



# RECONNAISSANCE

(Nmap - The Active Eye of The Pentester)

# Table of Content

**Who AM I**

**Reconnaissance (What is it)**

**Types of Reconnaissance**

**Nmap (The Active eye)**

**Nmap Switches**

**Nmap Script Engine (NSE)**

**Practicals**

**Questions**



# Who AM I

- ERIC NII SOWAH BADGER (NiiHack)
- S.O.C. Specialist (Pentest) at GCB Bank Ltd
- Consultant for Invetech Global
- LinkedIn: Eric Nii Sowah Badger
- TWITTER: ens\_nii
- Personal Website: <https://www.niihackgh.com>
- Invetech Global Website: <https://www.invetekglobal.com>



# Reconnaissance – What it is

- Information Gathering and getting to know the target systems is the first process in ethical hacking / the cyber kill chain
- Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system
- Ethical hackers attempt to gather as much information about a target system as possible during the reconnaissance stage.
- Reconnaissance is always the eye of the Ethical Hacker



# Types of Reconnaissance

## PASSIVE

This is the process of gathering information where there is no direct connection to the target.

## PASSIVE

This is a form of targeted information data collection that takes place when an individual's personal data, such as password, is stolen without the targeted individual's knowledge.

## PASSIVE

This can take place when the hacker is sifting through the target's garbage in order to obtain discarded papers.

1

1

2

2

3

3

## ACTIVE

This is the process of directly interacting or engaging with the targeted system to gain information.

## ACTIVE

This type of recon gathers information about the target by probing the targeted system.

## ACTIVE

This type of recon is faster to perform and generally yields more actionable information than passive recon





# Passive Reconnaissance Tools

## WIRESHARK

This is best known as network traffic analysis tool. This tool can be used to eavesdrop on the network traffic of a company

## FINDSUBDOMAINS.COM

This is one example of a variety of different websites designed to help identify website that belong to an organization.

## SHODAN

This is a search engine for internet-connect devices.

1

2

3

4

5

## GOOGLE

Google can provide a vast amount of information on a variety of topic. By using specialized google queries (google dorking), you can gather sensitive information for attacking your target.

(eg. Index of /Hollywood)

## VIRUSTOTAL

This is a website designed to help with analysis of potential malicious files.





# Active Reconnaissance Tools

## NMAP

This is probably the most well-known tool for active network reconnaissance

1

## OPENVAS

This is a vulnerability scanner that was developed in response to the commercialization of Nessus.

3

## METASPLOIT

This is primarily designed as an exploitation toolkit.

5

## NESSUS

This is a commercial vulnerability scanner used to identify vulnerable applications running on a system.

2

## NIKTO

This is a web server vulnerability scanner that can be used for reconnaissance in a manner similar to Nessus and OpenVAS.

4





# NMAP – The Active eye

- When it comes to hacking, knowledge is power. The more knowledge you have about a target system or network, the more options you have available.
- Nmap (Network Mapper) is a free and open source (license) utility for network discovery and security auditing.
- Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest.
- Like most pentesting tools, nmap is run from the terminal. Nmap is probably the most famous reconnaissance tool among Pentesters and Hacker.





