



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)**

### Information Gathering



## Objectives

**Note 1:** To proceed with Activity 2, completion of Activity 1 is required, which includes the following tasks:

- Testing the existing network
- Installing a security operating system

The objectives of this activity must be fully achieved by completing all assigned tasks and demonstrating them during the scheduled session.

**Recommendation:** It is advised to complete the activities outlined in this document between Week 3 and Week 4.

1. Understand multiple ways to Gather Information both Actively and Passively.
2. Scan your Network using Tools to identify the Services and its possible vulnerabilities.

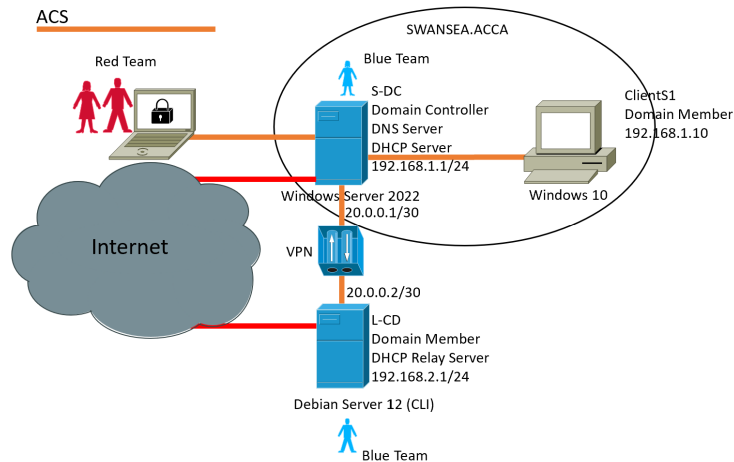
**Optional Changes:** Considering the number of Virtual Machines, you might ignore ClientL1 in your Activities. For Testing Purposes from a Client Machine, use ClientS1. However, if you wish to include ClientL1 in your Topology/ Testing, you are more than welcome.

## 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.

## Lab Topology



### PART 1: Recon a Network

Prior to start this activity, it is always recommended to capture a snapshot of the current VM state to back up your configurations using “Snapshot”.

#### Gathering Information on [www.itsecgames.com](http://www.itsecgames.com)

We will use `ping`, `tracert`, and `nslookup` (or `dig`) in Kali to passively gather details about a remote server's IP, network path, MTU, and DNS infrastructure, to understand attacker's reconnaissance for exploits like DoS or DNS-based attacks.

#### 1. Basic Ping to Resolve IP and Test Connectivity

*Why? Pinging reveals if the server is online, its IP address, and round-trip times (RTT), aiding in planning attacks like DDoS by confirming responsiveness.*

#### Test ITSECGAMES.COM

```
C:\Users\Administrator>ping www.itsecgames.com

Pinging itsecgames.com [31.3.96.40] with 32 bytes of data:
Reply from 31.3.96.40: bytes=32 time=14ms TTL=255
Reply from 31.3.96.40: bytes=32 time=14ms TTL=255
Reply from 31.3.96.40: bytes=32 time=14ms TTL=255
Reply from 31.3.96.40: bytes=32 time=14ms TTL=255

Ping statistics for 31.3.96.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 14ms, Average = 14ms
```

```
(securityadmin@seclogin)-[~]
$ ping -c 4 www.itsecgames.com
PING itsecgames.com (31.3.96.40) 56(84) bytes of data.
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=1 ttl=255 time=14.8 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=2 ttl=255 time=14.6 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=3 ttl=255 time=14.6 ms
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=4 ttl=255 time=14.7 ms

--- itsecgames.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 14.577/14.682/14.828/0.092 ms
```

The `-c 4` flag limits to 4 pings.

ICMP Echo Requests (56 data bytes + 8 ICMP header = 64 total) get Echo Replies, showing IP (31.3.96.40), RTT, and 0% loss if reachable.

## 2. Discovering Maximum Transmission Unit (MTU) with Fragmentation Flags

*Why? MTU knowledge helps craft oversized packets for fragmentation attacks or optimize payloads.*

How? Use the `-M do` (Don't Fragment) flag with varying packet sizes.

```
C:\Users\Administrator>ping www.itsecgames.com -f -l 1400

Pinging itsecgames.com [31.3.96.40] with 1400 bytes of data:
Reply from 31.3.96.40: bytes=1400 time=14ms TTL=255
Reply from 31.3.96.40: bytes=1400 time=14ms TTL=255
Reply from 31.3.96.40: bytes=1400 time=15ms TTL=255
Reply from 31.3.96.40: bytes=1400 time=14ms TTL=255

Ping statistics for 31.3.96.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 15ms, Average = 14ms
```

`-f`: Sets the "Don't Fragment" (DF) bit.

`-l 1400`: Specifies 1400 bytes of data. This is the payload size.

