Internship Final Report

PORT Guard

(Port Scanning Automation Tool)

Team Members

- Muhmmad Arsalan Javed (22i-1632)
- Sir Zaigham Abdullah Bin Qasim

Protect Lab

Department of Cyber Security
HOD Dr. Muhammad Asim

FAST - National University of Computer and Emerging Sciences

Date: 12/07/2024

Table of Contents

Introduction: 1
Why have we used NMAP only? 1
Comparison with other tools: 1
Key Features: 2
How to set up? 3
Prerequisites 3
Installation 3
Visual Representation of Each Feature: 4
Contributors: 12
Profiles: 12
License: 12

Project Title: PORT Guard (Port Scan-Automation)

Introduction:

Our Port Scanning project is an advanced web-based automation tool for Nmap (Network Mapper), the popular network scanning utility. Designed with a user-friendly interface, this tool allows users to configure and execute Nmap scans effortlessly, even if they have limited technical expertise.

Why have we used NMAP only?

We decided to automate python script for only NMAP tool as among the list of port scanning tools, NMAP stands out as the most featured and widely used tool. Below are some supporting points:

Comparison with other tools:

- **MASSCAN:**
  MASSCAN is a very fast network scanner but is basic compared to Nmap. It doesn't do advanced tasks like figuring out what services are running or what operating systems are in use.
- **OpenVAS:**
  OpenVAS is a powerful security scanner that can find vulnerabilities, but it's more complicated to set up and manage than Nmap, which can be a barrier for some users.
- **Zenmap:**
  Zenmap is just the graphical user interface (GUI) for Nmap. It looks nicer and is easier to use but doesn't offer any additional features beyond what Nmap provides.
- **Unicornscan:**
  Unicornscan is a scanning tool, but it doesn't provide as many options for detecting services or operating systems compared to Nmap.
- **Angry IP Scanner:**
  Angry IP Scanner is simple and easy to use, but it's not as powerful or feature rich as Nmap, making it less suitable for detailed scanning.
- **Netcat:**
  Netcat is a versatile tool for network communication but lacks the specialized scanning capabilities that Nmap offers for network discovery and assessment.
- **Hping:**
  Hping is great for testing firewall settings and performing advanced network tests, but it doesn't cover as many general scanning features as Nmap does.

Summary Table:

Tool	Strengths	Weaknesses
MASSCAN	Fast scanning	No service/OS detection
OpenVAS	Vulnerability scanning	Complex setup
Zenmap	User-friendly GUI	No extra features
Unicornscan	Unique scanning techniques	Limited service/OS detection
Angry IP Scanner	Simple and easy to use	Less powerful than Nmap
Netcat	Versatile network tool	Lacks scanning features
Hping	Firewall testing	Not as comprehensive as Nmap

Key Features:

Following are the features of our tool:

- **IP Range Scanning:**
  Easily input single IP addresses or entire ranges for scanning. (e.g. 192.168.198.129 or 192.168.198.129-200)
- **Scan using Domain Name:**
  User can also scan with domain name. (e.g. nu.edu.pk)
- **Mode Selection:**
  Choose between Normal and Advanced scanning modes.
- **Normal Scan:**
  Only tells open ports and running services.
- **Advanced Scan Options:**
  - Scan Types:
    Select from various scan types such as TCP SYN, UDP, and more.
  - Host Discovery:
    Customize host discovery methods.
  - Port Selection:
    Default or custom port ranges.
  - Service Detection:
    Determine service versions and operating systems.
  - Firewall Evasion:
    Options for evading firewalls and intrusion detection systems.
  - Nmap Scripting:
    Included specific Nmap scripts for enhanced functionality.

- Output Formats:
  Multiple output formats including XML, normal text, and greppable.

How to set up?

Follow these instructions to get a copy of the project up and running on your local machine for development and testing purposes.

