



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)

Setting up the environment



Objectives

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.

To install the given simulated network (OVA File) and configure the machines within the network intentionally vulnerable to various Cybersecurity Attacks.

To Understand the impact of insecure configurations considering Information Security Elements, assessing risks, enabling to identify threats and vulnerabilities within the simulated network with upcoming activities, continuing to test the network, and enhance the network security and making the network Cyber risk resilient.

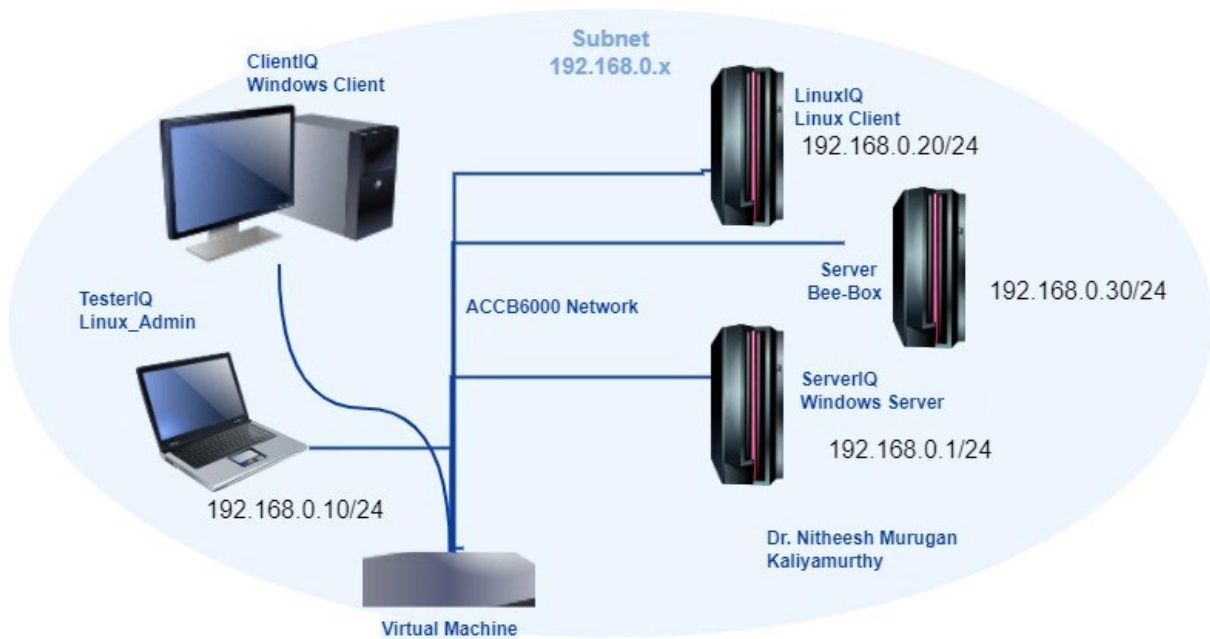
ETHICAL STATEMENT

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: Configure Basic Settings in all the VM's
Part 2: Configure Windows Server, Client, Ubuntu and Bee Box
Part 3: Documentation

Lab Topology



TesterIQ	Kali Linux	192.168.0.10/24	+ Labnet Internal Network + NAT	-	Kali	Kali
LinuxIQ	Ubuntu Linux	192.18.0.20/24	+ Labnet Internal Network	-	User1	Ubun7u
Server Bee-Box		192.168.0.30/24	+ Labnet Internal Network	-		
ServerIQ	Windows Server 2022	192.168.0.1/24	+ Labnet Internal Network	-	Administrator	P@ssw0rD
ClientIQ	Windows 10	DHCP	+ Labnet Internal Network	-	Administrator1	NotebookK@123

Sam Joe	s.joe P@\$\$w0rD
Murr Nat	m.nat P@\$\$w0rD
Dave Ralp	d.ral P@\$\$w0rD

Instructions for Virtual Machine Setup:

- + Lecturer has provided the OVA file containing the necessary virtual machines.
- + Configure the IP addresses for each VM according to the specified network topology. The initial passwords for the machines are provided in the table.