**Total Packet Size:** 1400 (data)

```
(securityadmin@seclogin)-[~]
$ ping -M do -s 1400 -c 4 www.itsecgames.com
PING itsecgames.com (31.3.96.40) 1400(1428) bytes of data.
1408 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=1 ttl=255 time=17.7 ms
1408 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=2 ttl=255 time=14.7 ms
1408 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=3 ttl=255 time=14.9 ms
1408 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=4 ttl=255 time=16.9 ms

--- itsecgames.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 14.702/16.052/17.706/1.282 ms
```

```
(securityadmin@seclogin)-[~]  
$ ping -M do -s 1473 -c 4 www.itsecgames.com  
PING itsecgames.com (31.3.96.40) 1473(1501) bytes of data.  
ping: sendmsg: Message too long  
ping: sendmsg: Message too long  
ping: sendmsg: Message too long  
ping: sendmsg: Message too long  
  
--- itsecgames.com ping statistics ---  
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3078ms
```

Linux uses -M do -s 1400.

**-M do:** Sets the "Don't Fragment" (DF) bit in the IP header, ensuring the packet is not fragmented if it exceeds the MTU.

**-s 1472:** Specifies 1472 bytes of data in the payload.

**-c 4:** Limits the ping to 4 packets.

**Total Packet Size:** 1472 (data) + 8 (ICMP header) + 20 (IP header) = 1500 bytes.

This command works on Linux systems with a ping version that supports the -M option (e.g., iputils-ping). If successful (0% packet loss), it indicates the MTU is at least 1500 bytes.

Reflection Thoughts:

On getting the outcome,

"1400-byte ping succeeds, while 1473-byte ping fails with "Frag needed and DF set."

What is the reason?

### 3. Tracing the Route with Traceroute and Understanding TTLs

Why? Maps the network path, exposing routers for potential attacks.

How?

```
C:\Users\soac-nk>tracert itsecgames.com

Tracing route to itsecgames.com [31.3.96.40]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    172.29.1.254
  2  <1 ms    <1 ms    <1 ms    172.30.2.254
  3  <1 ms    <1 ms    <1 ms    172.30.200.2
  4  <1 ms    <1 ms    <1 ms    159.86.188.126
  5  1 ms     1 ms     1 ms     159.86.189.170
  6  2 ms     1 ms     1 ms     psba.bradss-sbr2.ja.net [146.97.41.6]
  7  5 ms     5 ms     5 ms     ae2.bradss-sbr2.ja.net [146.97.41.5]
  8  5 ms     5 ms     5 ms     ae27.londpg-sbr2.ja.net [146.97.33.33]
  9  5 ms     5 ms     5 ms     ae29.londhx-sbr1.ja.net [146.97.33.1]
 10  5 ms     5 ms     5 ms     ae0.londhx-ban2.ja.net [146.97.35.198]
 11  5 ms     5 ms     5 ms     ldn-b2-link.ip.twelve99.net [62.115.175.130]
 12  5 ms     5 ms     5 ms     ldn-bb2-link.ip.twelve99.net [62.115.120.238]
 13 12 ms    12 ms    12 ms    adm-bb2-link.ip.twelve99.net [62.115.137.235]
 14 10 ms    11 ms    10 ms    adm-b10-link.ip.twelve99.net [62.115.120.229]
 15 11 ms    11 ms    11 ms    195.90.97.126
 16 12 ms    12 ms    12 ms    195.90.97.171
 17 14 ms    13 ms    14 ms    ae20-r2-tb-abl01.transip.net [157.97.168.30]
 18 12 ms    13 ms    13 ms    80.69.64.5
 19 12 ms    12 ms    12 ms    178-18-84-1.colo.transip.net [178.18.84.1]
 20 14 ms    14 ms    14 ms    web.mmebvba.com [31.3.96.40]

Trace complete.
```

```
(securityadmin@seclogin)-[~]
$ traceroute itsecgames.com
traceroute to itsecgames.com (31.3.96.40), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  2.144 ms  1.862 ms  1.722 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
```

```
C:\Users\Administrator>tracert itsecgames.com

Tracing route to itsecgames.com [31.3.96.40]
over a maximum of 30 hops:

  1    14 ms    15 ms    14 ms    web.mmebvba.com [31.3.96.40]

Trace complete.

C:\Users\Administrator>tracert www.itsecgames.com

Tracing route to itsecgames.com [31.3.96.40]
over a maximum of 30 hops:

  1    14 ms    14 ms    14 ms    web.mmebvba.com [31.3.96.40]

Trace complete.
```

```
C:\Users\soac-nk>ping www.itsecgames.com -i 4 -n 1

Pinging itsecgames.com [31.3.96.40] with 32 bytes of data:
Reply from 159.86.188.126: TTL expired in transit.

Ping statistics for 31.3.96.40:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
(securityadmin@seclogin)-[~]
$ ping -t 4 -c 1 www.itsecgames.com
PING itsecgames.com (31.3.96.40) 56(84) bytes of data.
64 bytes from web.mmebvba.com (31.3.96.40): icmp_seq=1 ttl=255 time=14.7 ms

--- itsecgames.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 14.719/14.719/14.719/0.000 ms
```

### Uses TTL increments

each hop replies with "Time Exceeded" until the target responds.

