

Scenario

As a security team member of Structureality Inc, we are working to improve our organization's security stance. We are currently tasked with performing asset discovery and finding open service ports. Open service ports are a threat vector. If discovered, an open service port is a target for attack. Adversaries may be able to gain access to and control over systems through open service ports. By evaluating the status of ports on systems, especially internet-exposed systems, we can work to reduce the attack surface by closing unnecessary ports.

In this lab, we will use a port scanner to detect open ports, enumerate service identities, and identify the operating system of targets. First, we will evaluate a border firewall from an outside location. Next, we will analyze the scan results from the Guest network. Finally, we will scrutinize the scan results of a server accessed from the Client network.

Understand wer environment

You will be working from a virtual machine named KALI hosting Kali Linux connected to the internal server subnet.

Objectives

This activity is designed to test wer understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

- 2.2 Explain common threat vectors and attack surfaces.
- 2.3 Given a scenario, analyze the results of a reconnaissance exercise.

Discovering outward facing open service ports

You are initially working from an external subnet (an internet simulation) in relation to the Structureality private network. You are performing a discovery and enumeration scan using nmap against the primary firewall of Structureality. Nmap is an open-source network scanner and security auditing tool.

1. Connect to the **KALI** and sign in as **root** using **Pa\$\$w0rd** as the password. (You are purposely signing in as root for this lab to access all of nmap's capabilities and avoid permissions issues. If we are working from a non-root account, we

must use sudo su to switch user context and elevate the Terminal window to root.) Open a Terminal window by selecting the **Terminal Emulator** from the Kali Linux toolbar (located at the top of the screen by default). This icon looks like a black computer screen with a cursor. Enter the following command to perform a port scan of the top 100 common ports of the company's border router Internet facing interface at 203.0.113.1, using the SYN scan method, while identifying the services on open ports and the OS, disable host discovery, and saving the results into a file.

```
nmap 203.0.113.1 -F -sS -sV -O -Pn -oN border-scan.nmap
```

This nmap command will perform several operations against the target:

- The "-F" parameter sets the scan to only test the top 100 popular ports.
- The "-sS" parameter sets the scan type to SYN scan. This is also the default scan type. The SYN scan is the most reliable scan option as it simulates the initial communication attempt from a valid client, while not completing the establishment of a full session. Therefore, the SYN scan has the best chance of determining the open state of TCP ports.
- The "-sV" parameter performs a version scan, which attempts to elicit the identity of services on open ports.
- The "-O" parameter attempts to identify the operating system.
- The "-Pn" parameter disables host discovery and assumes all IPs are actively in use.
- The "-oN" parameter saves the output of nmap to the specified filename (in addition to the screen display of the same).

```
(root@kali)-[~]
└─# nmap 203.0.113.1 -F -sS -sV -O -Pn -oN Border-scan.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-17 08:34 PDT
Nmap scan report for 203.0.113.1
Host is up (0.0013s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (92%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.80 seconds

(root@kali)-[~]
```

2. Enter the following command to display just the open port results:

```
grep open Border-scan.nmap
```

3. What port(s) are discovered as being open on this target? 25

```
(root@kali)-[~]
# grep open Border-scan.nmap
25/tcp open  smtp
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port

(root@kali)-[~]
#
```

Open service ports represent a threat vector to an organization. Especially ports that are discoverable from the internet. Open ports for services like email (i.e., port 25/tcp for SMTP) and web (i.e., port 80/tcp HTTP) can be targeted for attacks. If those services have vulnerabilities, an adversary may be able to compromise the system and gain remote control. You also discovered that port 22/tcp for SSH is open. This supports remote control/management/administration. But, is that necessary and warranted by the organization from the internet? If not, it should be closed. Generally, anything internet exposed needs to be hardened against any potential attack potential.

