



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Getting Ready



Objectives

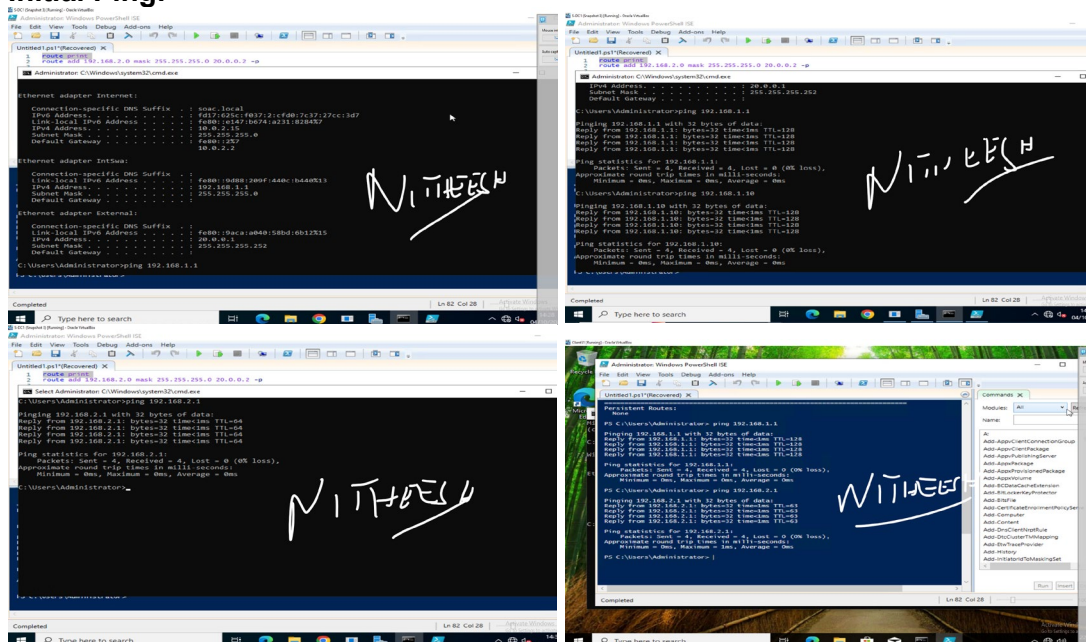
Note: Activity 1 is the base of all the other upcoming activities (Information Gathering, Vulnerability Assessment and Exploiting the Network Vulnerabilities). The objectives set to this activity need to be achieved overall by completing all the activities and demonstrating them during the scheduled time.

1. **Import and Start VMs:** Import the provided virtual machines into your virtualization platform. Power on the machines.
2. **Verify Network Configuration:** Perform the following network tests to confirm the VMs are correctly configured as per the provided network topology. Record the results for submission.
3. **Submit Evidence:** Capture screenshots of the test outputs and upload them to Moodle at the start of the assessment. This is part of your progressive coursework, and you are expected to work on it weekly following each lecture.
4. **Address Issues:** If the test results deviate from the expected outputs, upload the evidence to Moodle and consult your lecturer immediately.
5. **Setup Security-focused Operating System of your choice**
 - Add (For eg: Kali Linux) a security-focused OS to simulate assess to preform security measure in the network.
 - Assign a network address of your choice to the Security-focused OS(Kali Linux) to represent internal access in Swansea Network.
 - Connecting within Swansea Network should give you access to both Swansea and London Network.

Optional Changes: Considering the number of Virtual Machines, you might ignore ClientL1 in your Activities. For Testing Purposes from a Client Machine, use ClientS1. However, if you wish to include ClientL1 in your Topology/ Testing, you are more than welcome.

Outcomes of Activity 1

1. Initial Ping:



```

valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:27:68:c3 brd ff:ff:ff:ff:ff:ff
    altname enx0800272768c3
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 85507sec preferred_lft 74707sec
    inet6 fe80::2727:68c3:1:1:1:1/64 scope link
    valid_lft 85503sec preferred_lft 13503sec
    inet6 fe80::2727:68c3:1:1:1:1/64 scope link
3: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1b:53:86 brd ff:ff:ff:ff:ff:ff
    altname enx0800271b5386
    inet6 fe80::271b:5386:1:1:1:1/64 scope link
    valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1b:53:86 brd ff:ff:ff:ff:ff:ff
    altname enx0800271b5386
    inet6 fe80::271b:5386:1:1:1:1/64 scope link
    valid_lft forever preferred_lft forever
5: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1b:53:87 brd ff:ff:ff:ff:ff:ff
    altname enx0800271b5387
    inet6 fe80::271b:5387:1:1:1:1/64 scope link
    valid_lft forever preferred_lft forever
London:login@l-CD:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=127 time=1.29 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=127 time=0.442 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=127 time=1.43 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=127 time=0.513 ms
^C
-- 192.168.1.1 ping statistics --
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.442/0.820/1.233/0.355 ms
London:login@l-CD:~$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data:
64 bytes from 192.168.1.10: icmp_seq=1 ttl=127 time=5.01 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=127 time=0.937 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=127 time=0.788 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=127 time=1.23 ms
^C
-- 192.168.1.10 ping statistics --
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.788/1.931/5.012/1.751 ms
London:login@l-CD:~$

```

To import the given simulated network (OVA File) and test the configurations, troubleshoot the machines within the network ensuring the network is configured as stated.

