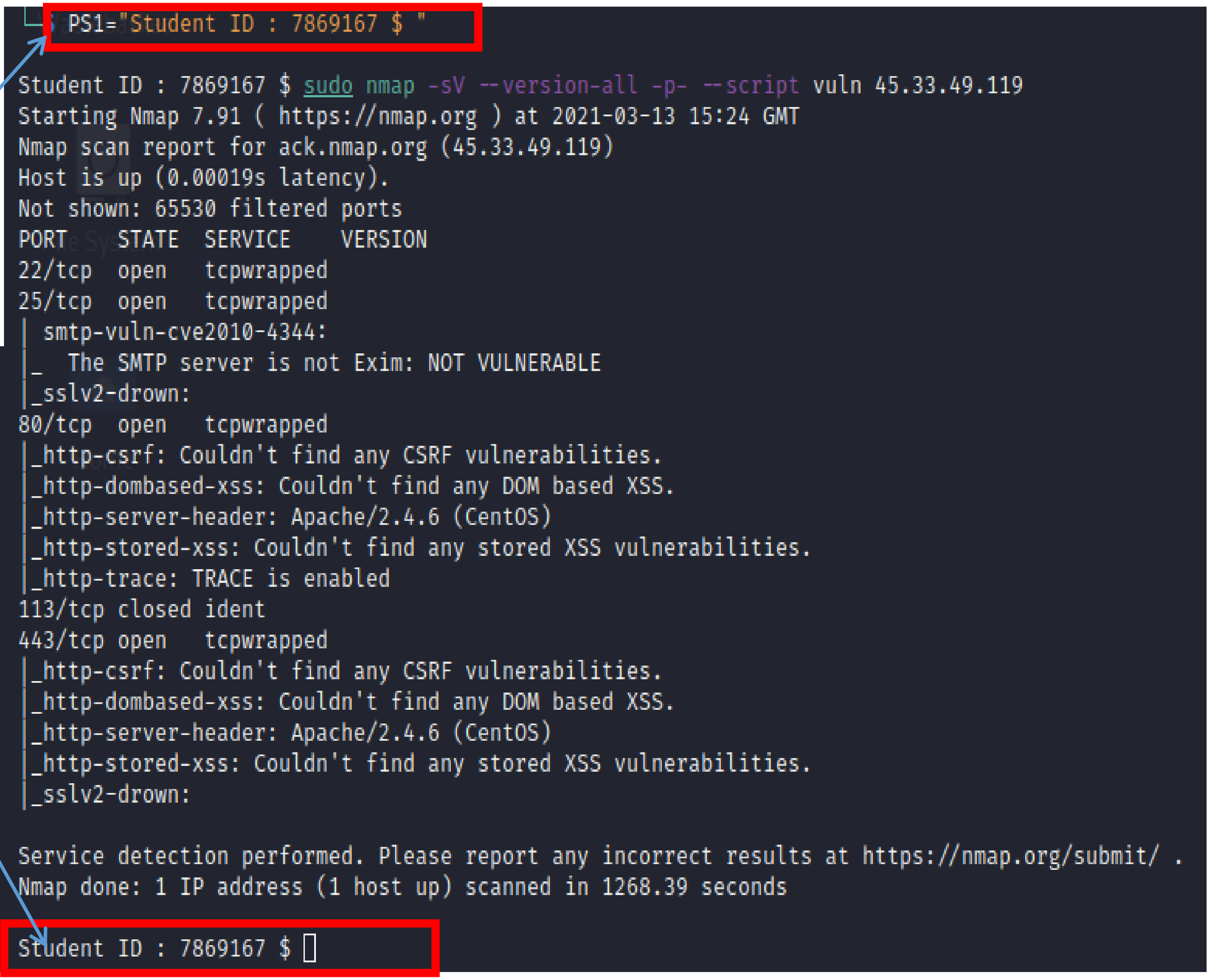
Example - Assessment With Screen Capture Video

VT-Based Assessment Methods

- Anonymous marking
  - Customize Bash Prompt
    - Change PS1 in ~/.bashrc, and then restart terminal
    - PS1=“ Student ID : 7869167 “



