



Ethical Hacking Essentials (EHE)

1 Master of Science in Cybersecurity



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023

EHE

Ethical Hacking Essentials



10100111010110100101
00101011101010110110
1001010001010010100
101011010110101101
0101101010101010101



10100111010110100101
00101011101010110110
1001010001010010100
10101101011010101101
0101101010101010101



10100111010110100101
00101011101010110110
1001010001010010100
10101101011010101101
0101101010101010101



10100111010110100101
00101011101010110110
1001010001010010100
10101101011010101101
0101101010101010101



10100111010110100101
00101011101010110110
1001010001010010100
10101101011010101101
0101101010101010101

Module 02

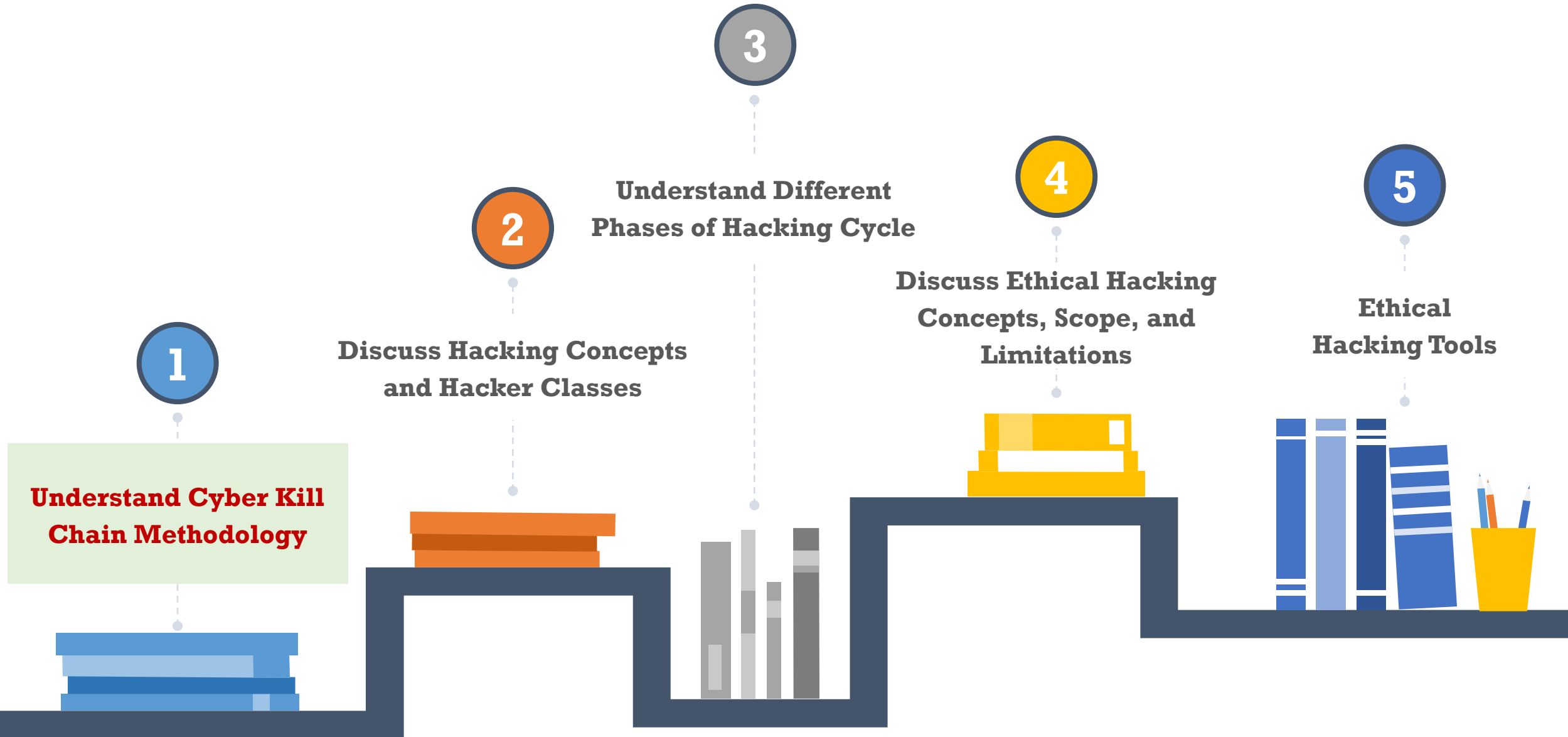
Ethical Hacking Fundamentals



Module Objectives

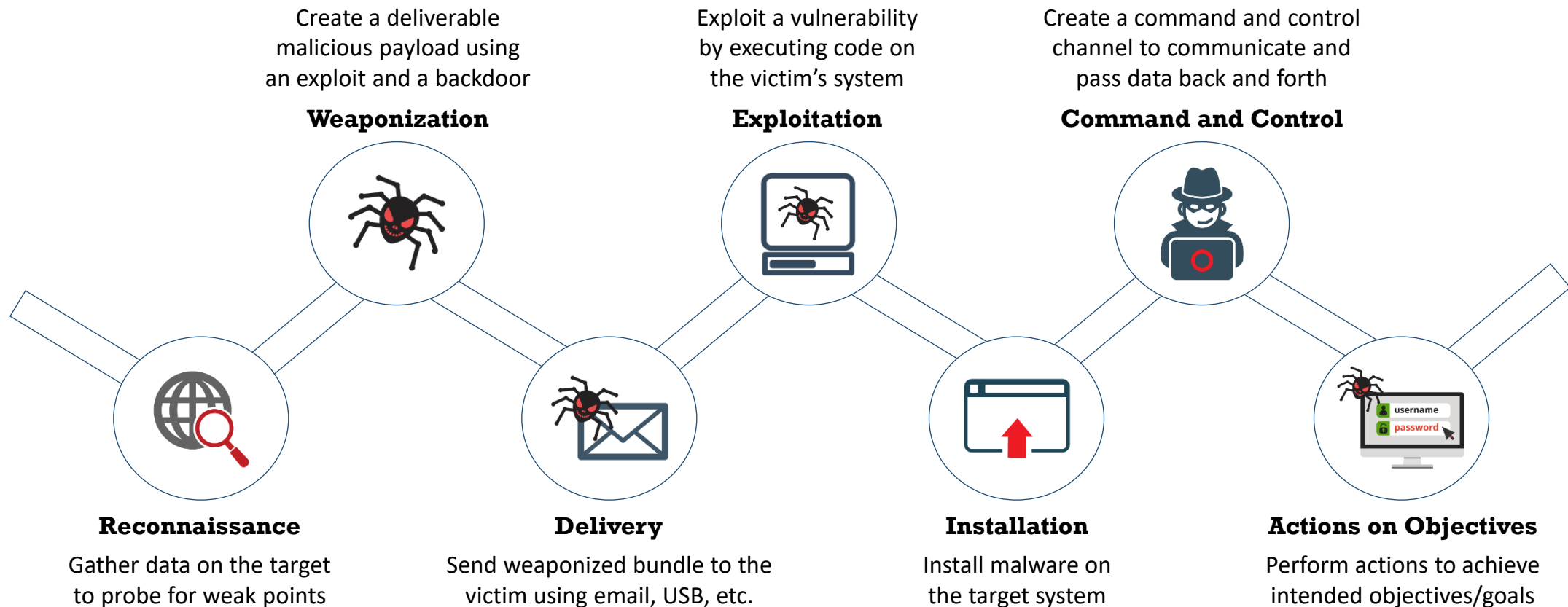
- 1 Understanding the Cyber Kill Chain Methodology
- 2 Understanding Tactics, Techniques, and Procedures (TTPs)
- 3 Overview of Indicators of Compromise (IoCs)
- 4 Overview of Hacking Concepts and Hacker Classes
- 5 Understanding Different Phases of Hacking Cycle
- 6 Understanding Ethical Hacking Concepts and Its Scope
- 7 Overview of Ethical Hacking Tools