4. Enter the following command to display just the OS detection results:

```
grep OS Border-scan.nmap
```

```
(root@kali)-[~]
# grep OS Border-scan.nmap
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (92%)
No exact OS matches for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .

(root@kali)-[~]
#
```

What OS was detected on the target? FreeBSD

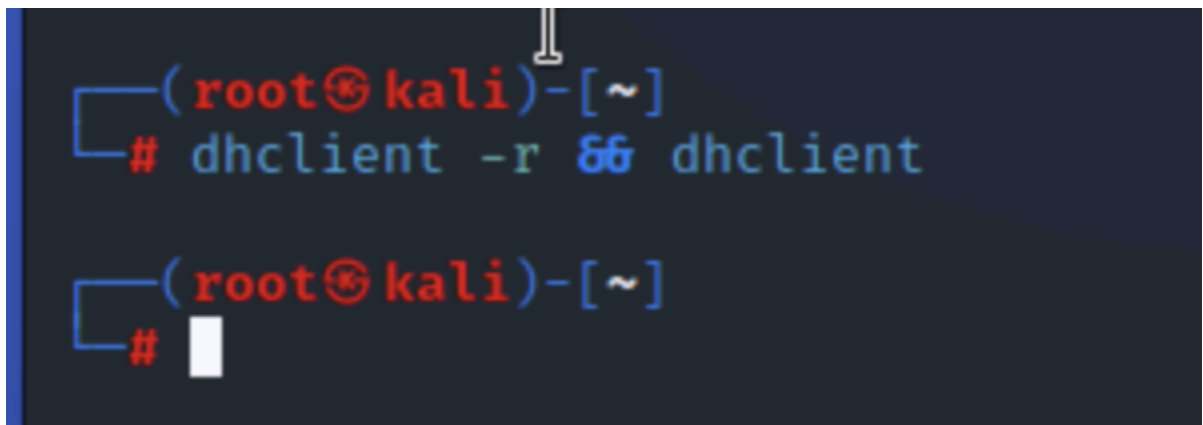
Being able to determine the OS of a target may allow an adversary to select a more effective exploit based on OS type and version. When possible, minimizing OS information made accessible to external entities would reduce this threat.

Discover threat vectors from a guest network

In addition to the threats from the internet, we should also be concerned about threat sources closer to home. A guest network may be a nice benefit to offer visitors, but if not properly configured, it could expose company resources to attack.

Change the network location of Kali workstation to perform an analysis of the attack surface from the guest network.

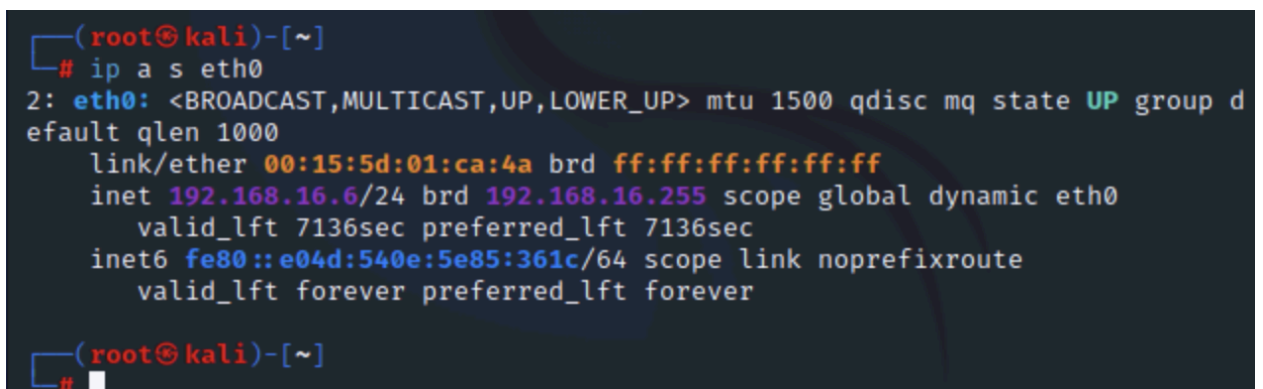
5. Select the **Resources** tab in the lab environment control pane. In the area for Kali, select the pull-down list under eth0, then select **VGUEST**. Select the **Instructions** tab in the lab environment control pane. The Terminal window should still be open. Enter **dhclient -r && dhclient**.



```
(root@kali)-[~]  
# dhclient -r && dhclient  
  
(root@kali)-[~]  
#
```

This command will release the previously assigned IP address from the internet subnet and obtain a new IP address in the server subnet.