Prerequisites

- Python 3.6+
- pip (Python package installer)
- Nmap (required)

Installation

Step 1:
Clone the Repository

```
https://github.com/AhmadHanif12/Port-Scanning-Automation.git
cd Port-Scanning-Automation
```

Step 2:
Open this directory

```
cd Nmap_Automation
```

Step 3:
Installing requirements

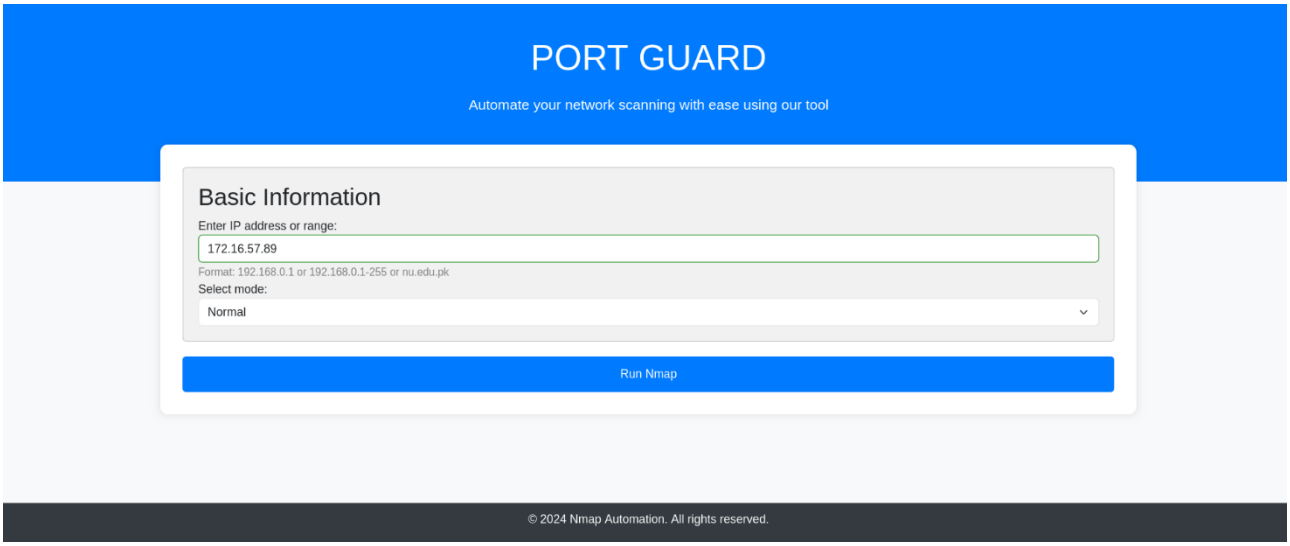
```
pip3 install requirements.txt
```

Step 4:
Run the tool

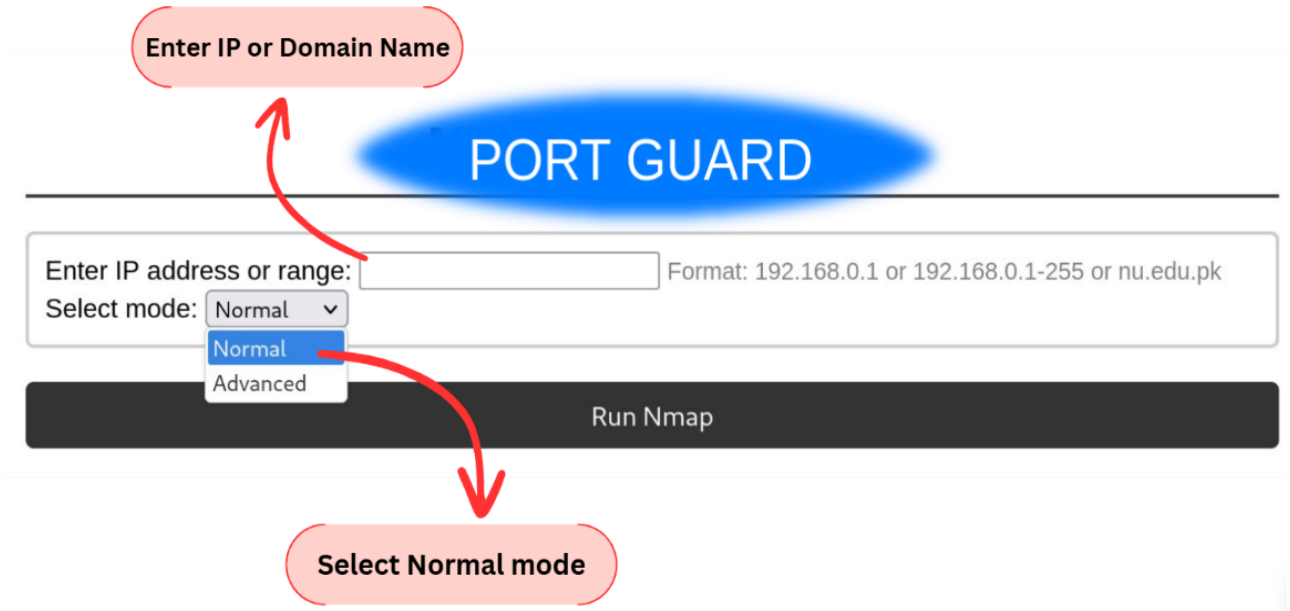
```
sudo python app.py
```

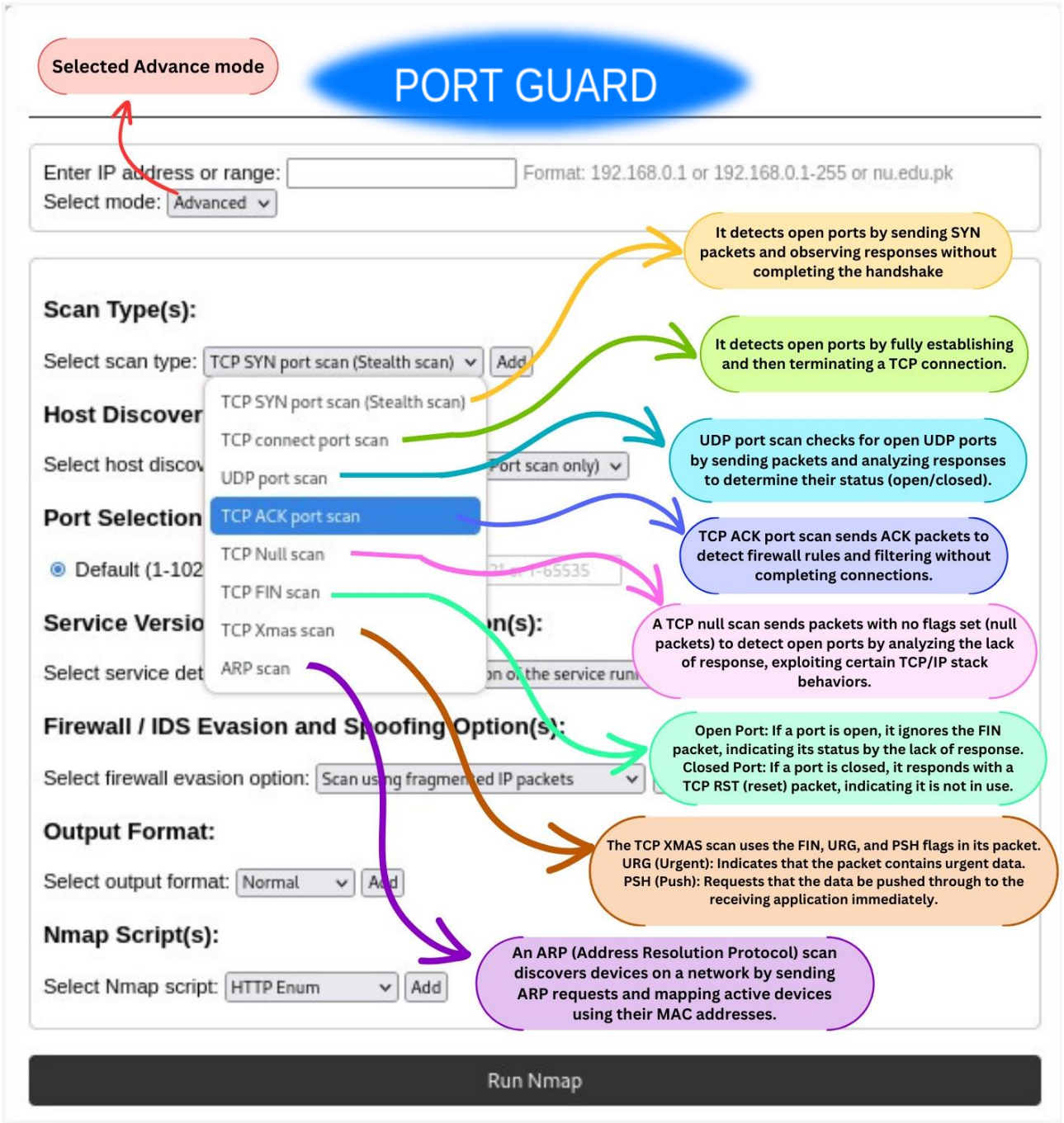
Step 5:
Visit http://127.0.0.1:8080/ in your browser.