Module Flow



Cyber Kill Chain Methodology

- ❑ The cyber kill chain methodology is a component of intelligence-driven defense for the identification and **prevention of malicious intrusion activities**
- ❑ It helps security professionals to understand the **adversary's tactics, techniques, and procedures beforehand**



Tactics, Techniques, and Procedures (TTPs)

The term Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors



Tactics

“Tactics” are the guidelines that describe the **way an attacker performs the attack** from beginning to the end



Techniques

“Techniques” are the **technical methods used by an attacker** to achieve intermediate results during the attack



Procedures

“Procedures” are **organizational approaches that threat actors follow** to launch an attack

Adversary Behavioral Identification



- ❑ Adversary behavioral identification involves the **identification of the common methods** or techniques followed by an adversary to launch attacks on or to penetrate an organization's network
- ❑ It gives the security professionals insight into **upcoming threats and exploits**

Adversary Behaviors



Internal Reconnaissance



Use of Command-Line Interface



Use of DNS Tunneling



Use of PowerShell



HTTP User Agent



Use of Web Shell



Unspecified Proxy Activities



Command and Control Server



Data Staging

Indicators of Compromise (IoCs)

Indicators of Compromise (IoCs) are the **clues, artifacts,** and **pieces of forensic data** found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure

IoCs **act as a good source of information** regarding the threats that serve as data points in the intelligence process

Security professionals need to **perform continuous monitoring** of IoCs to effectively and efficiently detect and **respond to evolving cyber threats**

01

02

03

Categories of Indicators of Compromise

Understanding IoCs helps security professionals to **quickly detect the threats** against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:



Email Indicators

- Used to send malicious data to the target organization or individual
- Examples include the sender's email address, email subject, and attachments or links



Network Indicators

- Useful for command and control, malware delivery, identifying the operating system, and other tasks
- Examples include URLs, domain names, and IP addresses



Host-Based Indicators

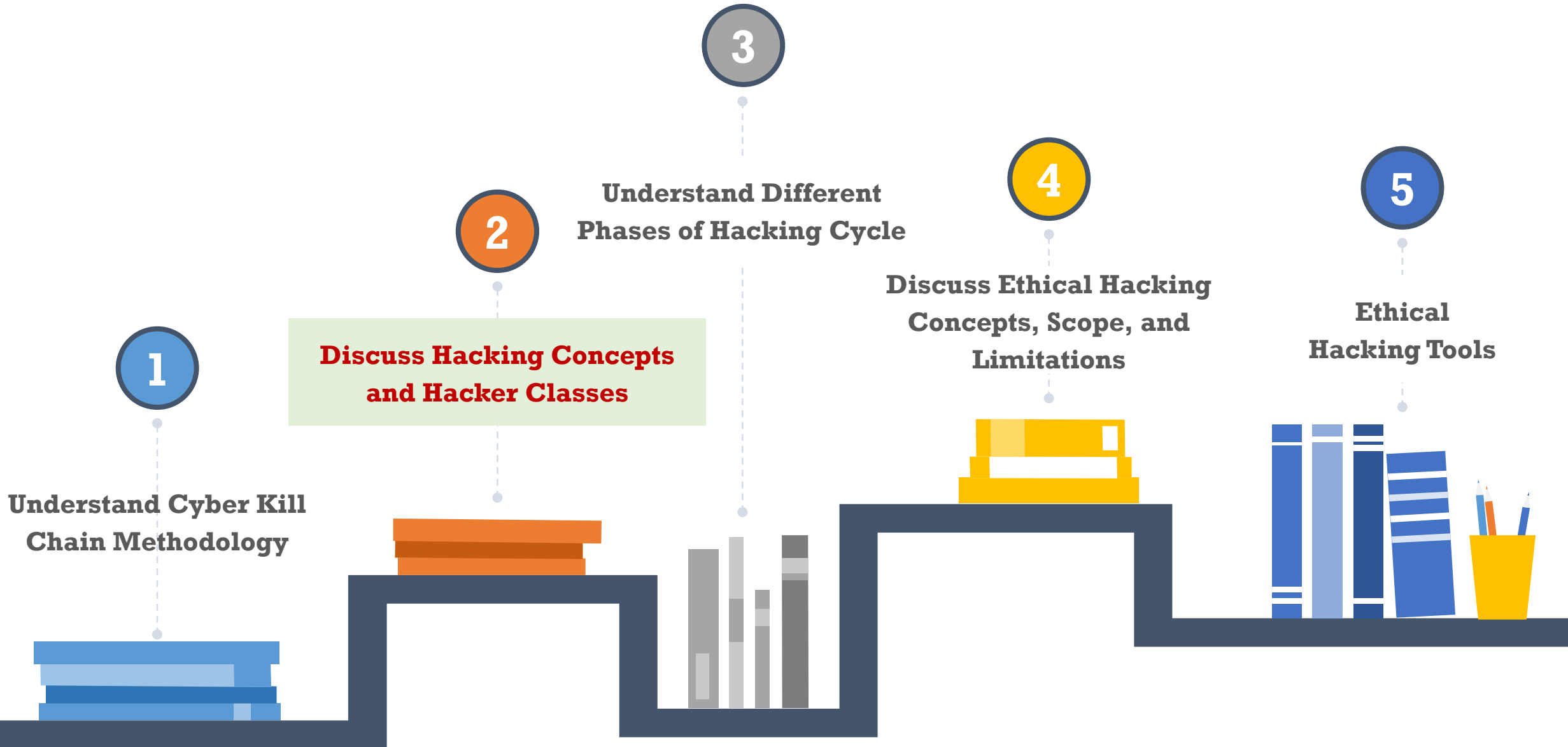
- Found by performing an analysis of the infected system within the organizational network
- Examples include filenames, file hashes, registry keys, DLLs, and mutex



Behavioral Indicators

- Used to identify specific behavior related to malicious activities
- Examples include document executing PowerShell script, and remote command execution

Module Flow



What is Hacking?



Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources



It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose



Hacking can be used to steal and redistribute intellectual property, leading to **business loss**

Who is a Hacker?

01

An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware



02

For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise



03

Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**



“

Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data

”

Hacker Classes/Threat Actors



Black Hats

Individuals with **extraordinary computing skills**; they resort to malicious or destructive activities and are also known as crackers



White Hats

Individuals who use their **professed hacking skills** for defensive purposes and are also known as security analysts



Gray Hats

Individuals who work both **offensively** and **defensively** at various times



Suicide Hackers

Individuals who aim to bring down the critical infrastructure for a "cause" and are **not worried about facing jail terms** or any other kind of punishment



Script Kiddies

An unskilled hacker who compromises a system by **running scripts, tools**, and software that were developed by real hackers

Hacker Classes/Threat Actors (Cont'd)

Cyber Terrorists



Individuals with a wide range of skills who are motivated by **religious or political beliefs** to create the fear through the large-scale disruption of computer networks

State-Sponsored Hackers



Individuals **employed by the government** to penetrate and gain top-secret information from, and damage the information systems of other governments

Hacktivist



Individuals who **promote a political agenda** by hacking, especially by using hacking to deface or disable website

Hacker Teams



A **consortium of skilled hackers** having their own resources and funding. They work together in synergy for researching the state-of-the-art technologies

Industrial Spies



Individuals who perform **corporate espionage** by illegally spying on competitor organizations and focus on stealing information such as blueprints and formulas

Hacker Classes/Threat Actors (Cont'd)



Insider

Any employee (trusted person) who has access to critical assets of an organization. They use **privileged access to violate rules** or intentionally cause harm to the organization's information system.



