

Theme 3 Pre-Reading Packet: Offensive Security and Incident Response



Dr Diarmuid Ó Briain
Version: 1.0

Copyright © 2026 C²S Consulting

Licensed under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



Table of Contents

1 Objectives.....	4
2 Introduction.....	4
3 Methods of Attack.....	5
3.1 Brute force and dictionary attacks.....	5
3.2 Denial of Service attacks.....	6
3.3 Spoofing.....	7
4 The Anatomy of a Cyber attack.....	9
4.1 Reconnaissance.....	9
4.2 Initial Exploitation and Establishment Persistence.....	9
4.3 Installing Tools & Lateral Movement.....	9
4.4 Collection, Exfiltration, and Exploitation.....	10
5 The Kali Linux Virtual Machine Setup.....	11
5.1 System updates, localisation, and network configurations.....	12
5.2 Guest additions, package cleanup, and environmental baselining.....	14
6 Exercise.....	14
7 Bibliography.....	15

Table of Figures

Figure 1: SYN Flood.....	6
Figure 2: Anatomy of a Cyber attack.....	9
Figure 3: Kali Linux Desktop.....	11
Figure 4: VirtualBox Network Configuration.....	13
Figure 5: Kali Linux Network test.....	13

1 Objectives

By the end of this Pre-Reading Packet (PRP), you will be able to:

- Deconstruct the phases of a cyber attack from initial reconnaissance and credential exploitation through lateral movement, obfuscation, and data exfiltration.
- Differentiate between automated authentication exploits—specifically brute force and dictionary attacks—while identifying the predictable patterns that weaken user passwords.
- Explain the network mechanics of Denial of Service (DoS) and masquerading vectors, contrastingly evaluating SYNchronise (SYN) floods, Smurf amplification, and Man-in-the-Middle (MitM) traffic interception.
- Deploy, baseline, and validate a secure Kali Linux virtual infrastructure, establishing safe hypervisor network translation modes and verifying upstream connectivity via the command line.

 **Important Notice for Students:** This document contains the foundational definitions, adversarial attack vectors, and workstation setup steps required for Theme 3 (Offensive Security & Incident Response). You are expected to master this material independently; it will be directly tested in the Theme 3 Individual Readiness Assurance Test (iRAT).

2 Introduction

In the previous topics under Theme 2, the structural boundaries of security programmes were established through Governance, Risk, and Compliance (GRC). However, policies and risk registers are only half the battle; to truly defend an enterprise, an organisation must understand how real-world adversaries exploit vulnerabilities, and how to respond when a breach occurs.

This is the domain of Offensive Security and Incident Response.

This PRP establishes the foundational technical elements required for the upcoming interactive topics. Mastering these core mechanics, from automated authentication attacks and Denial of Service (DoS) protocols to the anatomical phases of a cyber attack, provides the critical baseline necessary to deploy a Kali Linux testing workstation and prepare for real-world scenarios, including network mapping and live crisis simulations.

3 Methods of Attack

This section establishes the foundational baseline of modern adversarial techniques, focusing on how attackers weaponise automation to exploit weak authentication.

3.1 Brute force and dictionary attacks

Used to find or break passwords for user accounts.

3.1.1 Brute Force Attack

A Brute force attack is a crude form of attack where every possible password is tried. This method is unlikely to be practical unless the password is relatively short. It also depends on there being no limit to the number of attempts.

3.1.2 Dictionary Attack

A dictionary attack is a technique for guessing passwords by trying to determine by searching likely possibilities. This is made possible as users often choose weak passwords or simply leave the default password. Users often choose weak passwords such as:

- 'password', 'passcode', 'admin' and their derivatives
- a row of letters from the qwerty keyboard -- *qwerty* itself, *asdf*, or *qwertyuiop*)
- the user's name or login name
- the name of their significant other, a friend, relative or pet
- their birthplace or date of birth, or a friends, or a relatives
- their car license plate number, or a friends, or a relatives
- their office number, residence number or most commonly, their mobile number
- a name of a celebrity they like
- a simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of the letters
- a swear word.

Dictionary attack programs can usually determine passwords where it is a single word found in dictionaries, given and family names, very short passwords (usually thought to be 6 or 7 characters or less), or any password meeting a too restrictive and so predictable, pattern (eg, alternating vowels and consonants). Repeated research over some 50 years has demonstrated that around 40% of user-chosen passwords are readily guessable by sophisticated cracking programs armed with dictionaries and, perhaps, the user's personal information. An example of such a program is '*John the Ripper*'.



3.2 Denial of Service attacks

These are an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name-servers.

