CSC 4570/5570 – IT Security
Fall 2020

Lab 1 - Introduction, Baseline Security, and Risk Assessment

Table of Contents

Table of Contents 1

Lab Descriptors 2

- Logistics 2
- Objectives 2
- Assumptions 2
- Outcomes 2
- CAE Topics Addressed 2
- NICE Framework Categories 3

Introduction 4

Lab Details 4

- Review of Systems 4
    - Windows 10 Workstation 4
    - VyOS Router 5
    - Windows Server 2016 5
    - Ubuntu Server 5
    - Windows 10 Management Laptop 6

Additional Information 6

Deliverables 6

Resources 7

- VyOS 7
- Networking 7
- VMware 7
- Linux 8
- Windows 8
- Other Services 8
- Documentation 8

Lab Descriptors

Logistics

Due Date:	September 09, 2020 at 11:59pm
Submission Location:	iLearn for documents, cyber range environment for systems
Points Available:	8

Objectives

1. Understand the overview of the labs for the semester.
2. Understand how to access the CEROC CyberRange environment and interoperate with systems assigned to the team.
3. Understand the importance of virus/malware scanning software through the installation/configuration of anti-virus/anti-malware software on multiple platforms.
4. Understand how to establish a baseline security level for the team's systems using common tools.
5. Understand basic incident response and change management procedures.

Assumptions

This lab assumes the successful completion of Lab 0 which was sent to all class members by email prior to the beginning of the semester. Among the topics covered:

- IP Addresses and Subnetting
- Basic Linux commands and Linux distribution organization
- Firewall / VyOS Basics
- Operating System Installation Basics

Outcomes

1. Students will demonstrate an understanding of the course flow by using the core systems which will support communication and artifact submissions throughout the semester.
2. Students will demonstrate an understanding of anti-virus/anti-malware tools through installation and configuration.
3. Students will demonstrate an understanding of their working environment through evaluation and reporting about the state of each inherited system.

CAE Topics Addressed

CSF - 4	Basic Risk Assessment
CSF - 10	CIAAA-NP
CSF - 13	Security Mechanisms
CSF - 14	Malicious Activity Detection
CSP - 1A - 1N	Core Cyber Principles
ISC - 1A	Non-Storage Devices
ISC - 2	Storage Devices
ISC - 3A-3B	Virtualization / Cloud
ISC - 5	Networks
ISC - 12A	OS and Application Updates
ISC - 13A	Vulnerability Windows
BNW - 4	Common Network Devices
BNW - 6	Network Services
BNW - 6	Network Applications
BNW - 8	Use of basic network administration tools
LSA - 2	User Accounts Management
LSA - 3	Command Line Interfaces
LSA - 4	Configuration Management
LSA - 5	Updates and Patches
LSA - 7	Managing System Services
LSA - 8	Virtualization
OSA - 2	User Accounts Management
OSA - 3	Command Line Interfaces
OSA - 4	Configuration Management
OSA - 5	Updates and Patches
OSA - 7	Managing System Services
OSA - 8	Virtualization
WSA - 2	User Accounts Management
WSA - 3	Command Line Interfaces
WSA - 4	Configuration Management
WSA - 5	Updates and Patches
WSA - 7	Managing System Services
WSA - 8	Virtualization

NICE Framework Categories

- Securely Provision (SP)
- Operate and Maintain (OM)
- Analyze (AN)

- Investigate (IN)

Introduction

This lab will provide you with an introduction to the environment which you will be working within for the duration of the semester.

Lab Details

You are a member of a managed service provider, Pompeii Strategies. The firm has been contacted to take over the IT infrastructure of a company which has been abandoned by the previous, internal IT team. During this lab exercise, your team will be required to review the current IT assets and return them to production operation. Limited information is available about the systems or access account. Management will provide all of the information they have; however, it will be quickly realized that the previous team left little documentation behind.

In addition to the corrective measures taken to return the environment to production levels, your team will:

- Learn how to make use of the company's virtualized environment
- Make use of issue management software
- Create documentation which can be used to maintain and/or recreate the environment
- Communicate with your team members and external stakeholders

Remember that your team is assisting an active company. The team cannot simply erase everything and start over (unless your firm wishes to be the next group fired). The team must systematically assess and document the infrastructure.

Review of Systems

VyOS Router

Credentials: vyos/vyos

The VyOS router is your connection to your upstream Internet Service Provider (ISP). Through the project (collection of labs) you will be making adjustments to this router to accommodate operational needs and special requests. Critical work:

1. Ensure that the username and password provided will provide administrative access to the system.
2. Change the default admin (vyos) password to something secure. This must meet whatever password criteria that you are willing to set for the company.

