**Nmap Enumeration**

**Lab Overview**

For this lab, we will simulate enumeration of a LAN network. When a system administrator (or attacker) wishes to find what vulnerabilities are present on a LAN, they will perform a number of different tasks to gain different information about the target LAN. This process of gathering information about the target is known as enumeration. Enumeration is often essential in protecting or gaining a foothold on a target LAN environment.

To get started with enumeration, we will be using a common network mapping tool Nmap to perform scans on our target LAN. Nmap is very configurable and can be used to get very specific information about network configurations. It also can be used to scan entire ip ranges of all 65535 ports available.

**DISCLAIMER**

Doing this creates a lot of network traffic. It can also cause damage if the target LAN has not been configured correctly. For this reason, it is very important to only perform nmap scans on ip addresses that you have permission to scan. Use nmap at your own risk, and know what you are targeting before you run the scan.

**Before you start, you will need to complete with the following setups (If you have complete some steps before, you can skip them):**

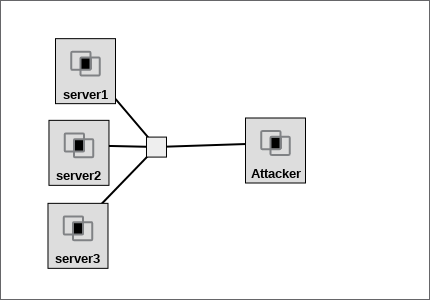
1. Setup user account on GENI and join a Project. (see Setup-User)
2. Setup Lab in GENI (see Setup-Lab). The RSpec file location is shown as follows.
3. Establish SSH connections from your host to the Attacking machine in the Lab (see Setup-Lab)

**RSpec File Location:**

<https://raw.githubusercontent.com/informationcomputerscience/EdGENI/master/Rspec-Files/NmapEnumeration-Rspec.txt>

**Network Topology**

The network for this lab will consist of 4 machines connected together in a LAN configuration. Our Attacker machine will act as our remote administrator who is conducting the enumeration. The purpose of the 3 other machines will be unknown to the administrator, and will be running various services commonly found on a LAN.



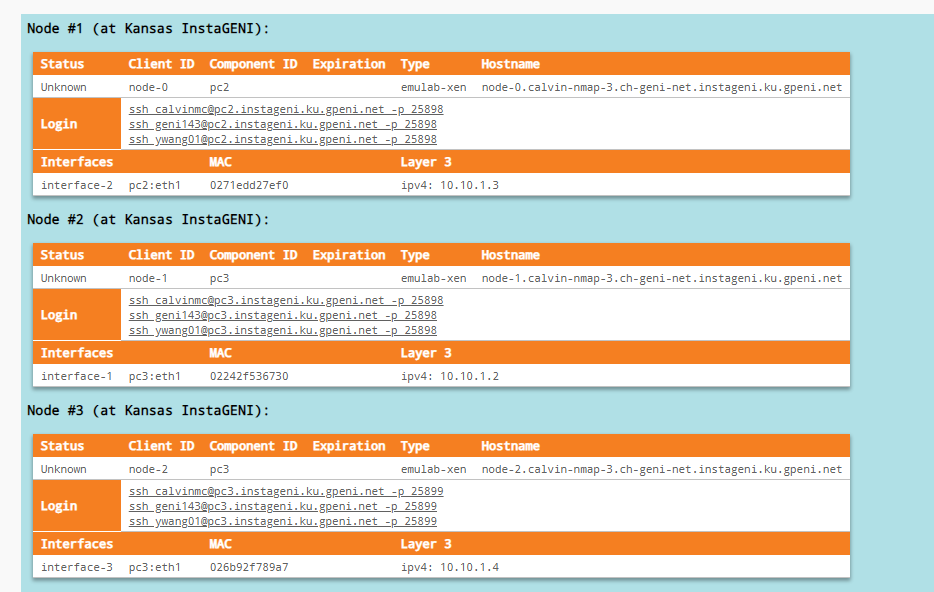
**Useful Information: Nmap Reference Manual**

[**https://nmap.org/book/man.html**](https://nmap.org/book/man.html)

**Task 1 - Understand our goal**

Since we will be pretending the Attacking machine is not apart of the LAN, we will run nmap from the attacking machine to perform enumeration. Nmap is very configurable, and can be ran with many different settings to find different information.