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

DoS attacks are considered violations of the Internet's proper use policy, and also violate the acceptable use policies of virtually all Internet Service Providers (ISP). They also commonly constitute violations of the laws of individual nations.

3.2.1 SYN Flood attacks

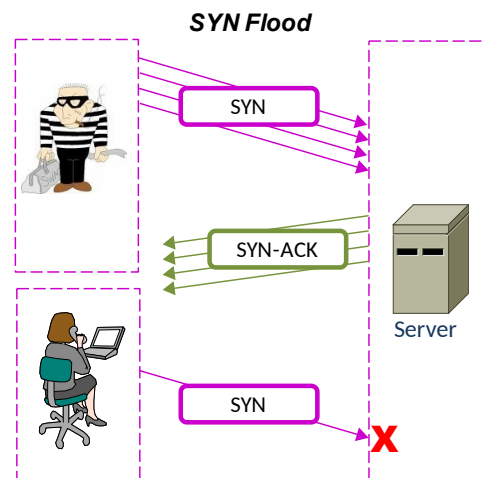


Figure 1: SYN Flood

A SYN flood is a form of DOS attack in which an attacker sends a succession of SYN requests to a target's system.

When a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

- The client requests a connection by sending a SYN message to the server
- The server acknowledges this request by sending SYN ACKnowledge (ACK) (SYN-ACK) back to the client
- The client responds with an ACK, and the connection is established

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol.

The SYN flood is a well known type of attack and is generally not effective against modern networks. It works if a server allocates resources after receiving a SYN, but before it has received the ACK.

There are two methods, but both involve the server not receiving the ACK. A malicious client can skip sending this last ACK message. Or by spoofing the source IP address in the SYN, it makes the server send the SYN-ACK to the falsified IP address, and thus never receive the ACK. In both cases the server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK.

If these half-open connections bind resources on the server, it may be possible to take up all these resources by flooding the server with SYN messages. Once all resources set aside for half-open connections are reserved, no new connections (legitimate or not) can be made, resulting in denial of service. Some systems may malfunction badly or even crash if other operating system functions are starved of resources this way.

3.2.2 Smurf attack

The Smurf attack is a way of generating significant computer network traffic on a victim network. This is a type of DOS attack that floods a target system via spoofed broadcast ping messages.

In such an attack, a perpetrator sends a large amount of Internet Control Message Protocol (ICMP) echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts (for example via a layer 2 broadcast), most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

3.3 Spoofing

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

3.3.1 Man in the Middle attacks

The MitM attack, in which an attacker spoofs Alice into believing the attacker is Bob, and spoofs Bob into believing the attacker is Alice, thus gaining access to all messages in both directions without the trouble of any cryptanalytic effort.

The attacker must monitor the packets sent from Alice to Bob and then guess the sequence number of the packets. Then the attacker knocks out Alice with a SYN attack and injects his own packets, claiming to have the address of Alice. Alice's firewall can defend against some spoof attacks when it has been configured with knowledge of all the IP addresses connected to each of its interfaces. It can then

detect a spoofed packet if it arrives at an interface that is not known to be connected to the IP address.

Many carelessly designed protocols are subject to spoof attacks, including many of those used on the Internet.

3.3.2 Spamming

Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognised form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, and file sharing network spam.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming is widely reviled, and has been the subject of legislation in many jurisdictions.

3.3.3 Sniffers

A sniffer attack is a snooping activity carried out by malicious users gaining access to network traffic, gathering it and either extract login information of users or use the packets in a form of replay attack.