Asterisks \* indicate blocked probes.

Reflection Thoughts:

On getting the outcome using different options in Ping command,

can you find out more options that you can use with ping to further dive into the network to identify more details?

#### 4. DNS Reconnaissance with Nslookup or Dig

Why? Reveals NS and IPs for DNS attacks (e.g., spoofing).

How?

```
C:\Users\Administrator>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> set type=a
> www.itsecgames.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:      itsecgames.com
Address:   31.3.96.40
Aliases:   www.itsecgames.com
```

```
> set type=cname
> www.itsecgames.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
www.itsecgames.com      canonical name = itsecgames.com
```

```
> set type=ns
> www.itsecgames.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
www.itsecgames.com      canonical name = itsecgames.com
itsecgames.com          nameserver = ns54.domaincontrol.com
itsecgames.com          nameserver = ns53.domaincontrol.com

ns54.domaincontrol.com  internet address = 173.201.74.27
ns54.domaincontrol.com  AAAA IPv6 address = 2603:5:22a2::1b
ns53.domaincontrol.com  internet address = 97.74.106.27
ns53.domaincontrol.com  AAAA IPv6 address = 2603:5:21a2::1b
> set type=a
> ns53.domaincontrol.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:      ns53.domaincontrol.com
Address:   97.74.106.27
```

In Linux

```
(securityadmin@seclogin)-[~]
$ dig itsecgames.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> itsecgames.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2948
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4000
;; QUESTION SECTION:
;itsecgames.com.                IN      A

;; ANSWER SECTION:
itsecgames.com.                15      IN      A      31.3.96.40

;; Query time: 8 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sun Oct 12 09:51:57 BST 2025
;; MSG SIZE rcvd: 59
```

```
(securityadmin@seclogin)-[~]
$ dig +short a itsecgames.com
31.3.96.40
```

```
(securityadmin@seclogin)-[~]
$ dig +short ns itsecgames.com
ns53.domaincontrol.com.
ns54.domaincontrol.com.
```

```
(securityadmin@seclogin)-[~]
$ dig +short a ns53.domaincontrol.com
97.74.106.27
```

```
(securityadmin@seclogin)-[~]
$ ping -c 4 ns53.domaincontrol.com
PING ns53.domaincontrol.com (97.74.106.27) 56(84) bytes of data.
64 bytes from ns53.domaincontrol.com (97.74.106.27): icmp_seq=1 ttl=255 time=14.7 ms
64 bytes from ns53.domaincontrol.com (97.74.106.27): icmp_seq=2 ttl=255 time=14.1 ms
^C
--- ns53.domaincontrol.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 14.111/14.413/14.715/0.302 ms
```

`dig` provides detailed DNS records.

`+short` simplifies output. Shows CNAME, A records, and NS IPs.

Pinging confirms reachability.

**Reflection Thoughts:**

What is so important in getting information like this?

Why do we get an output like this?

**For Additional Activities TO UNDERSTAND RECONNAISSANCE:**

Refer to Activity 2 Footprinting Annexure PDF File and continue.

Note: Some of the tools are outdated. Spend some time to identify recent tools and practice within the Virtual Environment.

Make sure you download the tools/software from valid sources.

|                                                                                                      |
|------------------------------------------------------------------------------------------------------|
| Part 1: Information Gathering and Reconnaissance Techniques                                          |
| <b>Use Web Data Extractor tool to extract data from web pages. (Web Scraping or Web Data Mining)</b> |
| <b>Use Email Tracker Pro to trace and track delivered email.</b>                                     |
| <b>Use TCP View tool to identify the processes running on a Machine.</b>                             |
| <b>Use Sublist3r tool to enumerate subdomains of Websites using OSINT</b>                            |
| <b>Use Recon -ng tool to gather information</b>                                                      |
| <b>Being Anonymous on the Internet</b>                                                               |

If you are confident enough on passive and active information gathering using Command Line Utilities and other tools, try those in your Virtual network and map the Network and its services.

## “SWANSEA.ACCA” - Network

### PART 2: Reconnaissance on Server swansea.acca

Apply techniques to the SWANSEA.ACCA network from Kali, targeting S-DC and L-CD.

This tutorial assumes Kali is on 192.168.1.0/24 with 192.168.1.2 as IP Address and can route via 20.0.0.0/30.

What is the Objective?

Identify (Recon) any internal/external vulnerable services (DNS, DHCP, IIS) within the Network.