Criminal Syndicates

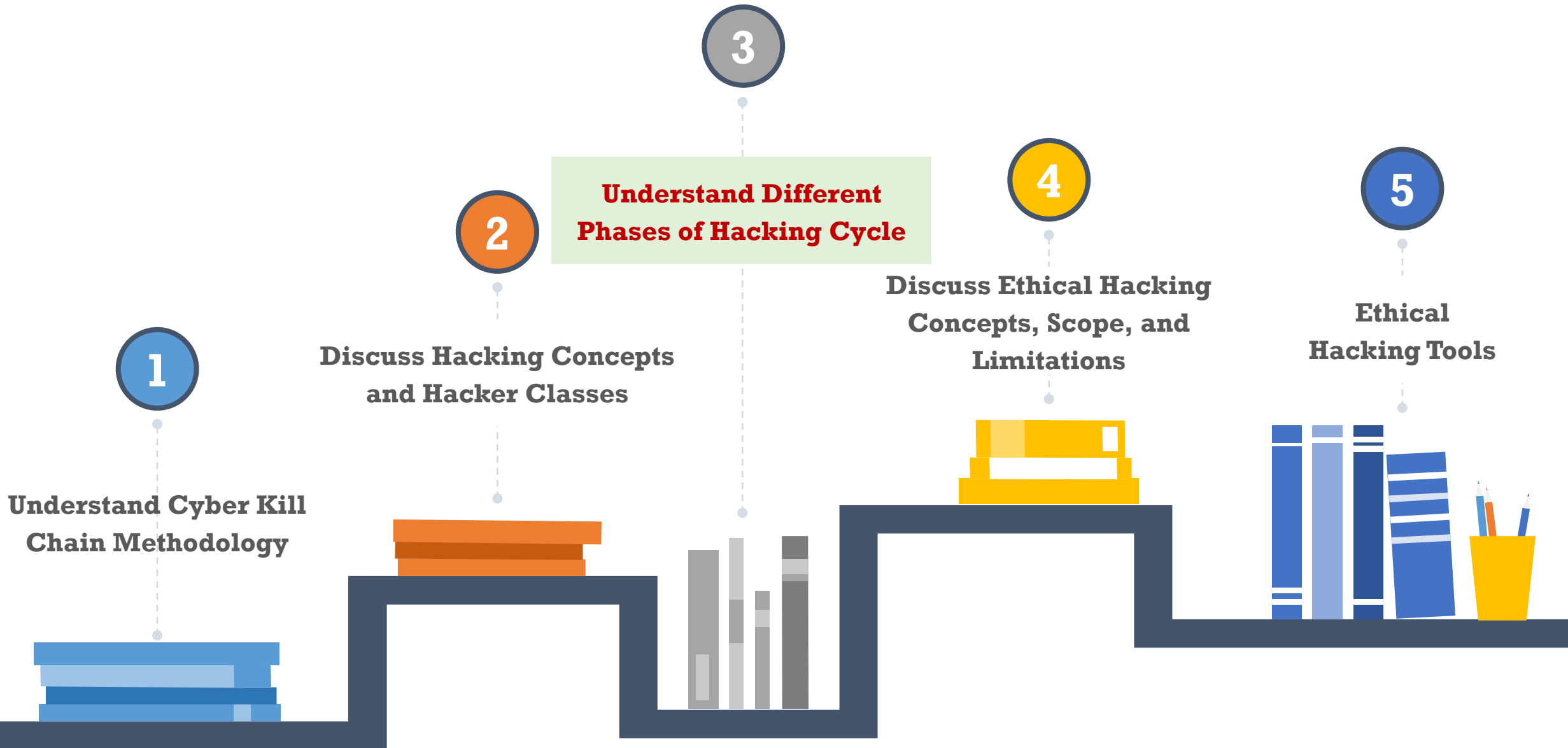
Groups of individuals that are involved in organized, planned, and **prolonged criminal activities**. They illegally embezzle money by performing sophisticated cyber-attacks.



Organized Hackers

Miscreants or **hardened criminals** who use rented devices or botnets to perform various cyber-attacks to pilfer money from victims.

Module Flow



Hacking Phase: Reconnaissance

- ❑ Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack.

Reconnaissance Types



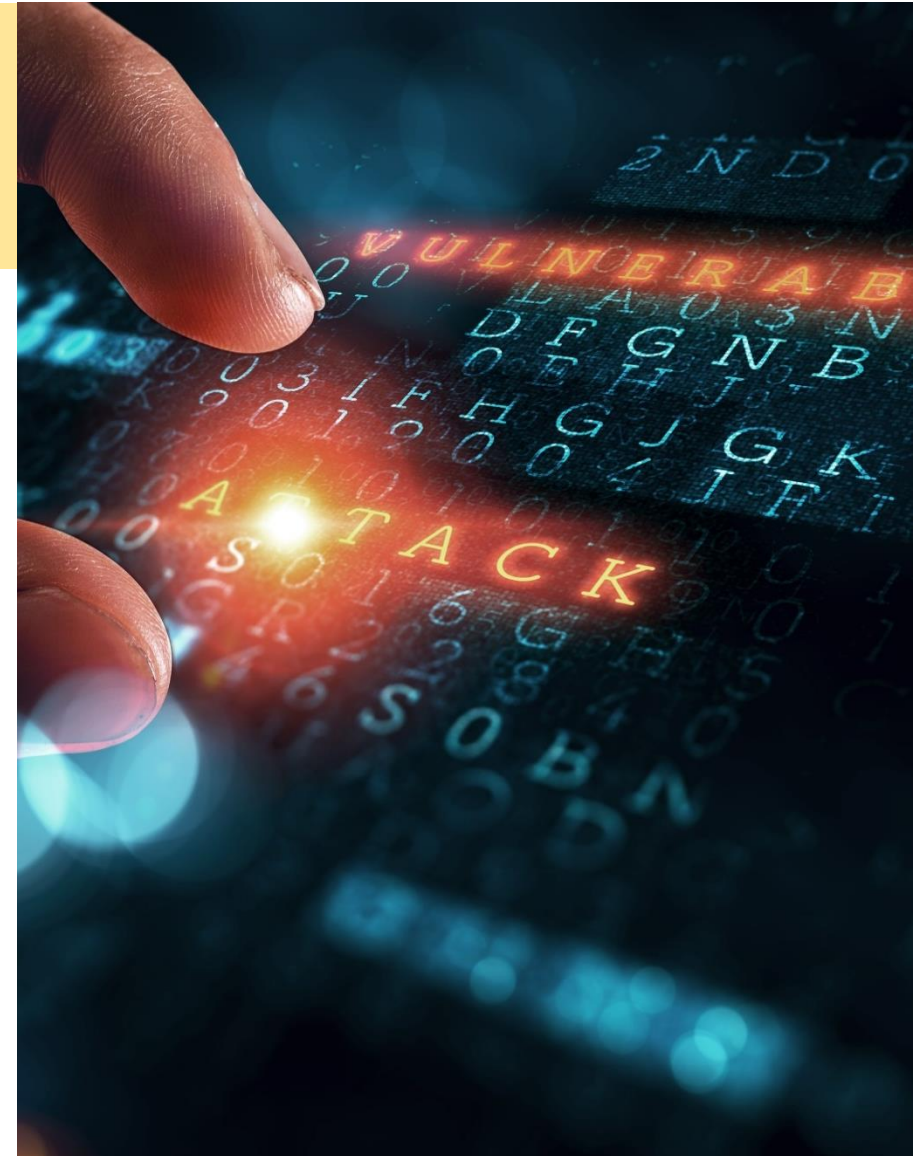
Passive Reconnaissance

- Involves acquiring information **without directly interacting with the target.**
- For example, searching public records or news releases.