4 The Anatomy of a Cyber attack

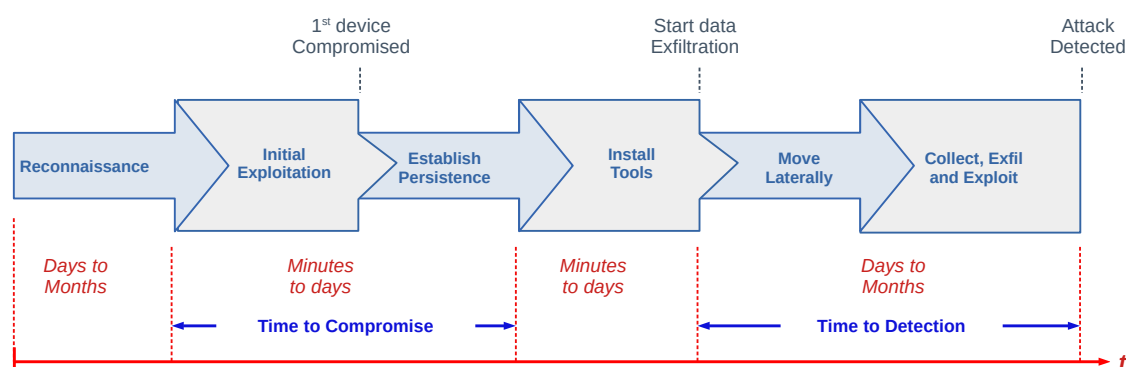


Figure 2: Anatomy of a Cyber attack

4.1 Reconnaissance

The first element of the anatomy of a cyber attack is reconnaissance. The attacker, often termed hackers, usually start by researching and gathering information about the target organisation. This phase is a search for useful vectors of attacks, network ranges, IP addresses, port numbers and domain names. Another avenue of research in the reconnaissance is a search for email addresses of key individuals throughout the organisation such as C-suite officers, managers and even employees. Vulnerable employees can be identified via phishing emails who may initially have been identified via corporate websites or personal contacts at trade shows or conferences.

The next reconnaissance step is a scan for vulnerabilities in the network, which is a process that can take some time. Once a viable attack vector has been identified via network vulnerabilities or employee email address, attackers proceed to an initial exploitation attack.

4.2 Initial Exploitation and Establishment Persistence

Once a foothold has been established via the network for example, the attack uses this to further infiltrate the organisation's network. To gain further access the attacking hacker requires access privileges. By using tools such as precomputed tables for caching the output of cryptographic hash functions, called rainbow tables, the hacker attempts to crack password hashes in an attempt to identify usable credentials to upgrade access to administrator privileges on either the foothold system or another nearby system.

4.3 Installing Tools & Lateral Movement

With the establishment of persistence the hacker has wider access to the network of systems and can traverse systems installing tools that leverage further access.

4.3.1 Move Laterally

The next phase of the anatomy of a cyber attack the move laterally or sometimes termed the expansion and obfuscation. Hackers intrude further on systems that may

not be related to the initial foothold. For example the foothold might be through WiFi on a printer and access is gained from it to a compromised computer that permits access to the control levels of the manufacturing operation. Installing malicious programs that enable the attackers to hide in multiple systems and regain access to the network even after one or more access vectors have been detected. This move laterally gives the hacker the space to obfuscate, or hide, the origins of the attack and establish exploit processes that avoid getting detected. The main purpose of obfuscation is confusing and disorienting the forensic experts and various tools and techniques such as spoofing, log cleaning, zombied accounts, and Trojan commands are used for this purpose.

4.4 Collection, Exfiltration, and Exploitation

With access achieved the final step is the collect and exfiltrate as much data as possible and exploit both the data and the access before detection and moved by cybersecurity experts to mitigate, remediate and block the attack.

5 The Kali Linux Virtual Machine Setup

Using the Kali Linux image provided on the website below, install **VirtualBox**, build the **.ova** image, install and run [1].

Login to the image with the default root username (**kali**) and password (**kali**).

There can be problems associated with the USB2.0 ports until the Oracle VirtualBox Guest Additions have been installed.

Adjust the Virtual screen to a preferred comfort level. For example:

View >> Virtual Screen 1 >> Scale to 200% (autoscaled output)