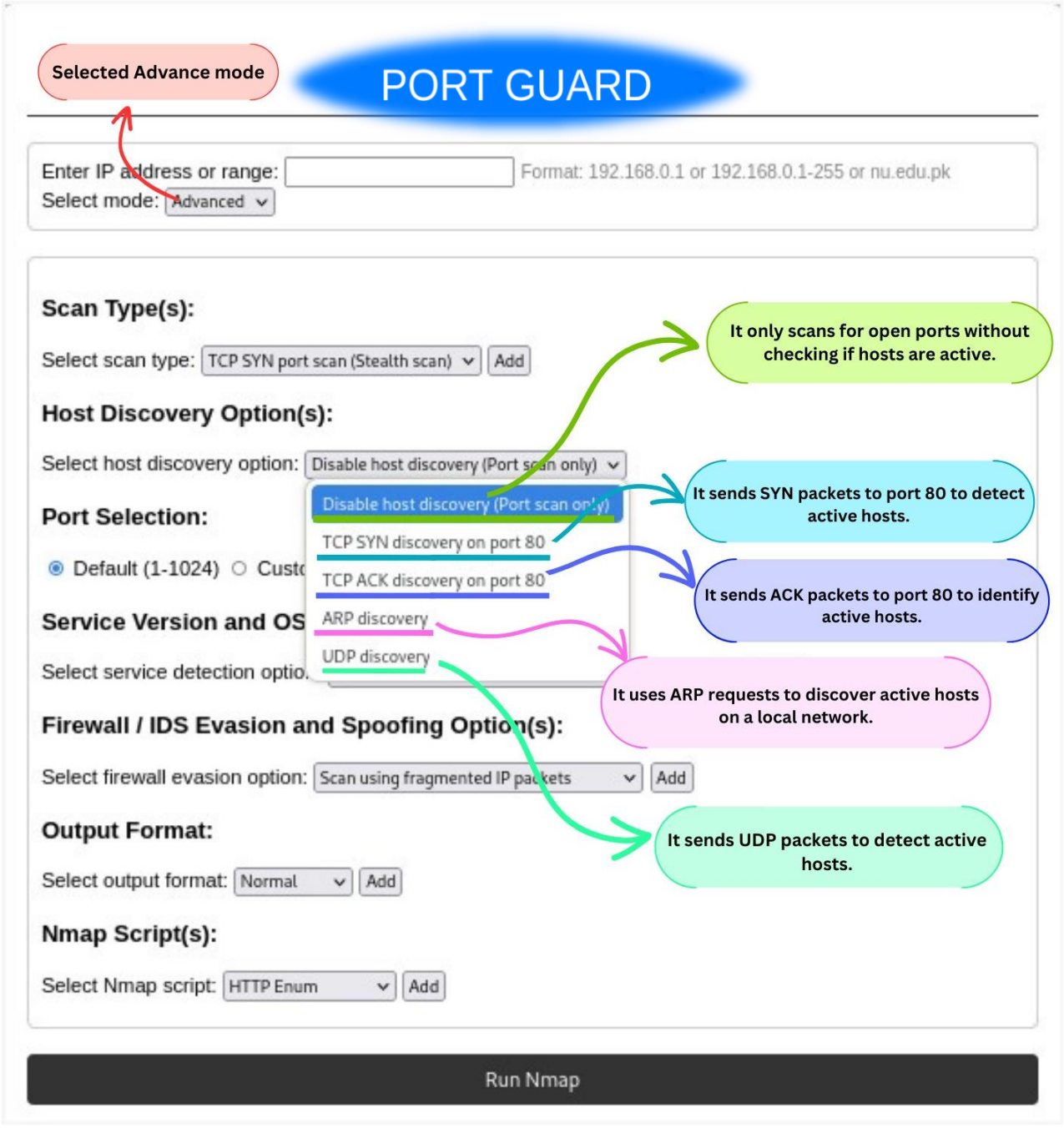
Now, the tool is ready for use in your browser.