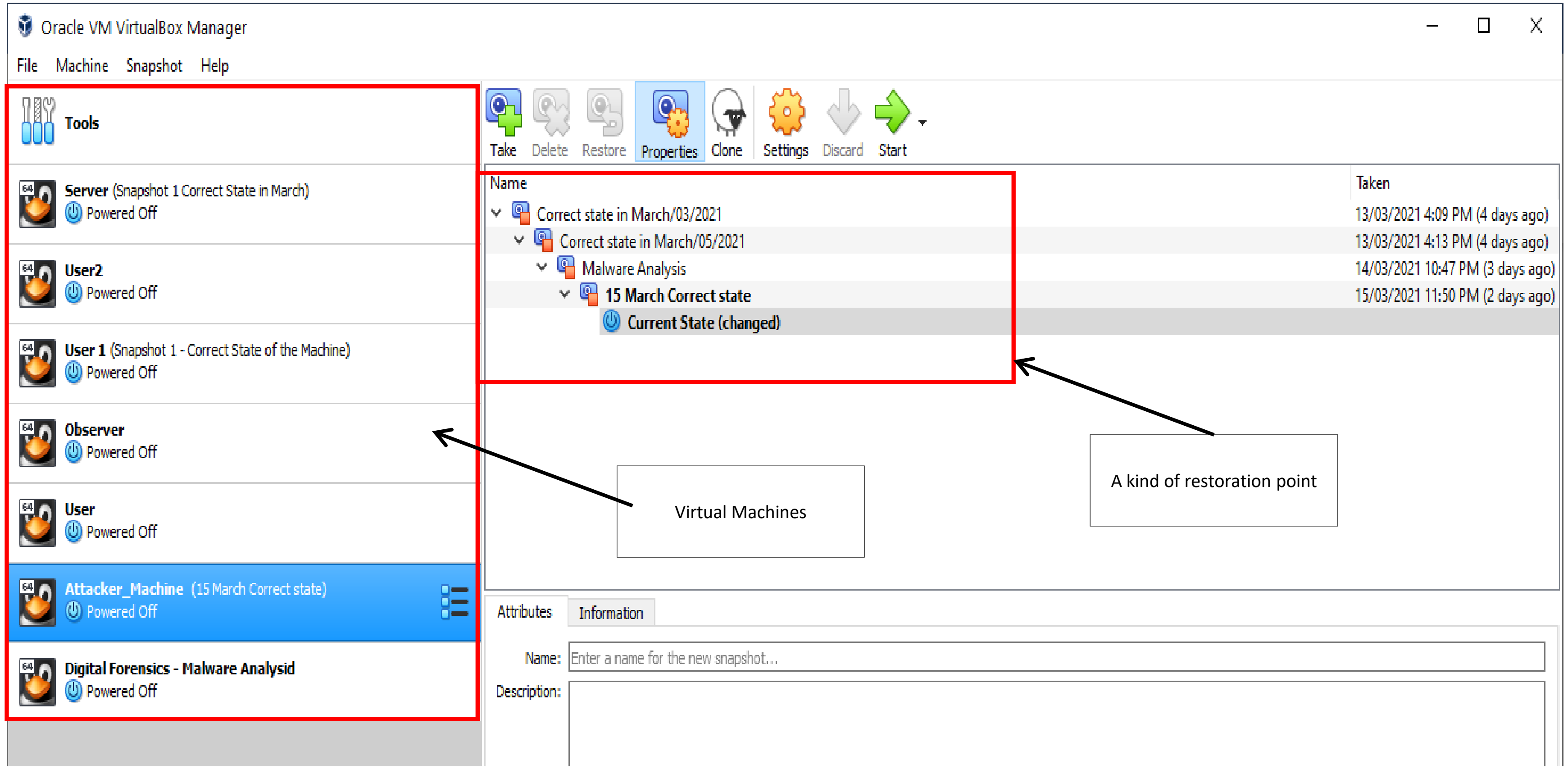
```
┌──(aminu㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV --version-all -p- --script vuln 45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-13 14:41 GMT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.00024s latency).
Not shown: 65530 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   tcpwrapped
25/tcp   open   tcpwrapped
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
80/tcp   open   tcpwrapped
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
113/tcp closed ident
443/tcp open   tcpwrapped
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1577.35 seconds
```



```
└─$ PS1="Student ID : 7869167 $ "

Student ID : 7869167 $ sudo nmap -sV --version-all -p- --script vuln 45.33.49.119
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-13 15:24 GMT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.00019s latency).
Not shown: 65530 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   tcpwrapped
25/tcp   open   tcpwrapped
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
80/tcp   open   tcpwrapped
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
113/tcp closed ident
443/tcp open   tcpwrapped
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1268.39 seconds

Student ID : 7869167 $
```