Active Reconnaissance

- Involves **directly interacting with the target by any means.**
- For example, telephone calls to the target's help desk or technical department.



Hacking Phase: Scanning



Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information based on information gathered during reconnaissance.

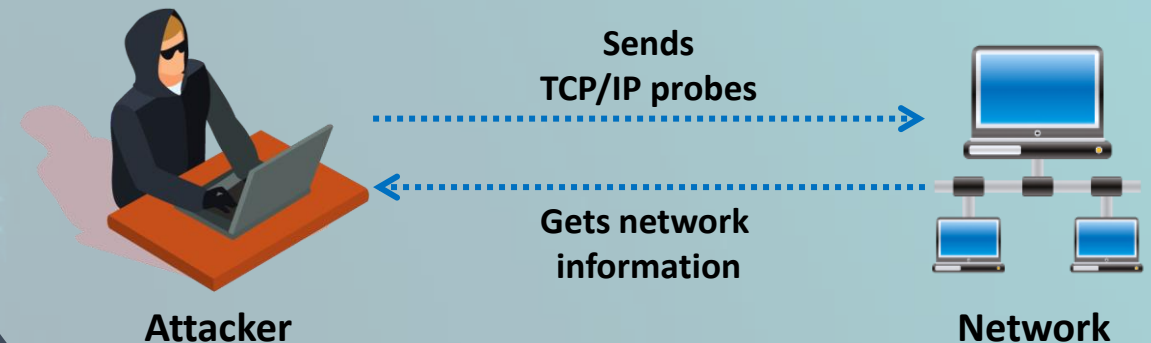


Scanning can include the use of dialers, **port scanners**, network mappers, ping tools, and vulnerability scanners.



Attackers extract information such as **live machines**, port, port status, OS details, device type, and **system uptime** to launch attack.

Network Scanning Process



Hacking Phase: Gaining Access

01

Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the target computer or network

02

The attacker can gain access at the **operating system, application, or network levels**



03

The attacker can **escalate privileges** to obtain complete control of the system

04

Examples include **password cracking**, buffer overflows, denial of service, and **session hijacking**

Hacking Phase: Maintaining Access



Maintaining access refers to the phase when the attacker tries to retain their **ownership of the system**



Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **backdoors**, **rootkits**, or **Trojans**



Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**



Attackers use the compromised system to **launch further attacks**

1

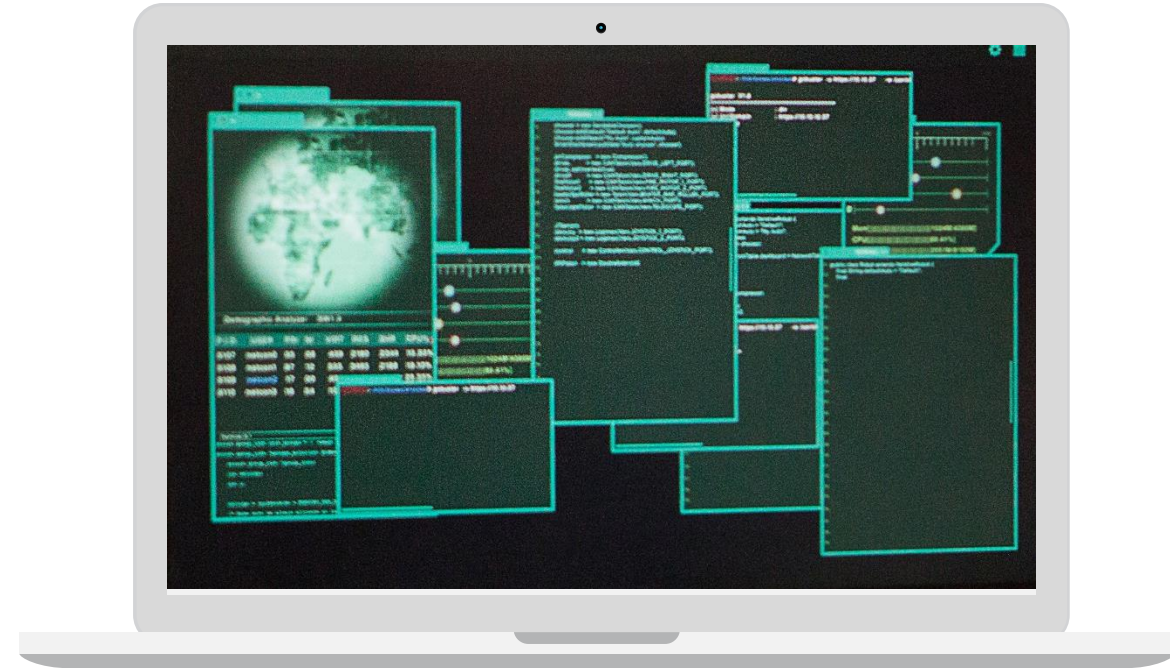
2

3

4

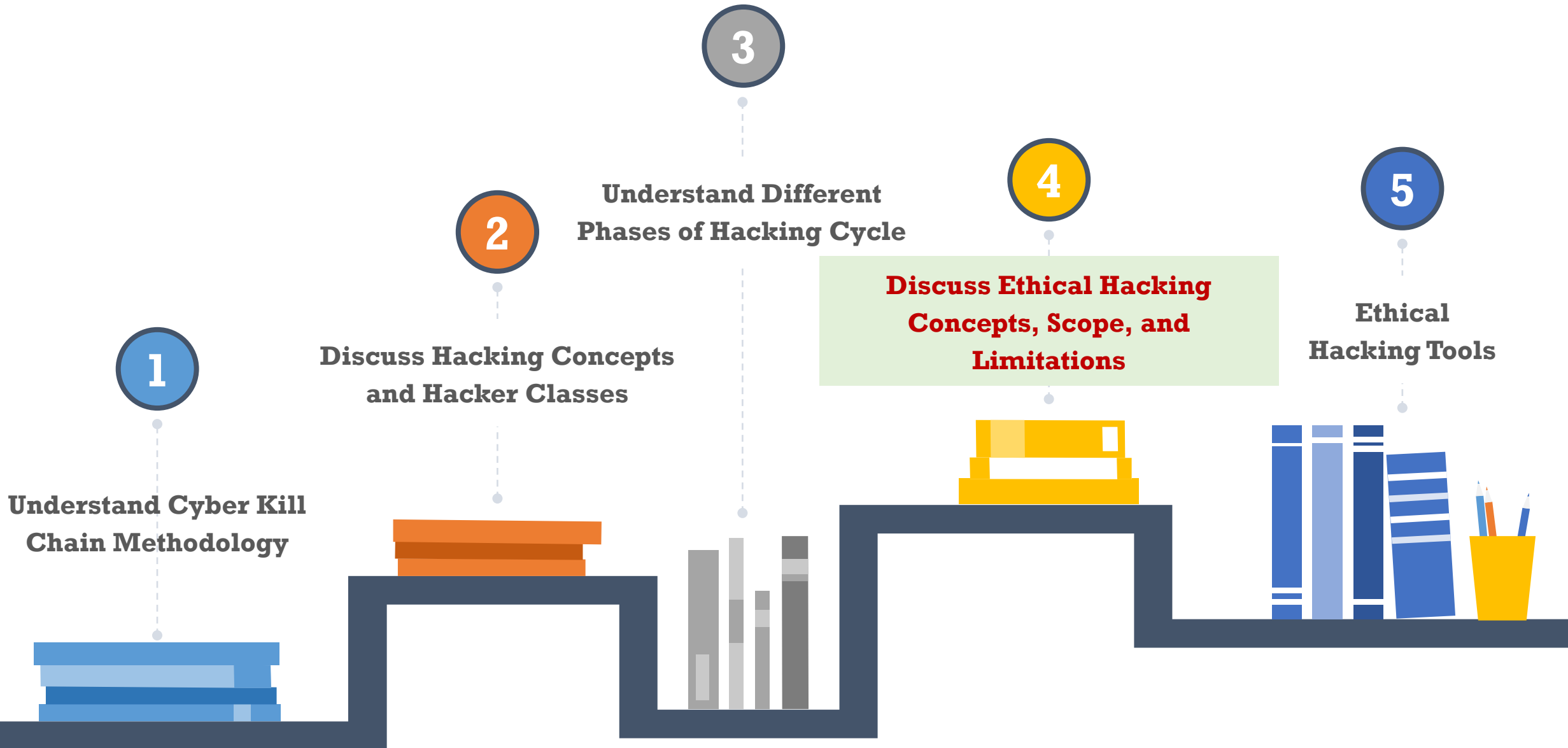
Hacking Phase: Clearing Tracks

- 01** Clearing tracks refers to the activities carried out by an attacker to **hide malicious acts**
- 02** The attacker's intentions include obtaining **continuing access** to the victim's system, remaining **unnoticed and uncaught**, and deleting evidence that might lead to their prosecution
- 03** The attacker overwrites the server, system, and application logs to **avoid suspicion**

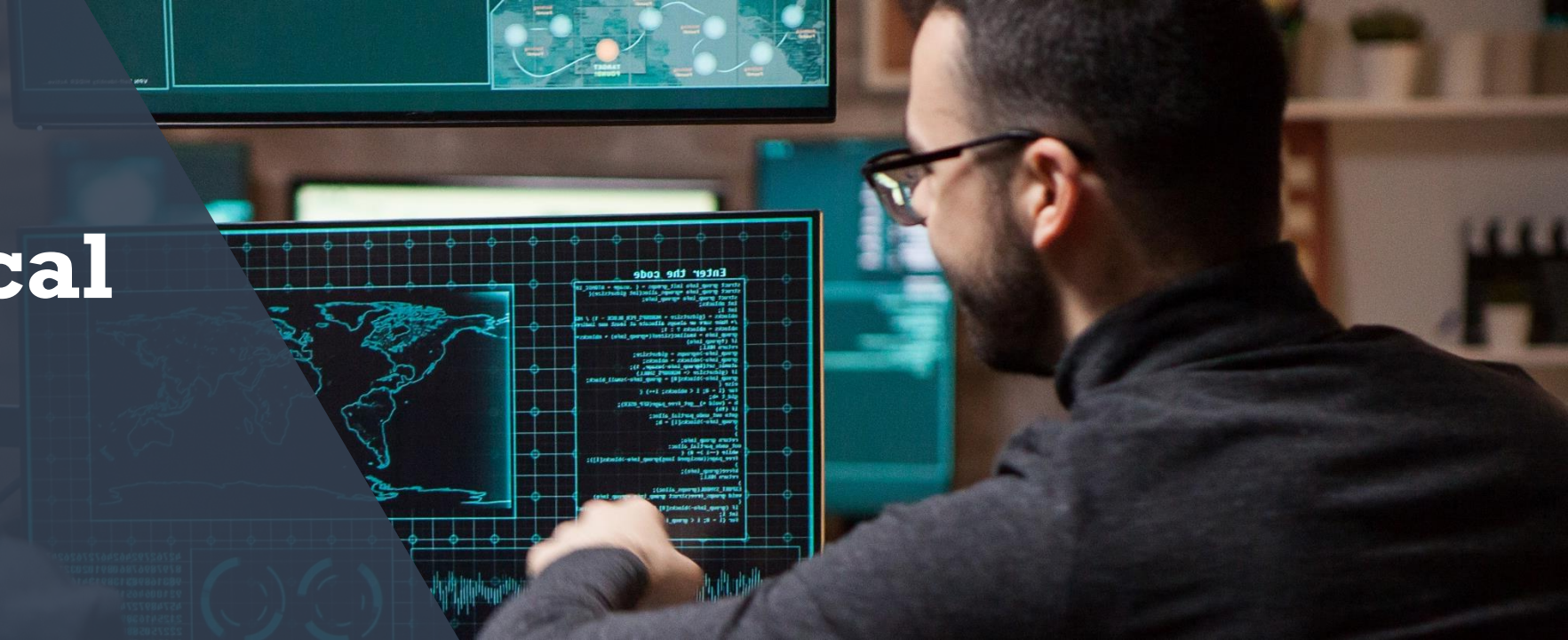


Attackers always cover their tracks to hide their identity

Module Flow



What is Ethical Hacking?



Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** and ensure system security



It focuses on simulating the techniques used by attackers to **verify the existence of exploitable vulnerabilities** in a system's security



Ethical hackers perform security assessments for an organization **with the permission of concerned authorities**

Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!



Ethical hacking is necessary as it **allows for counter attacks against malicious hackers** through anticipating the methods used to break into the system.

Reasons why organizations recruit ethical hackers



To **prevent hackers** from gaining access to the organization's information systems

To provide adequate preventive measures in order to **avoid security breaches**



To **uncover vulnerabilities** in systems and explore their potential as a security risk

To help **safeguard customer data**



To analyze and **strengthen an organization's security posture**

To **enhance security awareness** at all levels in a business



Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1

What can an intruder see on the **target system**?
(Reconnaissance and Scanning phases)

2

What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)

3

Does anyone at the target organization **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)

4

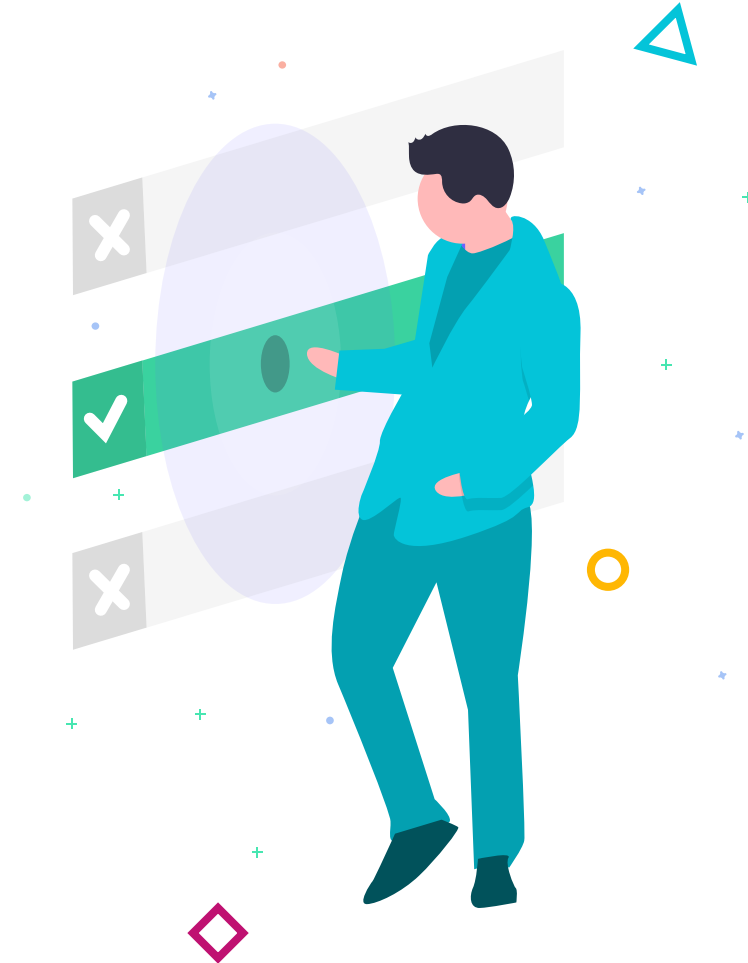
Are all **components of the information system** adequately protected, updated, and patched?