Our goal as a administrator, is to find what vulnerabilities might be on the LAN and report our findings. The 3 unknown machines will be running various services that could introduce potential vulnerabilities to the target LAN especially if running out of date software. We need to identify the IP range of the 3 machines to clearly define our target.

****

In the Slice Resources of the GENI Portal, you can find the ipv4 address of our three target machines. Each node has its own ip address and it is located at the very bottom line of the node details. It is located under the Layer 3 heading. You can see from the example above, Node 1 has an ip address 10.10.1.3, you machines will likely have a slightly different address.

Make note of the IP addresses of the three target machines. We will be using it in our Nmap scans and will also be using it as a reference to report our findings.

**Update Report: Start a report to document your goal and include the target machines IP addresses.**

**Task 2 - Enumerate with nmap**

Now that we know how to reach our Target, let's start performing our nmap scans against our individual hosts.

The general syntax for nmap usage follows this format:

nmap <options> <target\_IP>

You can add many different options to get different information. It is important to not blindly run commands that you do not understand. Perform various nmap scans against our target machines. Make note of the different information that can be found by each scan. You should be looking for open ports, services running, software, and version information. This will also be used to report our findings.

**NOTE:** the *nmap* will be installed to the attacker machine once your geni instance is ready. It may take a few minutes. That means running *nmap* command immediately after the attacker machine is ready could tell you nmap is not installed. Don’t worry. Wait for a few minutes and try the command again. It will work.

**Examples:**

nmap -sn 10.10.1.0/24

The above command will test whether all machines in the 10.10.1.0/24 subnet are alive (10.10.1.0–10.10.1.255). You may need to change this for the lab network.

nmap -A -oA nmap $targetip

This will scan the 1024 most common ports, run OS detection, run default nmap scripts, and save the results in a number of formats in the current directory.

nmap -v -p- -sT $targetip

This will scan all 65535 ports on $targetip with a full connect scan with verbose output. This scan could take a very long time.

It is important to conduct various scans to collect the most information possible. This is not a one size fits all scenario and the information you collect might vary based on which scans you conduct. This should be done in best effort.

**Update Report: Add any information your found in the nmap scans. I.E: open ports, services running, software, and version information.**

**Task 3 - Determine Machines**

Now that we have some information about the machines in our target LAN, we can use this information to determine the purpose of the 3 unknown machines. Remember our target LAN belongs to a business. These 3 machines (servers) are performing some function for the business, and we will make assumptions about these machines based on their functionality.

Use the nmap information (open ports, services running, software, and version information) to make these assumptions. If you do not know what the significance is of these details, perform a google search to find out what functionality is being performed.

For example, if your nmap scan of one of the machines looks like the screenshot below:



You can see this machine has tcp port 80 open and it’s service is http. If you did not know what the functionality of the http is used for, craft a google search similar to the one below:

**“http”+”80/tcp”** or something similar. This will take some digging to get an understanding of each services functionality.

**Update Report: Determine the business purpose of each machine, and state the functionality of every unique running service. Add this information to your report.**