Building a Learning Portfolio With VT

- With VMs, students can easily save their hands-on learning activities by using a new VM for each assignment
  - each student would have an archive of virtual hard disk files



Server (Snapshot 1 Correct State in March)
Powered Off

User2
Powered Off

User 1 (Snapshot 1 - Correct State of the Machine)
Powered Off

Observer
Powered Off

User
Powered Off

Attacker_Machine (15 March Correct state)
Powered Off

Digital Forensics - Malware Analysid
Powered Off

Name	Taken
Correct state in March/03/2021	13/03/2021 4:09 PM (4 days ago)
Correct state in March/05/2021	13/03/2021 4:13 PM (4 days ago)
Malware Analysis	14/03/2021 10:47 PM (3 days ago)
15 March Correct state	15/03/2021 11:50 PM (2 days ago)
Current State (changed)	

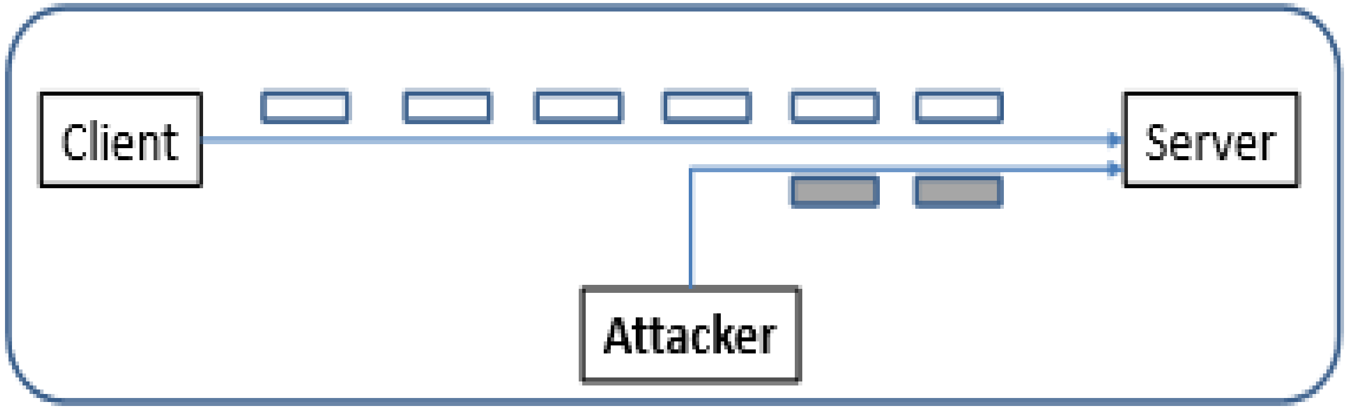
Name: Enter a name for the new snapshot...

Description:

Virtual Machines

A kind of restoration point

Sample practical experiments



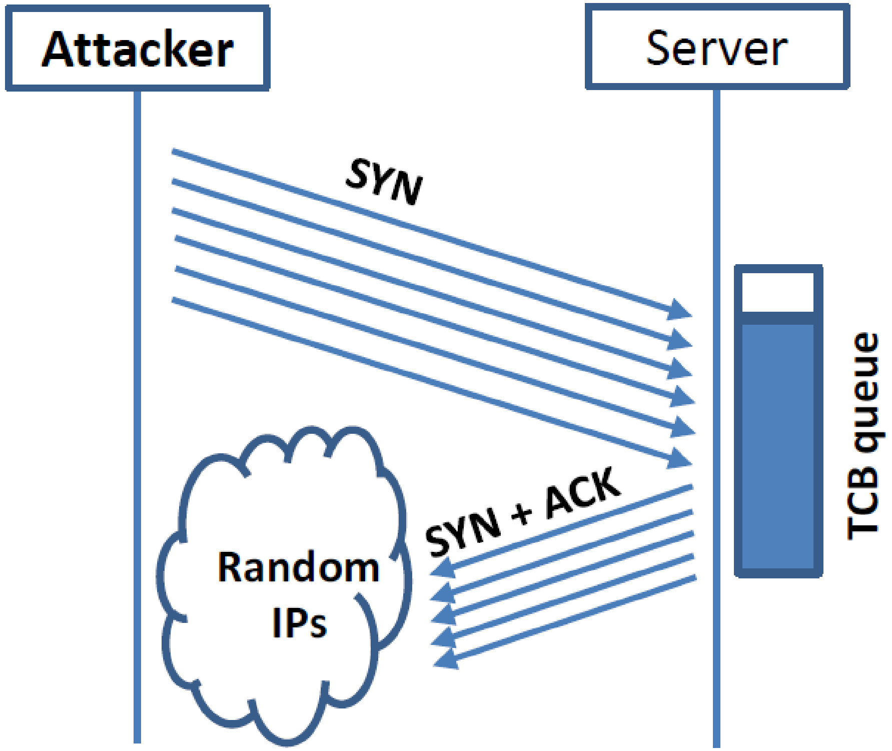
Injecting data into a TCP/UDP connection

Sample practical experiments

Idea : To fill the queue storing the half-open connections so that there will be no space to store TCB for any new half-open connection, basically the server cannot accept any new SYN packets.

Steps to achieve this : Continuously send a lot of SYN packets to the server. This consumes the space in the queue by inserting the TCB record.

- Do not finish the 3rd step of handshake as it will dequeue the TCB record.



SYN Flooding Attack

- Counter measures
- Turn ON the SYN Cookie countermeasure:

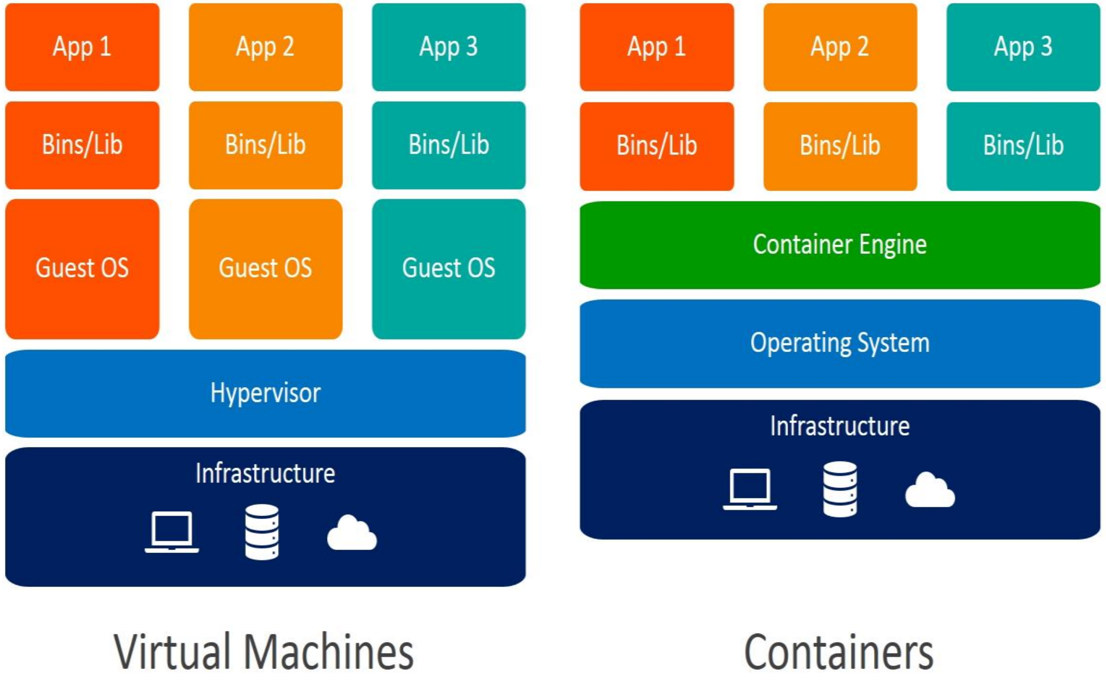
VM Vs Containers

- The industry standard today is to use Virtual Machines (VMs) to run software applications

- Docker is a platform for developers and sysadmins to build, run, and share applications with containers.