5

How much time, effort, and money are required to obtain **adequate protection**?

6

Are the **information security measures** in compliance with legal and industry standards?



Scope and Limitations of Ethical Hacking

Health Care
Doctor
Hospital
Pharmacist
Nurse
Dentist
First Aid
Surgeon
Emergency

MEDICAL



Scope

- ❑ Ethical hacking is a crucial component of **risk assessment**, **auditing**, **counter fraud**, and information systems security **best practices**
- ❑ It is used to **identify risks** and highlight **remedial actions**. It also reduces ICT costs by resolving vulnerabilities

Limitations

- ❑ Unless the businesses already know what they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience
- ❑ An ethical hacker can only help the organization to better **understand its security system**; it is up to the organization to **place the right safeguards** on the network



Skills of an Ethical Hacker



Technical Skills

- In-depth **knowledge of major operating environments** such as Windows, Unix, Linux, and Macintosh
- In-depth **knowledge of networking** concepts, technologies, and related hardware and software
- A **computer expert** adept at technical domains
- **Knowledgeable about security areas** and related issues
- **“High technical” knowledge** for launching sophisticated attacks

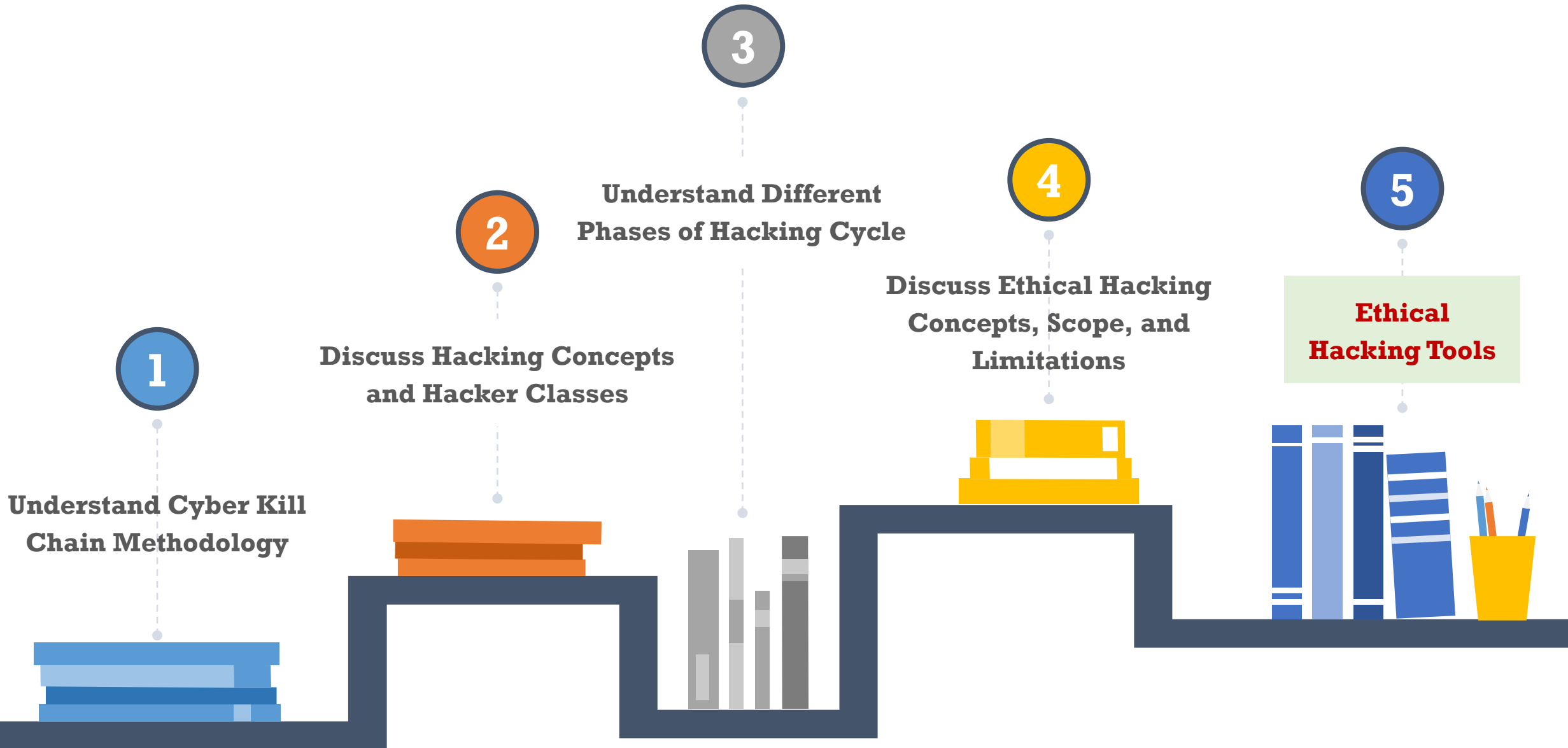


Non-Technical Skills

- The **ability to learn** and adopt new technologies quickly
- **Strong work ethics** and good problem solving and communication skills
- Committed to the **organization’s security policies**
- An awareness of **local standards and laws**



Module Flow



Reconnaissance Using Advanced Google Hacking Techniques



Google hacking refers to the use of advanced Google search operators for **creating complex search queries** to extract sensitive or hidden information that helps attackers **find vulnerable targets**

Popular Google advanced search operators

Search operators	Description
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[location:]	Finds information for a specific location



Reconnaissance Tools

Web Data Extractor

It extracts **targeted contact data** (email, phone, and fax) from the website, extracts the URL and meta tags (title, description, keyword) for website promotion, and so on

Web Data Extractor Pro 3.9. Trial Version. You are on day 5 of your 15 day evaluation period.

Process log | ***Results** | Bad URLs (12) | Stored Sessions

MetaTag (26) | Email (17) | Phone (122) | Fax (118) | Link (66) | Domain (1)

Filter

Description	Keywords	Title	Url	Host	Domain	Page size	Page last modified
A brief description of this we...	keywords, or phrases, ...	Certified Hacker	http://www.certifiedhacker.com/	certifiedhacker.com	com	9660	2011-02-10
Professional Real Estate Ser...	real estate, real estate...	Professional Real Es...	http://certifiedhacker.com/corporate-team...	certifiedhacker.com	com	5845	2011-02-10
		Clear Construction	http://certifiedhacker.com/Real%20Estate...	certifiedhacker.com	com	5381	2011-02-10
		Under the Trees	http://certifiedhacker.com/Under%20Cons...	certifiedhacker.com	com	5151	2017-12-27
A short description of your c...	Some keywords that b...	Your company - Ho...	http://certifiedhacker.com/Under%20the%...	certifiedhacker.com	com	3653	2017-12-27
Turbo max powerfull one pa...	Turbo max , owltempla...	Turbo Max Theme - ...	http://certifiedhacker.com/Recipes/index...	certifiedhacker.com	com	5899	2011-02-10
		P-Folio	http://certifiedhacker.com/Turbo%20Max/...	certifiedhacker.com	com	12125	2017-12-27
A brief description of this we...	keywords, or phrases, ...	Unite - Together is B...	http://certifiedhacker.com/Pfolio/index.html	certifiedhacker.com	com	11606	2017-12-27
Online Booking	booking, hotel, hotels,...	Online Booking	http://certifiedhacker.com/Social%20Medi...	certifiedhacker.com	com	15094	2017-12-27
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	20280	2017-12-27
A short description of your c...	Some keywords that b...	Your company - Abo...	http://certifiedhacker.com/Recipes/Chick...	certifiedhacker.com	com	9594	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Con...	http://certifiedhacker.com/Recipes/about...	certifiedhacker.com	com	5762	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/recipe...	certifiedhacker.com	com	12716	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Menu	http://certifiedhacker.com/Recipes/menu...	certifiedhacker.com	com	7909	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Con...	http://certifiedhacker.com/Recipes/conta...	certifiedhacker.com	com	5828	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Site...	http://certifiedhacker.com/Recipes/recipe...	certifiedhacker.com	com	11965	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Bro...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	16031	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Con...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	14163	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: FAQ	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	14047	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Typ...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	12661	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Sea...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	27877	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/recipe...	certifiedhacker.com	com	12451	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Me...	http://certifiedhacker.com/Recipes/menu...	certifiedhacker.com	com	11584	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Prin...	http://certifiedhacker.com/Recipes/menu...	certifiedhacker.com	com	5693	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Hot...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	39498	2011-02-10
Online Booking	booking, hotel, hotels,...	Online Booking: Che...	http://certifiedhacker.com/Online%20Boo...	certifiedhacker.com	com	12968	2011-02-10