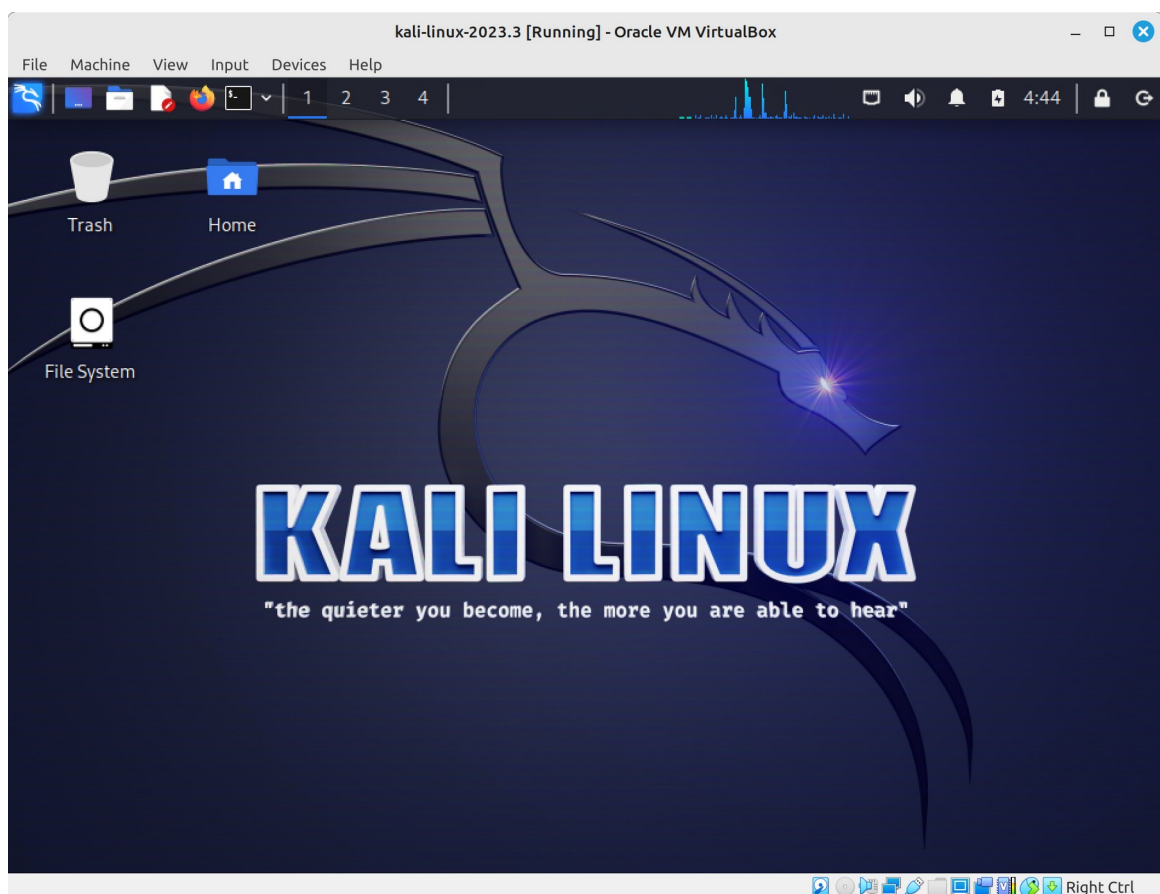


Figure 3: Kali Linux Desktop

5.1 System updates, localisation, and network configurations

5.1.1 Update and Upgrade

Run up a shell, use upgrade to download package information from the Kali Linux repository sources and then install available upgrades of all packages currently installed on the system. This can take some time.

```
(kali㉿kali)-[~]  
└─$ sudo apt update && sudo apt -y upgrade  
[sudo] password for kali: kali
```

5.1.2 Keyboard

Run up a shell and establish the keyboard layout. For example British English.

```
(kali㉿kali)-[~]  
└─$ setxkbmap -layout gb
```

```
(kali㉿kali)-[~]  
└─$ setxkbmap -query  
rules:          evdev  
model:          pc105  
layout:         gb
```

5.1.3 Network

Confirm connectivity with the Internet.

```
(kali㉿kali)-[~]  
└─$ ip addr list dev eth0 | grep 'inet ' | awk '{print $2}'
```

10.0.2.15/24

The IP Address is assigned by Network Address Translation (NAT) to the Virtual Machine (VM). It is possible to bridge the VM Ethernet interface (eth0) with the active interface on the host to get an IP address from the real world Dynamic Host Configuration Protocol (DHCP) Server.