Containers are

- Lightweight
- Easy to start -- Only a few seconds
- Less OS maintenance
- Efficient



Challenges – Teaching with Virtualisation Tech

Backward compatibility

Compatibility issues when using legacy system can be time-consuming and difficult to solve.

- A good and descent PC, Cloud

Backup

Frequent software updates can make it difficult to access backup at times.

– Snapshots

Security

Unlike some tech solutions, virtualization is not really a “set it and forget it” type of solution.

– Regular updates

Learning curve

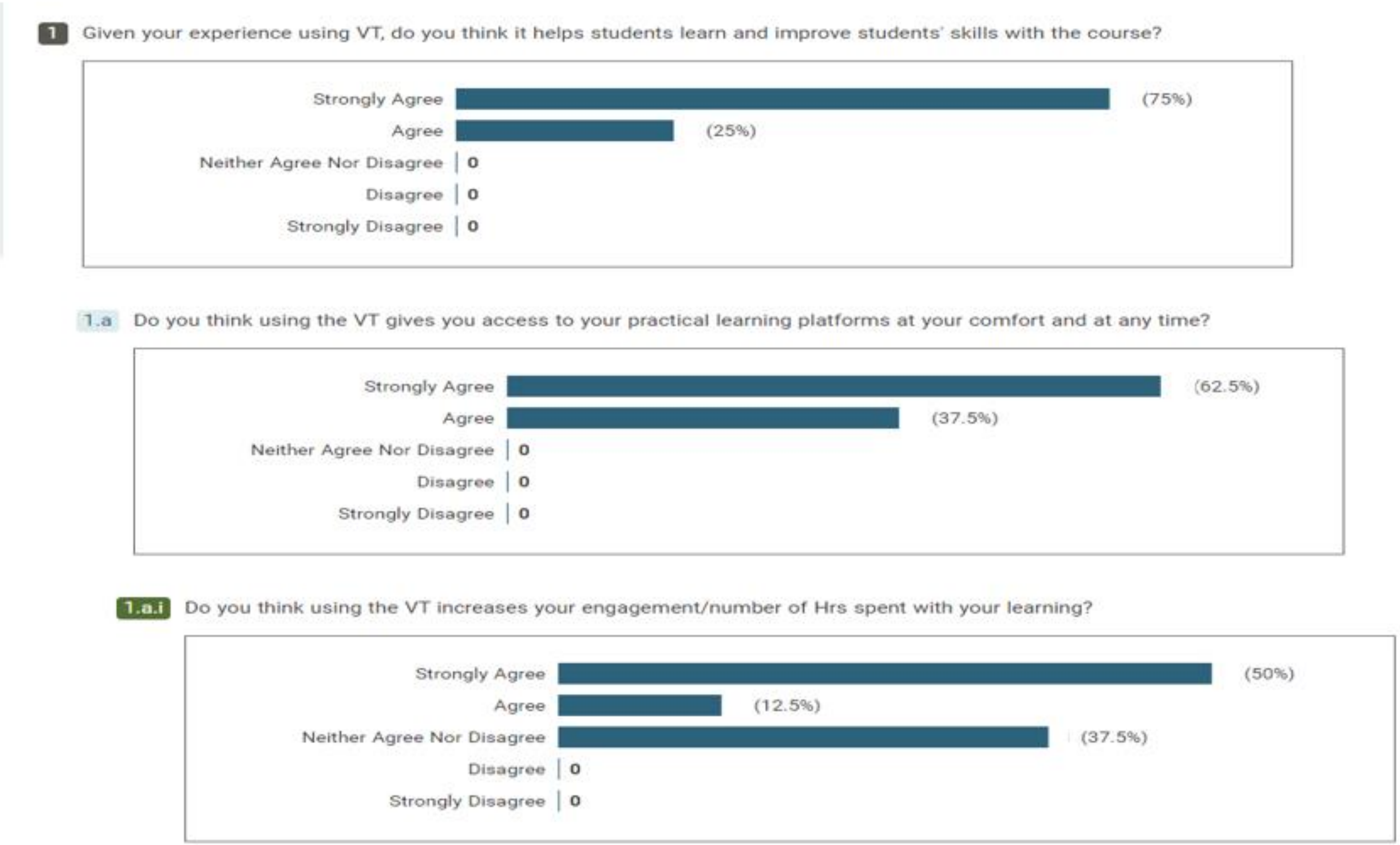
A misconception exists that virtualization is difficult to learn.