Important Notes:

- + Ensure that each machine's hostname, IP address, and network adapter settings are consistent with the addressing table provided above.
- + While core configurations such as IP addresses and network adapter settings must align with the lab requirements, other settings may be customized according to individual needs or specific project objectives.
- + If necessary, you may add additional network adapters; however, ensure that all machines are connected to the internal network Labnet to establish proper LAN connectivity. All machines should be able to successfully communicate within the network.

Part 1: Basic Settings

1. Verify that all virtual machines (VMs) are configured according to the specified settings. If discrepancies are found, make the necessary adjustments to align with the provided topology:
 - a. Network Adapters
 - b. IP Address and Subnets
 - c. Usernames and password
2. Test connectivity by pinging between the VMs. Ensure that all ping tests are successful.
3. Capture a snapshot of the current VM state to back up your configurations.

Part 2: Windows Server

1. Turn off the Internet Explorer Enhanced Security Configuration for both Administrators and Users.
Hint: Click on the Local Server in Server Manager
2. In Role based features, install the following
 - a. Telnet Server and Client.

b. IIS (Common HTTP Features)

3. Make sure the Server Manager tab is not starting automatically at logon.
4. Install a web browser of your choice
5. Turn off Firewall in Windows Server and Client
6. Install Active Directory – accb6000.local
7. Install DNS Server role. This Server will be the DNS Server for all the applicable VM's in the network. Make sure you create A Records, PTR Records and Reverse Lookup zones.
8. Install DHCP Server for the Windows Client
9. Install Web Server (IIS) Role and create <http://web.accb6000.local> website without any security (Disable Windows Internal Authentication)
10. Windows 10 Client: A domain-joined workstation that will receive a DHCP lease from the Windows Server.
11. Ubuntu (192.168.0.20): A Linux server with typical services (SSH, FTP, etc.).

Further Configurations

In Part 4, we are purposefully misconfiguring each system to include multiple security vulnerabilities that mirror real-world attack vectors. You may follow this and/or add your own misconfigurations depending on your plan for the demonstration. Some of the below asked mis configurations could be done later while attempting to exploit the vulnerabilities.

1. Disable Security Features (e.g., firewalls, antivirus, and automatic updates) on each system to make them susceptible to common attacks.
2. Disable the firewall, configure weak password policies, and enable insecure protocols (e.g., RDP without Network Level Authentication).
 - a. Weak Passwords: Set passwords that are easily guessable or do not meet complexity requirements.
 - b. Unpatched Systems: Avoid applying security updates to expose systems to known vulnerabilities.
 - c. Unrestricted Network Communication: Allow all machines to communicate without segmentation or restrictions.
3. Misconfigure IIS and DNS services to allow exploitation.
 - a. Recursive DNS queries, potentially leading to DNS amplification attacks.
 - b. Misconfigured Services: Enable and misconfigure services such as HTTP, DNS, RDP, SMB, FTP, and SSH, leading to common vulnerabilities like:
 - i. Directory browsing in IIS.
 - ii. Anonymous access in FTP.
 - iii. Open and unnecessary ports across the network.

4. In Windows 10, Join the domain with weak credentials, disable local security features, and configure SMBv1 to allow attacks.
5. In Linux Machine, Set up SSH with weak configurations, allow root login, and use insecure protocols like FTP and Telnet.
6. Ensure the vulnerable web applications (e.g., DVWA) are in low security mode, allowing exploits like SQL injection, cross-site scripting (XSS), and remote file inclusion (RFI).

Part 3: Documentation

- ✓ Record and document the process of creating these vulnerabilities in detail, noting each configuration change and the resulting vulnerability.
- ✓ Highlight how specific misconfigurations can lead to different types of attacks (e.g., misconfiguring SMBv1 opens the network to exploits like EternalBlue).
- ✓ Document the IP address and service configurations for each machine.
- ✓ Ping the vulnerable machines to ensure they are reachable.
- ✓ Check that all the services (e.g., IIS, FTP, SSH) are up, running and accessible.
- ✓ Ensure weak password policies are enforced.
- ✓ Verify network connectivity between the Kali Linux machine and all other machines.
- ✓ Record Video Snippets for your Demonstration