Note: Refer to your Network Operating Systems and Services (ACCA5023) Module Contents.

To setup OS to assess the impact of insecure configurations within the given network.

- ✓ consider Information Security Elements, assessing risks to identify threats and vulnerabilities within the simulated network

Upcoming Activities: You will be continuing to test the network, assess the security posture and enhance the network security and making the network Cyber risk resilient.

ETHICAL STATEMENT

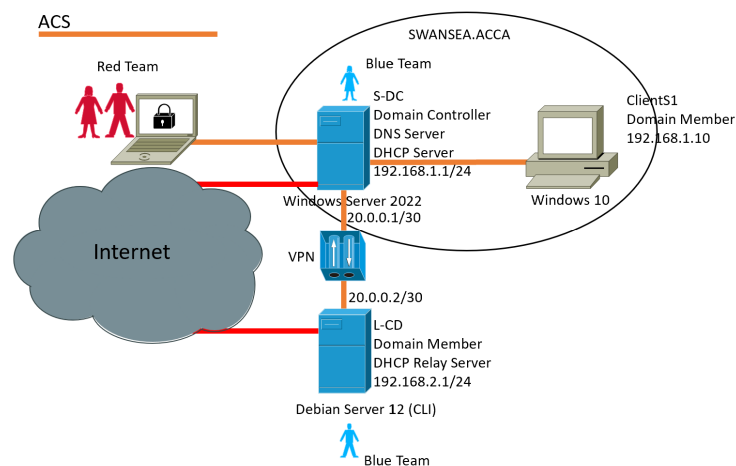
The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should get approval from your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Part 1: Test and Troubleshoot (if needed) the Network as per the topology

Part 2: Setup Security OS within the Network

Lab Topology



- The OVA File is shared with you by your Lecturer.

Part 1: Basic Settings

1. Power-On the Virtual Machines and Test their Connectivity

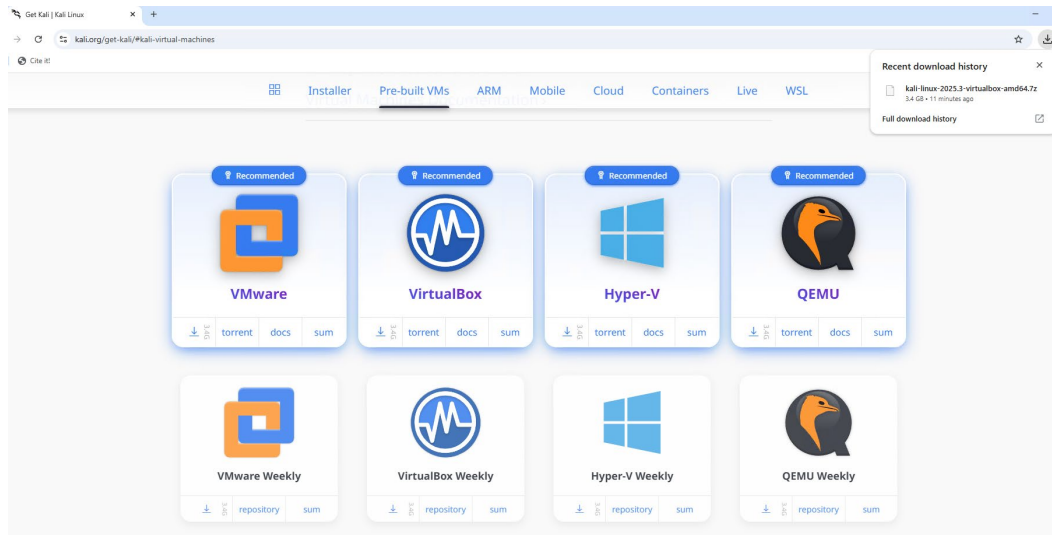
Useful Commands

- a. cmd – command prompt
 - b. ipconfig / ip address
 - c. ping "ip address"
 - d. ncpa.cpl – Network Adapters
 - e. route print
2. Capture a snapshot of the current VM state to back up your configurations using "Snapshot".

Important: Submit the screenshot in Moodle – as part of your Coursework deliverables

Part 2: Install Security OS

1. In this example, Kali Linux is used for description. However, you are open to use any Security related OS.
2. Download Kali Linux for Virtual Box



3. Install Kali Linux and assign Swansea Network IP Address
4. Test Connectivity

Reference:

https://www.youtube.com/playlist?list=PLddfEpDxAoTt8mx4VcThYm_hSDid1WjZd