NMap – VM Environment

## Connect to the plass201jump.cit.byui.edu computer. As a cybersecurity feature, a [jump box](https://en.wikipedia.org/wiki/Jump_server) device is also known as a [bastion host](https://en.wikipedia.org/wiki/Bastion_host) when it is hardened against attack.

## From the jump box, connect to your team's Kali Linux device at 172.16.25.x

## Run Nmap scans from the Kali Linux device to **discover the following and report your results**:

1. How many total devices were discovered and are currently running on this network (try the -sn flags)?

|  |  |
| --- | --- |
|  | 218 |

## Which port numbers are open on each of your systems? (e.g. what port numbers are open on your Kali Linux VM, your Windows VM, and your DC-2 VM?)

|  |  |
| --- | --- |
|  | DC-280/tcp Kali 22/tcp Windows 21/tcp22/tcp135/tcp139/tcp445/tcp3389/tcp |

|  |  |
| --- | --- |
|  | http, ssh, ftp, ssh, msrpc, netbios-ssn, microsoft-ds, ms-wbt-server |

1. Which network services are running on those ports?

## What operating systems are running on your team's systems? (remember this is looking from the "outsiders" perspective where they may not have been told what is on those systems)

|  |  |
| --- | --- |
|  | Linux 3.2 - 4.9 Windows 10 1709-1909  Linux 2.6.32 |

## Create your own question of something else you would like to know about one or more of your team's systems and record your findings below. Here are a few suggestions to get you started:

## What other flags or switches are available on Nmap? What could it help you discover or learn about your team's systems?

## What scripts can you find to extend the capabilities of Nmap? What do they help you discover about your team's systems?

## How do red teams use NMap and other scanning tools to prepare for the next phase of the red team framework (Gain Access)Links to an external site.? What can you discover about your team's systems using these techniques?

## What other scanning tools are available on Kali Linux? What can you discover on these systems using those other scanning tools?

|  |  |
| --- | --- |
|  | What other flags or switches are available on Nmap? What could it help you discover or learn about your team’s systems? I learned about the “man nmap” command that can yield information about flags and switches. I also learned about nmap cheat sheets which contain common flags and switches we can use. |