Processing time: 00:00:08.623 | Sites processed: 79 / 79 | Downloaded: 865 KB | Avg. Speed: 128 KB/s

<http://www.webextractor.com>

Whois Record for CertifiedHacker.com

Domain Profile

Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	NETWORK SOLUTIONS, LLC. Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com (p) 18003337680
Registrar Status	clientTransferProhibited, clientTransferProhibited
Dates	6,160 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2018-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,477,906 domains) NS1.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains)
Tech Contact	PERFECT PRIVACY, LLC 12808 Gran Bay Parkway West, Jacksonville, FL, 32258, us wf6j599s4d9@networksolutionsprivateregistration.com (p) 15707088780
IP Address	162.241.216.11 - 1,025 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 13 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 16 years

<https://whois.domaintools.com>

Reconnaissance Tools (Cont'd)

IMCP Traceroute

```
Select Command Prompt - tracet 216.239.36.10

C:\Users\ADMINI~>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    10.10.10.2
  2   4 ms     8 ms    14 ms    115.249.169.81
  3  13 ms    13 ms    11 ms    115.255.252.226
  4  14 ms    13 ms    13 ms    74.125.51.2
  5  27 ms    25 ms    16 ms    108.170.253.121
  6  47 ms    46 ms    48 ms    72.14.233.129
  7  82 ms    83 ms    83 ms    72.14.239.212
  8  93 ms    93 ms    93 ms    209.85.245.163
  9  91 ms    91 ms    92 ms    72.14.233.35
 10  *         *         *         Request timed out.
 11  *         *         *         Request timed out.
 12  *         *         *         Request timed out.
```



TCP Traceroute

```
Parrot Terminal

[root@parrot]~#tcptraceroute www.google.com
Running:
      traceroute -T -0 info www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  10.10.10.2 (10.10.10.2)  0.312 ms  0.172 ms  0.207 ms
 2  maa05s05-in-f4.1e100.net (172.217.163.164) <syn,ack> 17.775 ms 17.367
    ms 17.491 ms
```

UDP Traceroute

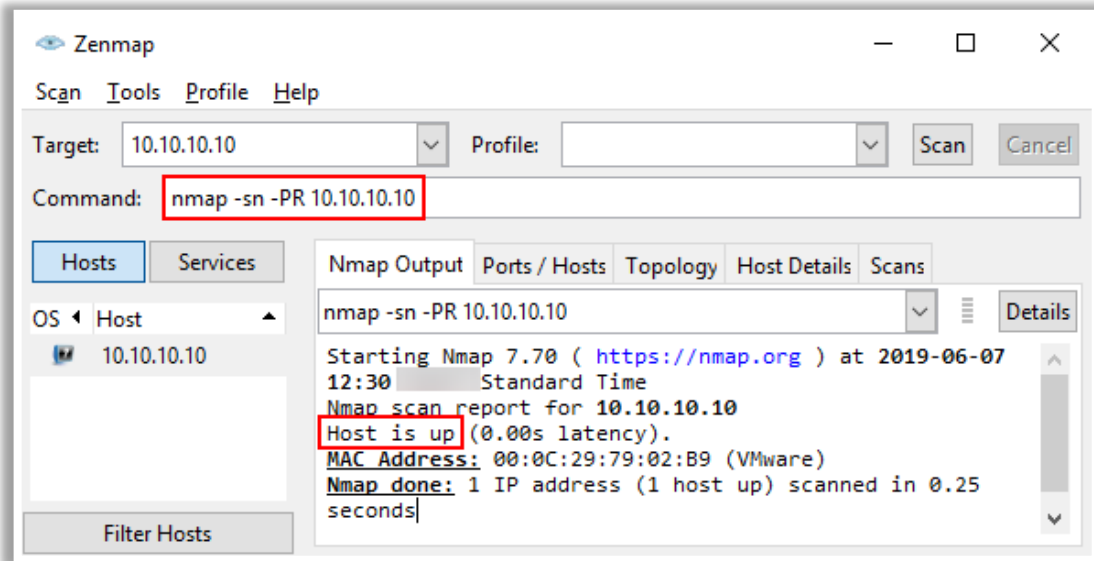
```
Parrot Terminal

[root@parrot]~#traceroute www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  10.10.10.2 (10.10.10.2)  0.260 ms  0.189 ms  0.196 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
```

Scanning Tools

Nmap

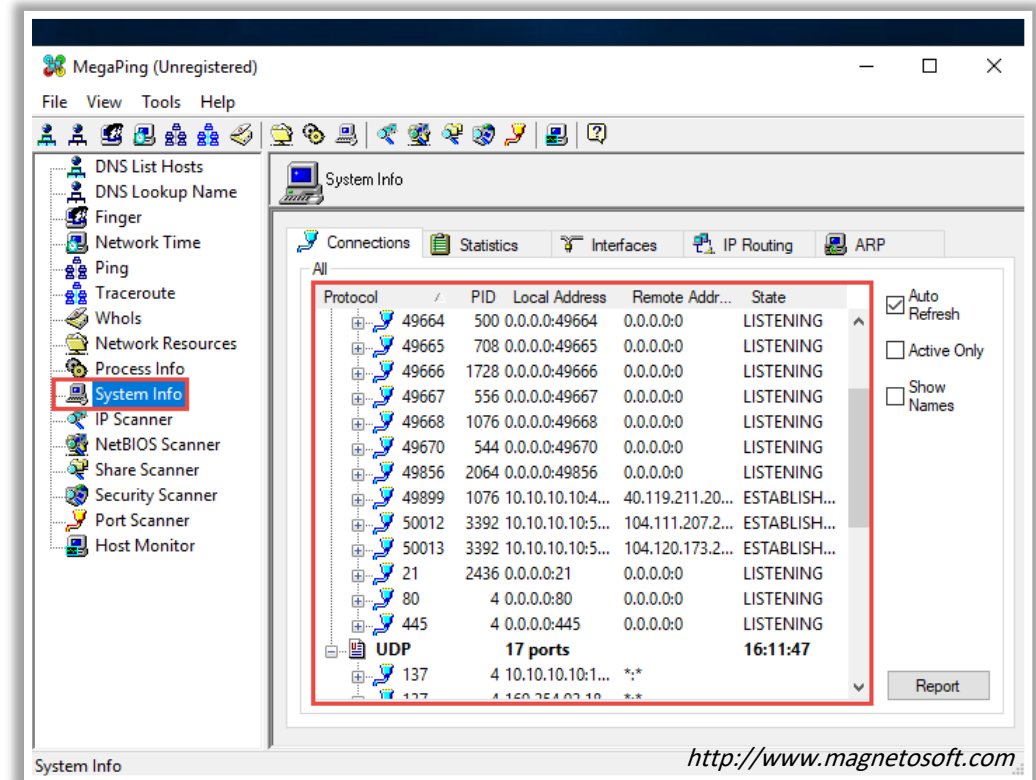
Use Nmap to extract information such as **live hosts** on the network, open ports, services (application name and version), types of packet filters/ firewalls, as well as operating systems and versions used