- Training and practices

Instructor Observations

- VT solve the logistics problems associated with hands-on activities
- It also helped to improve interaction with students and enabled more content coverage during class
- More hands-on projects
- Assessments are more aligned ILOs and comprehensive
- Coverage of material increased
- More interaction between
  - students and instructors – students ask questions more frequently
  - students and instructors – problems solving

Students Feedback on using the VT in Cybersecurity class



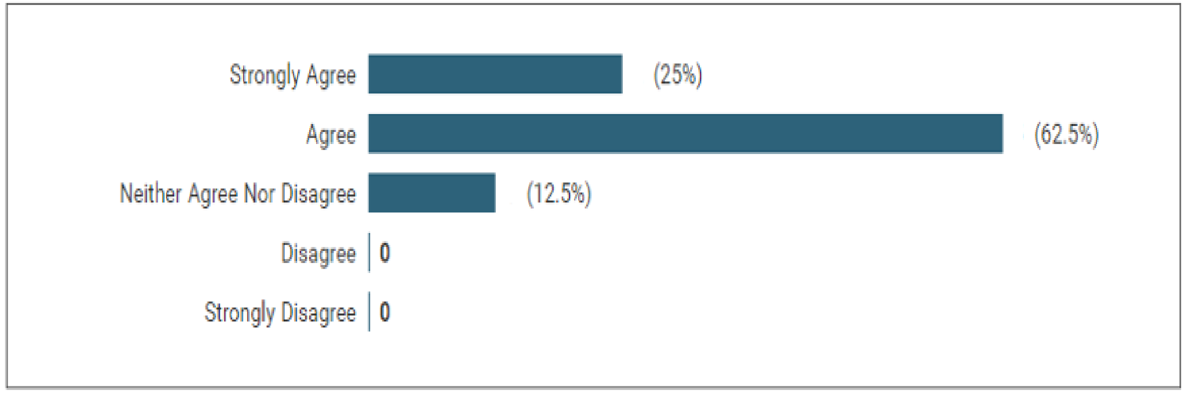
1 Given your experience using VT, do you think it helps students learn and improve students' skills with the course?

1.a Do you think using the VT gives you access to your practical learning platforms at your comfort and at any time?

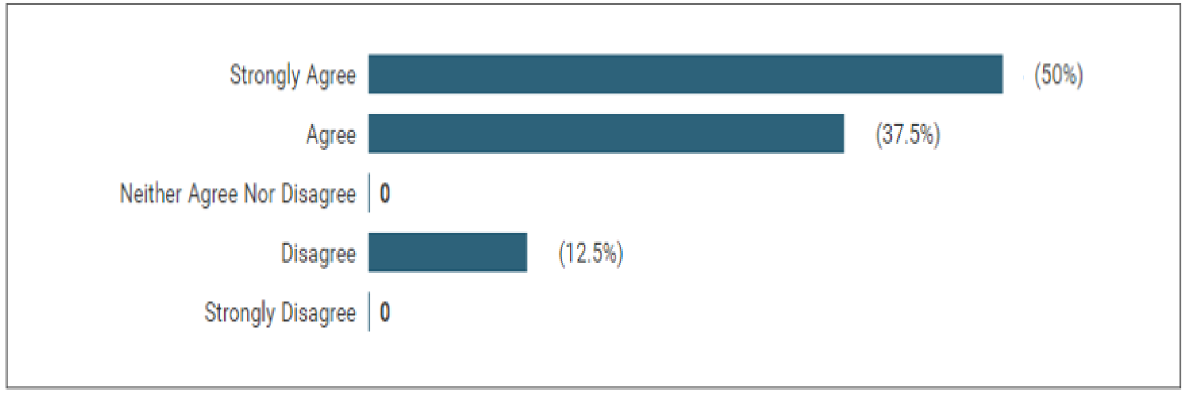
1.a.i Do you think using the VT increases your engagement/number of Hrs spent with your learning?