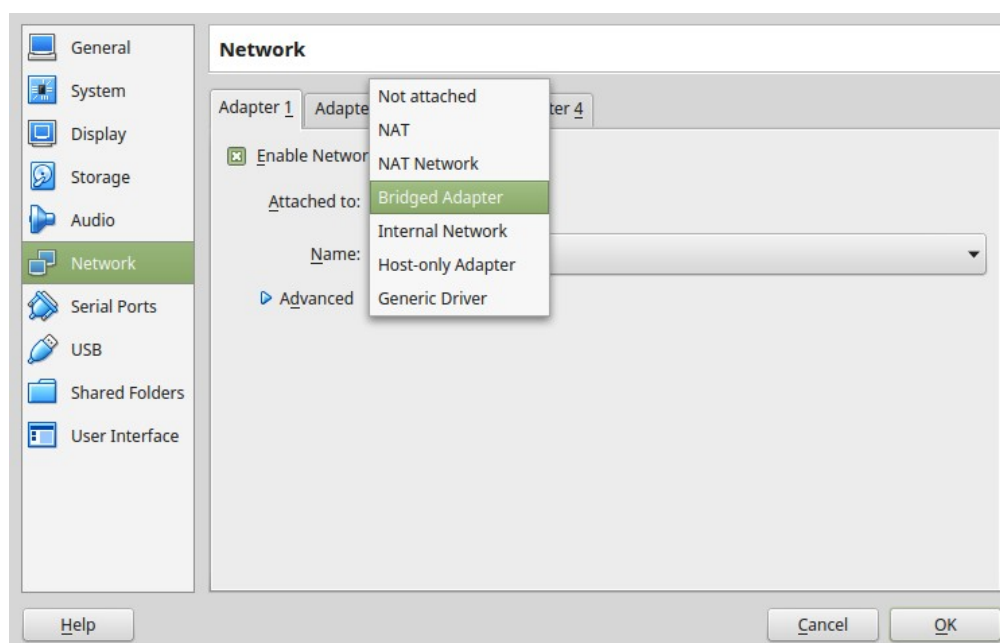


Figure 4: VirtualBox Network Configuration

Whichever system is used the IP Packet InterNet Groper (PING) test to the main google nameserver at 8.8.8.8 should elicit a response.

```
(kali㉿kali)-[~]  
$ ping -c3 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=18.7 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=16.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=16.4 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 16.193/17.113/18.729/1.146 ms
```

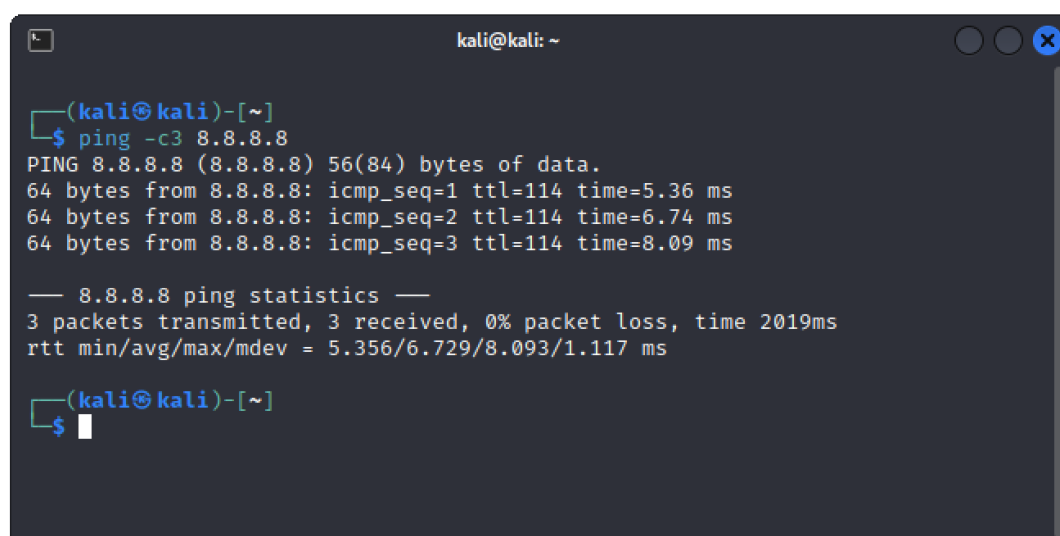


Figure 5: Kali Linux Network test

5.1.4 Change theme

Some prefer the light theme to the default dark theme. To change if required:

Settings >> Appearance >>

Style: Kali-Light

Icons: Flat-Remix-Blue-Light

5.2 Guest additions, package cleanup, and environmental baselining

5.2.1 Install Oracle Guest Additions

Oracle VirtualBox Guest Additions provides the VM device drivers and system applications to optimise the Kali Linux operating system for better performance and usability.

```
(kali㉿kali)-[~]  
└─$ sudo apt install -y virtualbox-guest-x11
```

5.2.2 Clean the install packages and reboot

Remove any packages that were automatically installed and are no longer required, then reboot the VM.

```
(kali㉿kali)-[~]  
└─$ sudo apt autoremove
```

```
(kali㉿kali)-[~]  
└─$ sudo reboot now
```

6 Exercise

Before the next class install VirtualBox on your computer.

Download the Kali Linux Virtual Machine.

Set it up and perform basic test to see that it is running.

```
(kali㉿kali)-[~]  
└─$ ping -c 3 8.8.8.8
```

```
(kali㉿kali)-[~]  
└─$ ping -c 3 8.8.8.8
```

```
(kali㉿kali)-[~]  
└─$ nmap --version
```

7 Bibliography

- [1] *Get Kali Linux: Virtual Machines*. OffSec. Accessed: Jun. 10, 2026. [Online]. Available: <https://www.kali.org/get-kali/#kali-virtual-machines>

This page is intentionally blank