3. **The previous router was destroyed, and this was set up as a replacement. However, all the configuration was lost and must be set up manually to give your network internet access!**
    a. Check the resources at the end of this document to find VyOS's documentation
    b. Set eth1 (WAN) to gain an IP address from DHCP
    c. Set eth2 (LAN) to have a static IP address of 192.168.teamnum.1/25
    d. Set eth3 (DMZ) to have a static IP address of 192.168.teamnum.129/25
    e. Setup NAT rules for both LAN and DMZ
    f. Setup system DNS to 192.168.1.2 (Domain Controller)
    g. Setup DNS forwarding for LAN subnet
    h. Setup DNS listen-address as LAN address (the .1 address)
    i. Setup DNS allow from for LAN subnet
    j. Repeat g - i for DMZ
4. Run all updates on the router ensuring that the software is up to date.

Windows 10 Workstation

Credentials: user/password

This system will serve as your primary work system allowing interaction with the other servers in the company's IT infrastructure. Critical work:

1. Install Windows 10
    a. Make the username: **User**
    b. Create a password
    c. Finish installation
    d. Setup networking (IP will be 192.168.teamnum.3)
    e. Use your router for DNS for now.
    f. Add to domain after Windows Server setup

Windows Server 2016

Credentials: Administrator/P@ssw0rd!

The Windows Server 2016 system will provide basis domain infrastructure for the network through Active Directory Services and Domain Name Services. Your domain name will be **pompeii.local**. Critical work:

1. Create an administrative password
2. Add both Active Directory and DNS roles
3. Promote server to primary domain controller
4. Create a new forest with "pompeii.local" as the domain name

Ubuntu Server

Credentials: user/toor

1. Get familiar with the ubuntu environment.
    a. Test out some of the commands from Lab 0
2. Add a new user that has “sudo” privileges (add one per team member).
3. Make sure that networking is set up properly.
    a. IP should be 192.168.teamnum.130
    b. Make router the DNS server.
4. Install Apache2
5. Check user permissions and accounts (remove old sudo users).
6. Check and install updates.

Windows 10 Management Laptop

Credentials: user/password

The Windows 10 Management Laptop will not be connected to the domain. This is your device that will be used when you are not in the office and for other labs.

Additional Information

Note that all of the activities in this lab and the following labs will highlight one or more of the principles of

- Separation (of domains/duties)
- Isolation
- Encapsulation
- Modularity
- Simplicity of Design
- Minimization of Implementation
- Open Design
- Complete Mediation
- Layering (Defense in Depth)
- Least Privilege
- Fail safe Defaults / Fail Secure
- Least Astonishment (Psychological Acceptability)
- Minimize Trust Surface (Reluctance to Trust)
- Usability

Deliverables

The following items must be submitted to iLearn for evaluation:
Only submit PDFs. It will not be graded if it is not in a PDF.

1. A well-documented changelog that you will update and submit for each lab **(This is a separate document)**.

2. In regards to your account management activities, which of the cybersecurity principles are in play?

3. In regards to the subnetting structure of your network, which of the cybersecurity principles are in play?

4. Screenshot the results from this command on the vyos router: **show configuration commands**

5. Screenshot confirming network connectivity per machine. (Screenshot of Youtube or using the command wget google.com)

In addition to the deliverables, your team's environment will be evaluated through various automated and manual review processes.

Resources

VyOS

- VyOS configuration overview - https://docs.vyos.io/en/latest/configuration-overview.html
- VyOS ethernet configuration documentation - https://docs.vyos.io/en/latest/interfaces/ethernet.html
- Video of sample config: https://youtu.be/o-m5ivd9EHY?t=491

Networking

- Subnetting Demystified Series - https://www.youtube.com/playlist?list=PL7a_V2KlyF_y3WNG8gxufyY6nm3QOkyn1

VMware

- VMware Web Client Introduction - https://www.youtube.com/watch?v=xqdW1qllw-Q (You may want to mute the sound; the music is obnoxious!)
- vSphere Web Client Support Videos - https://www.vmware.com/support/vsphere/vsphere-web-client-video.html

Linux

- Ubuntu Linux Tutorials - https://tutorials.ubuntu.com/
- Linux System Administration Basics - https://www.linode.com/docs/tools-reference/linux-system-administration-basics/#smtp-servers-and-email-issues
- Linux Security Tools - https://www.ubuntupit.com/best-20-linux-security-tools-recommendation-from-the-linux-experts/

Windows

- Windows Server 2016 Tutorial Step by Step Full - https://www.youtube.com/playlist?list=PLcRhfKiWZmM9F7lY6DRXVwiYpNB2RO6F9
- Using Windows Admin Tools Like a Pro Series - https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/
- TutorialsPoint Windows Administration Tutorials - https://www.tutorialspoint.com/listtutorials/windows/administration/1

Documentation

- Cyborg Systems - Documentation is the Most Valuable Thing You Do - http://cyborginstitute.org/projects/administration/documentation/