6. Enter **ip a s eth0**. (This command displays the IP configuration information for just the eth0 interface.)



```
(root@kali)-[~]  
# ip a s eth0  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d  
efault qlen 1000  
    link/ether 00:15:5d:01:ca:4a brd ff:ff:ff:ff:ff:ff  
    inet 192.168.16.6/24 brd 192.168.16.255 scope global dynamic eth0  
        valid_lft 7136sec preferred_lft 7136sec  
    inet6 fe80::e04d:540e:5e85:361c/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
  
(root@kali)-[~]  
#
```

7. Enter the following command to perform a port scan against the guest network's gateway device at 192.168.16.254 of the top 100 common ports, using the SYN scan method, while identifying the services on open ports and the OS, and saving the results into a file.

```
nmap 192.168.16.254 -F -sS -sV -O -oN guest-scan.nmap
```

```
(root@kali)-[~]
# nmap 192.168.16.254 -F -sS -sV -O -oN guest-scan.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-17 08:52 PDT
Nmap scan report for 192.168.16.254
Host is up (0.00076s latency).
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  Unbound 1.17.1
80/tcp    open  http    OPNsense
443/tcp   open  ssl/https OPNsense
8000/tcp   open  http-alt OPNsense
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.93%I=7%D=7/17%Time=68791C44%P=x86_64-pc-linux-gnu%(GetRequest,94,"HTTP/1.0\x20301\x20Moved\x20Permanently\r\nLocation:\x20https://\r\nContent-Length:\x20\r\nConnection:\x20close\r\nDate:\x20Thu,\x2017\x20Jul\x202025\x2015:52:35\x20GMT\r\nServer:\x20OPNsense\r\n\r\n")%(HTTPOptions,94,"HTTP/1.0\x20301\x20Moved\x20Permanently\r\nLocation:\x20https://\r\nContent-Length:\x20\r\nConnection:\x20close\r\nDate:\x20Thu,\x2017\x20Jul\x202025\x2015:52:35\x20GMT\r\nServer:\x20OPNsense\r\n\r\n")%(RTSPRequest,1ED,"HTTP/1.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html\r\nContent-Length:\x20345\r\nConnection:\x20close\r\nDate:\x20Thu,\x2017\x20Jul\x202025\x2015:52:35\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<?xml version='1.0'\x20encoding='iso-8859-1'\x20?>\n<!DOCTYPE\x20html\x20PUBLIC\x20'-//W3C//DTD\x20XHTML\x201.0\x20Transitional//EN'\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20'http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd'\n>\n<html\x20xmlns='http://www.w3.org/1999/xhtml'\x20xml:lang='en'\x20lang='en'\n>\n\x20<head>\n\x20\x20<title>400\x20Bad\x20Request</title>\n\x20</head>\n\x20<body>\n\x20\x20<h1>400\x20Bad\x20Request</h1>\n\x20</body>\n</html>\n")%(FourOhFourRequest,B3,"HTTP/1.0\x20301\x20Moved\x20Permanently\r\nLocation:\x20https://nice%20ports%2C/Trinity.txt.bak\r\nContent-Length:\x20\r\nConnection:\x20close\r\nDate:\x20Thu,\x2017\x20Jul\x202025\x2015:52:40\x20GMT\r\nServer:\x20OPNsense\r\n\r\n")%(GenericLines,1ED,"HTTP/1.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html\r\nContent-Length:\x20345\r\nConnection:\x20close\r\nDate:\x20Thu,\x2017\x20Jul\x202025\x2015:52:41\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<?xml version='1.0'\x20encoding='iso-8859-1'\x20?>\n<!DOCTYPE\x20html\x20PUBLIC
```

8. Enter the following command to display just the open port results:

```
grep open guest-scan.nmap
```

```
(root@kali)-[~]
# grep open guest-scan.nmap

25/tcp open smtp Postfix smtpd
53/tcp open domain Unbound 1.17.1
80/tcp open http OPNsense
443/tcp open ssl/https OPNsense
8000/tcp open http-alt OPNsense
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

(root@kali)-[~]
#
```

What is the name of the service found on several open ports? Enter the exact name in the text box below: **OPNsense**

The service detected on ports 80, 443, and 8000 is the firewall. These ports can be used to access the firewall's management interface. It is not a secure deployment if a guest network member can access the management interface of the company firewall. These ports should be closed on the guest network. Keep in mind, that some ports should remain open to support valid communications, such as DNS (53), web (80/443), and email (25/465/587 (SMTP), 110/995 (POP3), 143/993 (IMAP)).