Students Feedback on using the VT in Cybersecurity class

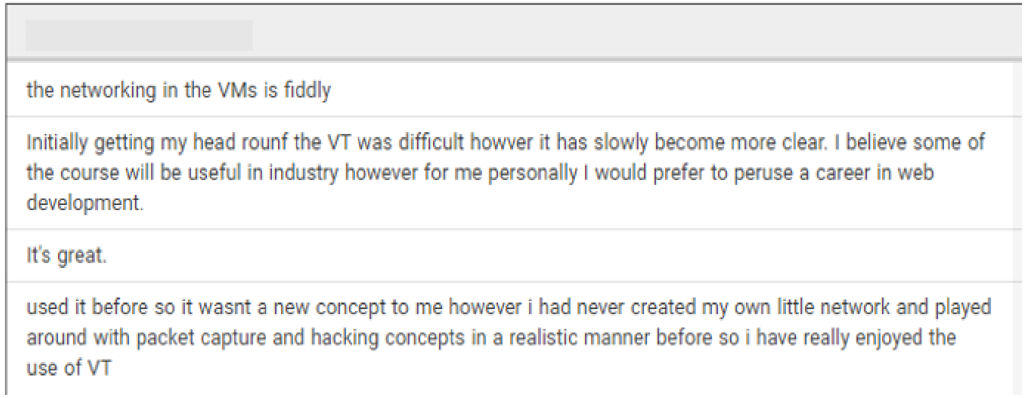
1.a.ii Do you think using the VT enabled you to scale your work and demonstrate your learning from anywhere?



1.a.iii Given the time you spent getting your head around the VT, do you think it is worth it?



1.a.iv Please provide any comments on your overall experience of the use of VT



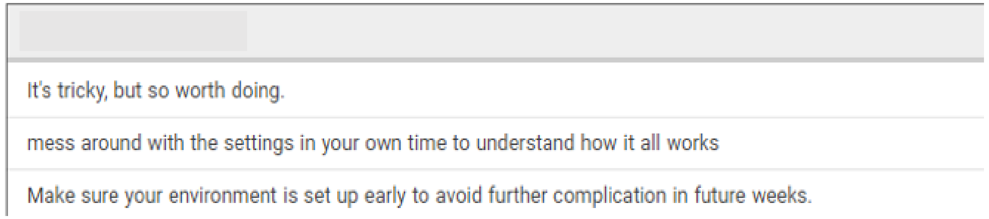
the networking in the VMs is fiddly

Initially getting my head rounf the VT was difficult howver it has slowly become more clear. I believe some of the course will be useful in industry however for me personally I would prefer to peruse a career in web development.

It's great.

used it before so it wasnt a new concept to me however i had never created my own little network and played around with packet capture and hacking concepts in a realistic manner before so i have really enjoyed the use of VT

1.a.v What advice would you give to another student taking this module regarding the use of VT?



It's tricky, but so worth doing.

mess around with the settings in your own time to understand how it all works

Make sure your environment is set up early to avoid further complication in future weeks.

References

- Du, Wenliang. Computer & internet security: a hands-on approach. Independently published, 2019.
- Salah, K., Hammoud, M. and Zeadally, S., 2015. Teaching cybersecurity using the cloud. *IEEE Transactions on Learning Technologies*, *8*(4), pp.383-392.
- Çakýroglu, Ü., 2014. Evaluating students' perspectives about virtual classrooms with regard to Seven Principles of Good Practice. South African Journal of Education, 34(2).
- Huang, A., 2019. Teaching, learning, and assessment with virtualization technology. *Journal of Educational Technology Systems*, *47*(4), pp.523-538.
- Ogunyemi, A. and Johnston, K., 2010. The use of virtual machines to support hands-on learning experiences in undergraduate systems-oriented courses. In Proc. 4th Int. Conf. Dynamic Informatics (pp. 3-5). South Africa: Monash University.