#### 1. Basic Ping, MTU Discovery and Traceroute

*Why?*

*Test connectivity to S-DC (swansea.acca)*

*MTU for potential exploits.*

*Note: The MTU could be used during your further test while scanning the network.*

*Map paths*

*Find information about routing*

*Hints:*

*ping -c 4 swansea.acca*

*ping -M do -s 1400 -c 4 swansea.acca*

*ping -M do -s 1473 -c 4 swansea.acca*

*ping -c 4 l-cd.swansea.acca*

*ping -t 2 -c 1 l-cd.swansea.acca*

*tracert swansea.acca*

*dig swansea.acca*

Confirm MTU.

Could an attacker target IIS/DHCP on S-DC with this information?

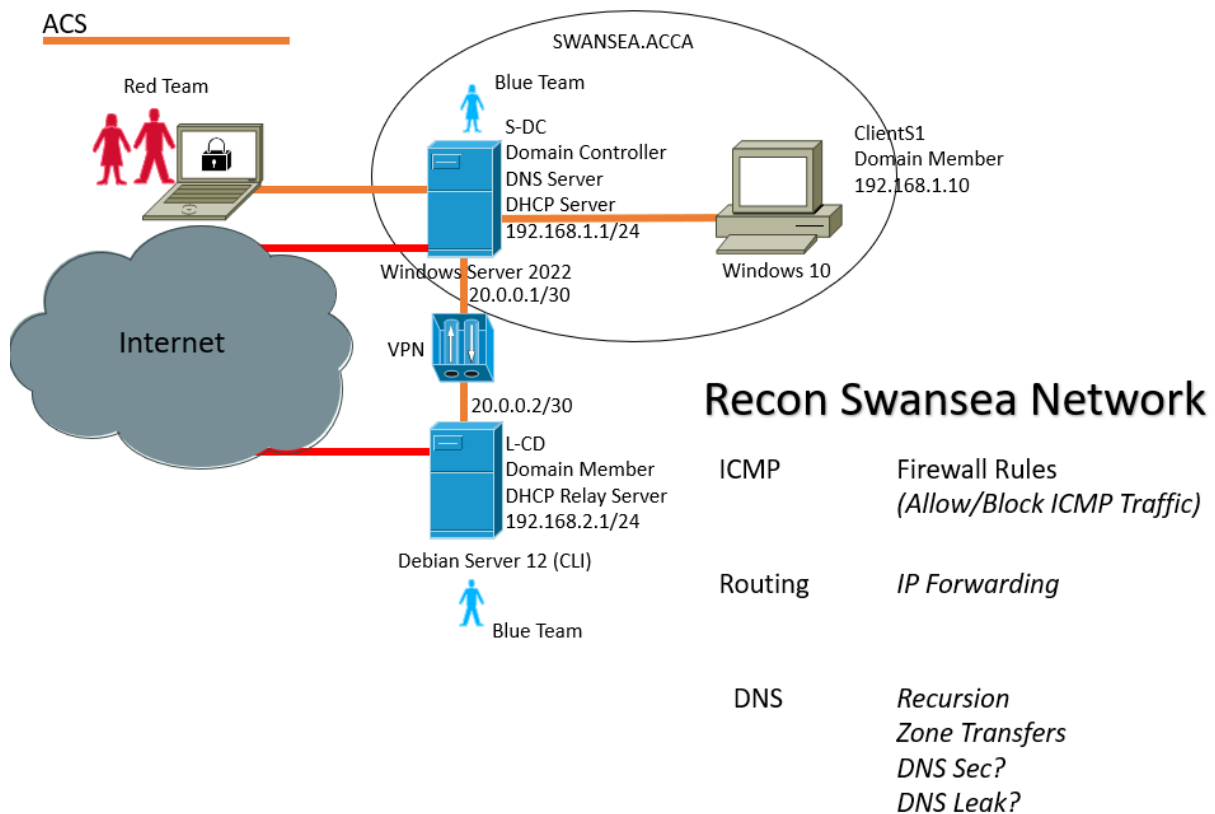
Confirm DNS is authoritative with a "aa" flag.

Confirm if the DNS reveals NS and L-CD IP.

## Mitigation Hints

By completing this Activity (2), you are evaluating the security posture of your Swansea Network's configuration. Below are some potential vulnerabilities you might identify, provided as a guide.

Keep in mind this is only a starting point. To achieve a "very good, excellent, or exceptional" outcome, it is essential to detect all vulnerabilities, beyond those listed below. (not limited to the below stated ones)



## Reference:

[https://www.youtube.com/playlist?list=PLddfEpDxAoTt8mx4VcThYm\\_hSDid1WjZd](https://www.youtube.com/playlist?list=PLddfEpDxAoTt8mx4VcThYm_hSDid1WjZd)