<https://nmap.org>

MegaPing

Includes scanners such as Comprehensive Security Scanner, **Port scanner** (TCP and UDP ports), IP scanner, NetBIOS scanner, and Share Scanner



<http://www.magnetosoft.com>

Scanning Tools (Cont'd)

Unicornscur

In Unicornscan, the OS of the target machine can be identified by **observing the TTL values** in the acquired scan result

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#unicornscur 10.10.10.16 -Iv
adding 10.10.10.16/32 mode 'TCPscan' ports '7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,
65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-16
4,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,4
43-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,
653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080
,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1
718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,243
0,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,
3542-3545,3632,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,53
08,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838
,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,1
0000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,2001
2,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-3
2780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,6134
8,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer t
han 8 Seconds
TCP open 10.10.10.16:2103 ttl 128
TCP open 10.10.10.16:80 ttl 128
TCP open 10.10.10.16:445 ttl 128
TCP open 10.10.10.16:139 ttl 128
TCP open 10.10.10.16:135 ttl 128
TCP open 10.10.10.16:3389 ttl 128
TCP open 10.10.10.16:88 ttl 128
```

Possible OS is Windows

<https://sourceforge.net>



Hping2/Hping3

<http://www.hping.org>



NetScanTools Pro

<https://www.netscantools.com>



SolarWinds Port Scanner

<https://www.solarwinds.com>



PRTG Network Monitor

<https://www.paessler.com>



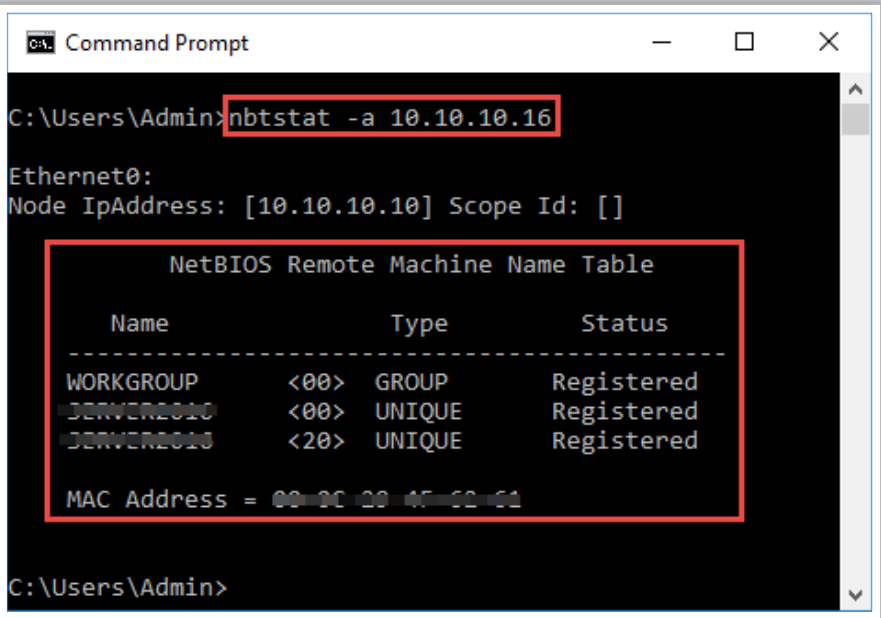
OmniPeek Network Protocol Analyzer

<https://www.liveaction.com>

Enumeration Tools

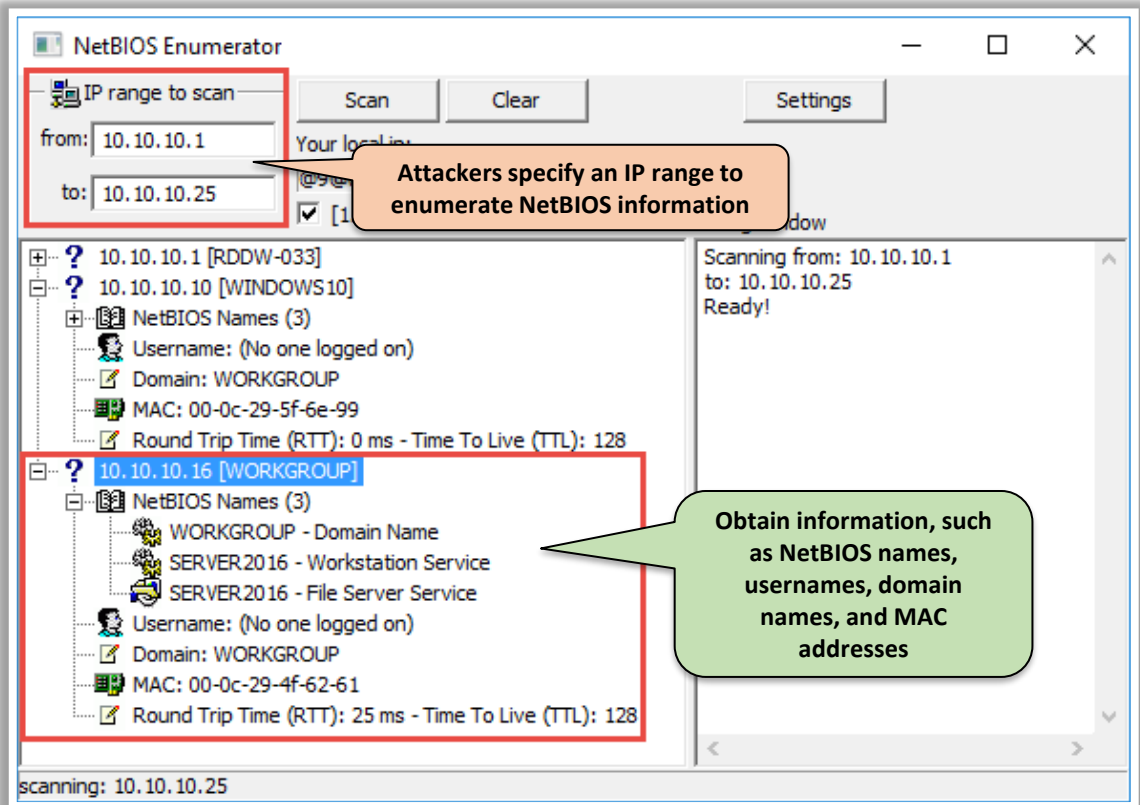
Nbtstat Utility

The nbtstat utility in Windows displays NetBIOS over **TCP/IP** (NetBT) **protocol statistics**, **NetBIOS name tables** for both the local and remote computers, and the **NetBIOS name cache**



NetBIOS Enumerator

NetBIOS Enumerator helps to enumerate details, such as **NetBIOS names**, **Usernames**, **Domain names**, and **MAC addresses**, for a given range of IP addresses



Other NetBIOS Enumeration Tools:

Global Network Inventory
<http://www.magnetosoft.com>

Advanced IP Scanner
<https://www.advanced-ip-scanner.com>

Hyena
<https://www.systemtools.com>

Nsauditor Network Security Auditor
<https://www.nsauditor.com>

<http://nbtenum.sourceforge.net>

Module Summary

1

This module has discussed the cyber kill chain methodology, TTPs, and IoCs in detail

2

It also discussed hacking concepts and hacker classes

3

This module also discussed in detail on different phases of hacking cycle



4

It has discussed ethical hacking concepts such as its scope and limitations and the skills of an ethical hacker

5

Finally, this module ended with an overview of ethical hacking tools

6

In the next module, we will discuss in detail on information security threats, vulnerabilities, and malware concepts