**Task 4 - Determine Vulnerabilities**

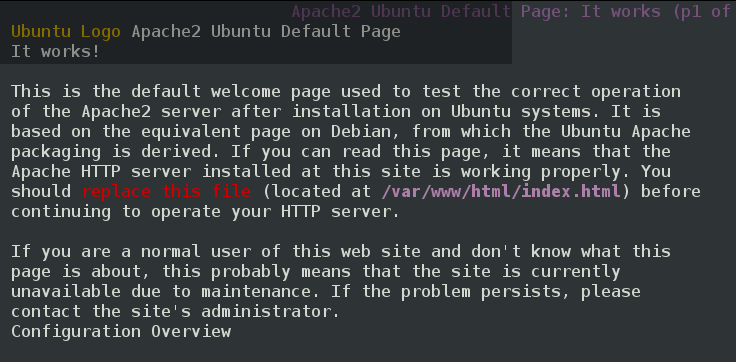
After completing tasks 1-3, we should have a better understanding of our target LAN. Referring back to our goal, we are looking for the vulnerabilities that may be present on our target LAN. Let’s do some more research about our nmap information (open ports, services running, software, and version information) and look for possible vulnerabilities. To do this research, a Google search will hopefully yield the results we are looking for.

For example: for the machine that has tcp port 80 open, we can guess that this server is hosting some sort of website for the business. We can use a Web Browser to see what website is being served to the internet. Open any browser, and travel to **http://<ip-of-machine-with-port-80>**

You should be looking at the default web page for apache2 running on ubuntu.

**TIP:** if you only have access to a command line environment, you can use **lynx** for text only web browsing. Lynx should be installed by default on the Attacker machine. From the terminal try: **lynx http://<ip-of-machine-with-port-80>**

You should see the text-only version of the default apache webpage. Lynx can be very useful for times that you do not have access to a GUI, or if you wish to safely view a website that might be hosting malicious code. Press q then y to exit the lynx browser.



After determining this machine is running Ubuntu linux, it is fairly safe to assume it is running PHP as a backend. Try to find out which version of PHP is being used. Try browsing to **http://<ip-of-machine-with-port-80>/phpinfo.php**

You should be able to find which PHP version is being used by this machine.

Try googling **“php <version>”+”vulnerabilities”**

We are looking for CVE numbered vulnerabilities. These have been publicly disclosed and verified the bigger vulnerability websites such as cvedetail.com. Make note of the CVE number, and the link from where it was found.

**NOTE:** It is entirely possible that there are many vulnerabilities for each of these services. Try to get the most important one, or one with the greatest severity. We are only trying to demonstrate the how the process of vulnerability hunting works, and not looking for a comprehensive search. There is also the possibility that there isn’t any vulnerabilities currently known for a particular service, or that we do not possess enough information to determine if the vulnerability is truly present. If you do not find one, just move on. Some should be fairly obvious with a few well crafted google searches. Just in the example above, you should realise how large the list of potential vulnerabilities actually is.

**Update Report: Determine any vulnerabilities present on the LAN and add them to your report. Report the php version number and any CVE number associated with it’s vulnerabilities. Report at least one other vulnerability and its CVE number.**

**Task 5 - Report your findings (Conclusion)**

In this lab we have covered quite a lot of material. We learned about nmap and how to use it to enumerate information from a target. We have learned how to determine the functionality of machines based on the information we enumerate. And we have learned how to take enumerated information and look for corresponding vulnerabilities. These are important skills for any cybersecurity professional or systems administrator looking to improve the security posture of a network.

While all of this useful information is great to learn, it is not very useful unless reported in a actionable way. Although our search for vulnerabilities has not been comprehensive, we should format our report in a way that is easy to disseminate information from. Instead of creating a large list of all the information collected in steps 1-4, we should section our report into separate sections about each machine, giving all of the details about each machine in its own section. Your report should follow the following format:

Goal & Target IPs

Machine 1 - IP address

Nmap enumeration details

Machine Functionality

Possible Vulnerabilities

Machine 2 - IP address

...

It may not be very clear why this is important at the moment, but in reality, the report is the most important piece for improving the security of a network. Security recommendations need to be actionable, and also well documented. Reports are frequently used by other people, such as the C-level executives, directors, administrators and managers. There may be a variety of different levels of technical understanding, but they all will need to take security seriously if they wish to improve the security posture. Having a report that is easy to follow will greatly increase the value of the document as well as the work performed by the security professional.