9. Enter the following command to display just the OS detection results:

```
grep OS guest-scan.nmap
```

What is the OS discovered on the target? FreeBSD

Discover the attack surface of the internal network

Guest network members are usually temporary visitors. But, what about the long term risk of internal entities - both computers and users? Scanning internal network systems for open service ports can reveal aspects of the internal attack surface. In this exercise, we will position our Kali workstation in the Client subnet, but scan a system in the Server subnet.

10. Select the **Resources** tab in the lab environment control pane. In the area for Kali, select the pull-down list under eth0, then select **vLAN_CLIENTS**. Select the **Instructions** tab in the lab environment control pane. The Terminal window should still be open. Enter **dhclient -r && dhclient**. Enter **ip a s eth0**.

```
(root@kali)-[~]
# dhclient -r && dhclient
Killed old client process

(root@kali)-[~]
# ip a s eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:ca:4a brd ff:ff:ff:ff:ff:ff
    inet 10.1.24.66/24 brd 10.1.24.255 scope global dynamic eth0
        valid_lft 691186sec preferred_lft 691186sec
    inet6 fe80::e04d:540e:5e85:361c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[~]
#
```

11. Enter the following command to perform a port scan against the legacy server in the Server network of the top 100 common ports, using the SYN scan method, while identifying the services on open ports and the OS, and saving the results into a file.

```
nmap 10.1.16.2 -F -sS -sV -O -oN server-scan.nmap
```



```

(root@kali)-[~]
# nmap 10.1.16.2 -F -sS -sV -oN server-scan.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-17 09:09 PDT
Nmap scan report for 10.1.16.2
Host is up (0.0016s latency).
Not shown: 88 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         hMailServer smtpd
80/tcp    open  http         Microsoft IIS httpd 10.0
111/tcp   open  rpcbind      2-4 (RPC #100000)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  imap         hMailServer imapd
443/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: structureality)
587/tcp   open  smtp         hMailServer smtpd
2049/tcp  open  mountd       1-3 (RPC #100005)
3306/tcp  open  mysql        MySQL 5.5.5-10.11.3-MariaDB
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2012|7 (98%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7::-:professional
Aggressive OS guesses: Microsoft Windows Server 2016 (98%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (93%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows 7 Professional (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Hosts: mail.structureality.com, MS10; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.65 seconds

(root@kali)-[~]
#

```

12. Enter the following command to display just the open port results:

```
grep open server-scan.nmap
```

What services are discovered to be accessible over open ports on this target?

```

(root@kali)-[~]
# grep open server-scan.nmap
25/tcp    open  smtp         hMailServer smtpd
80/tcp    open  http         Microsoft IIS httpd 10.0
111/tcp   open  rpcbind      2-4 (RPC #100000)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  imap         hMailServer imapd
443/tcp   open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: structureality)
587/tcp   open  smtp         hMailServer smtpd
2049/tcp  open  mountd       1-3 (RPC #100005)
3306/tcp  open  mysql        MySQL 5.5.5-10.11.3-MariaDB
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

(root@kali)-[~]
#

```

The number of open service ports on this server is significant. While many of these services may be present for a valid reason, that needs to be verified. Any necessary service should be configured to use encrypted communications, even internally. Also, notice that all of these service ports are discoverable as open (and service versions elicited) because there is no firewall separating the Client and Server networks. This is evidence of a lack of effective network segmentation. It needs to be recognized that internal systems represent a real threat vector. An insider can cause just as much harm as an external intruder.

13. Enter the following command to display just the OS detection results:

```
grep OS server-scan.nmap
```

```
(root@kali)~# grep OS server-scan.nmap
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7::-professional
Aggressive OS guesses: Microsoft Windows Server 2016 (98%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (93%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows 7 Professional (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Hosts: mail.structureality.com, MS10; OS: Windows; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

The Windows Server 2016 OS has reached its EOL (End of Life) on Jan 11, 2022. This means it is no longer considered an actively developed and supported OS. However, it may continue to receive security updates through Jan 12, 2027. At that date, it will be labeled EOSL (End of Service Life). This system should be slated for replacement before it reaches the EOSL date.

14. What is a threat vector? A pathway that could support an intrusion attempt
15. What is an attack surface? The collection of exposed vulnerabilities
16. What nmap parameter option performs a scan which displays service identification? -sV
17. Where can threats originate? Externally, Internally, Third-party software
18. What are two primary response options to the discovery of an open port hosting an insecure service? Close the exposed port, Configure service encryption