# Nmap is ...

**POWERFUL**

**EASY**

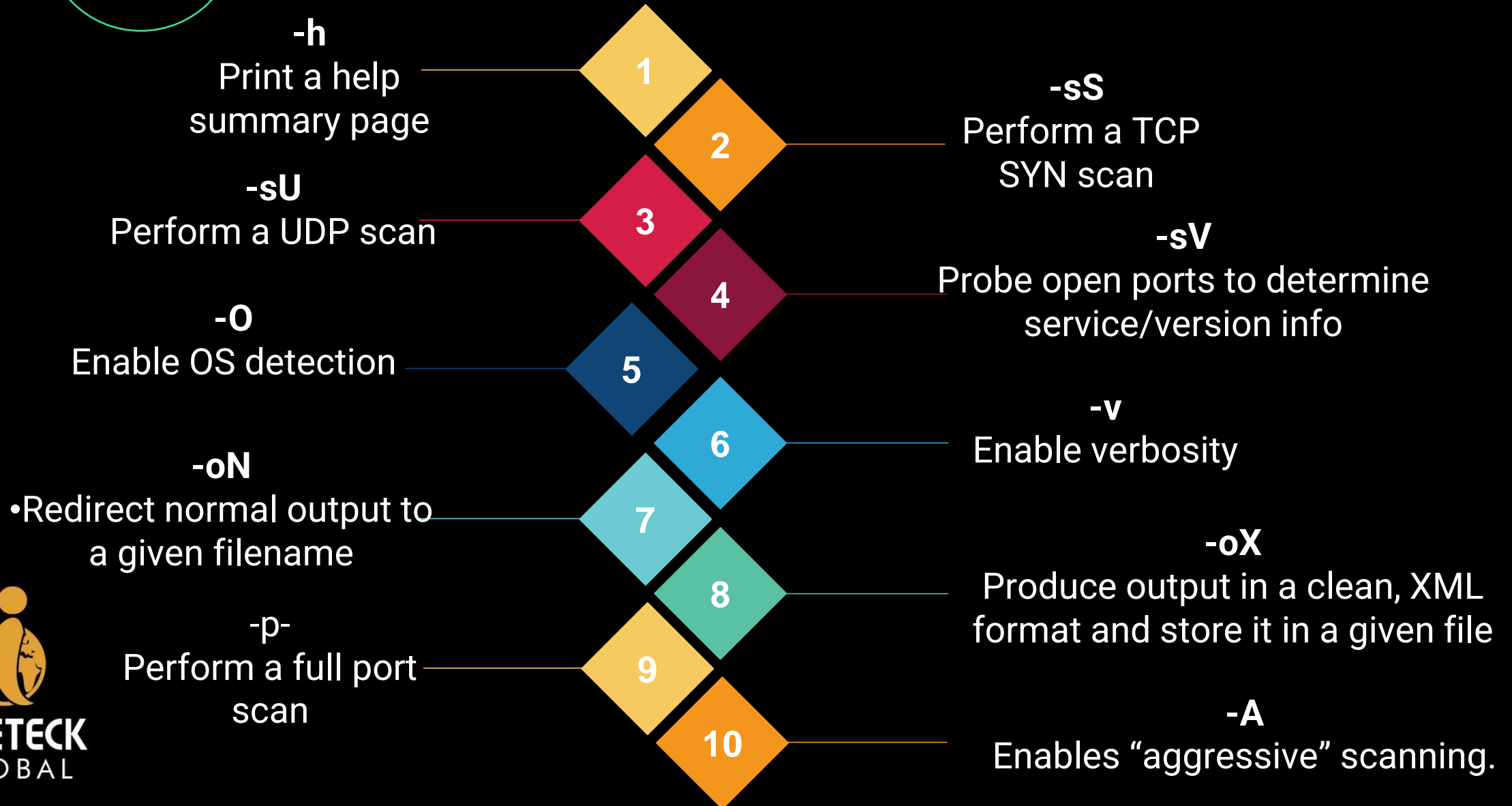
**FLEXIBLE**

**FREE**

**POPULAR**



# Nmap Switches



# Nmap Script Engine (NSE)

## 1. SAFE

Won't affect the target

## 2. INTRUSIVE

Not safe: likely to affect the target

## 6. BRUTE

Try to brute force credentials for running services

## 5. AUTH

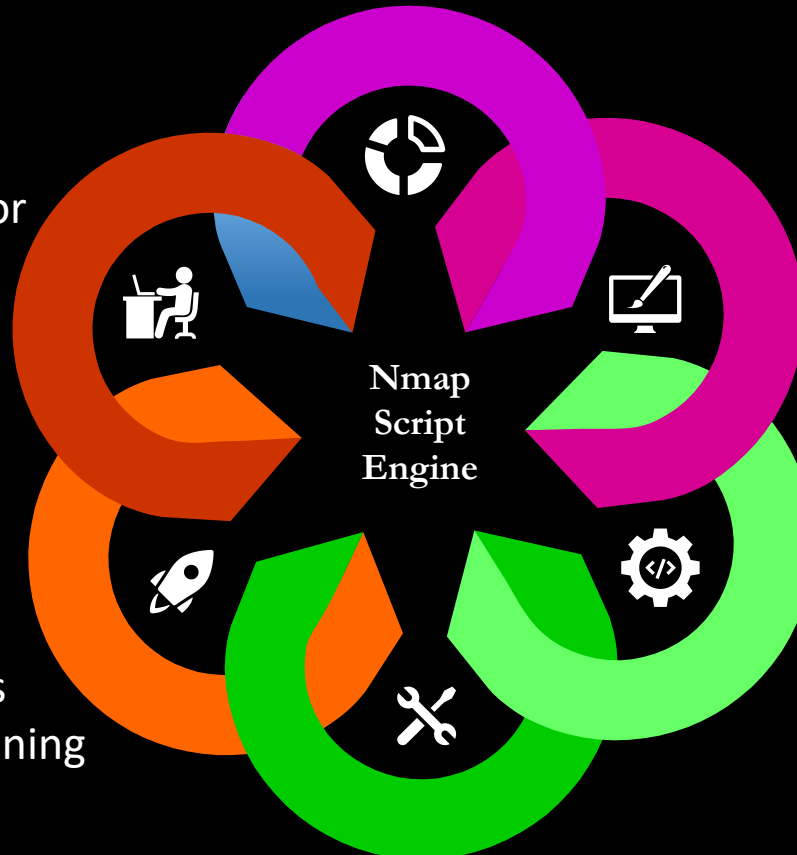
Attempt to bypass authentication for running services

## 4. EXPLOIT

Try to exploit a vulnerability

## 3. VULN

Scan for vulnerabilities



# PRACTICALS

# References

- [Nmap - Switches and Scan Types in Nmap – JournalDev](#)
- [TryHackMe | Nmap](#)
- [Nmap: the Network Mapper - Free Security Scanner](#)
- [Ethical Hacking - Reconnaissance \(tutorialspoint.com\)](#)
- [Reconnaissance in The Cyber Kill Chain - Cyber Security Insights \(stunsnroses.tech\)](#)

# Questions



*Thank You*