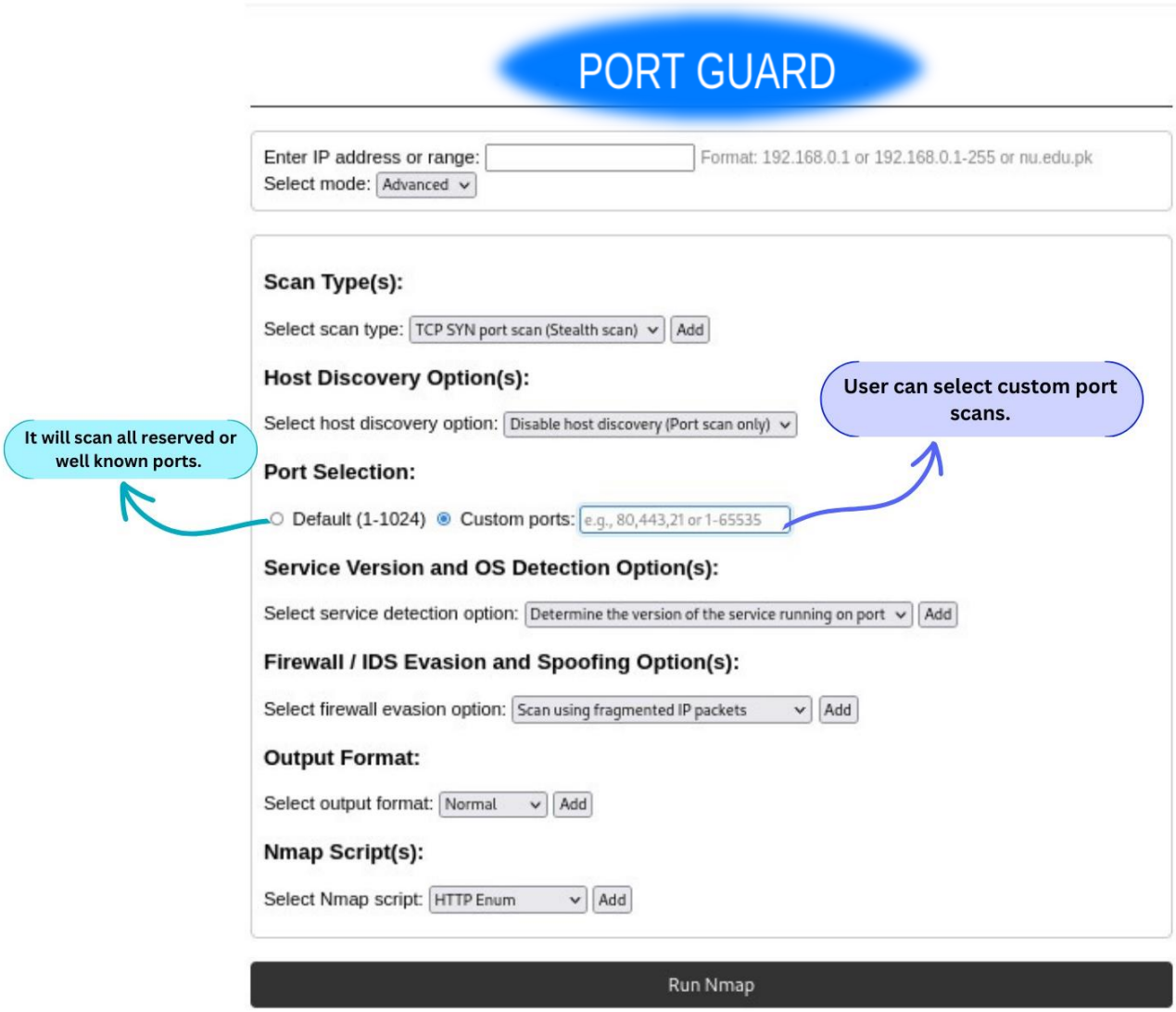


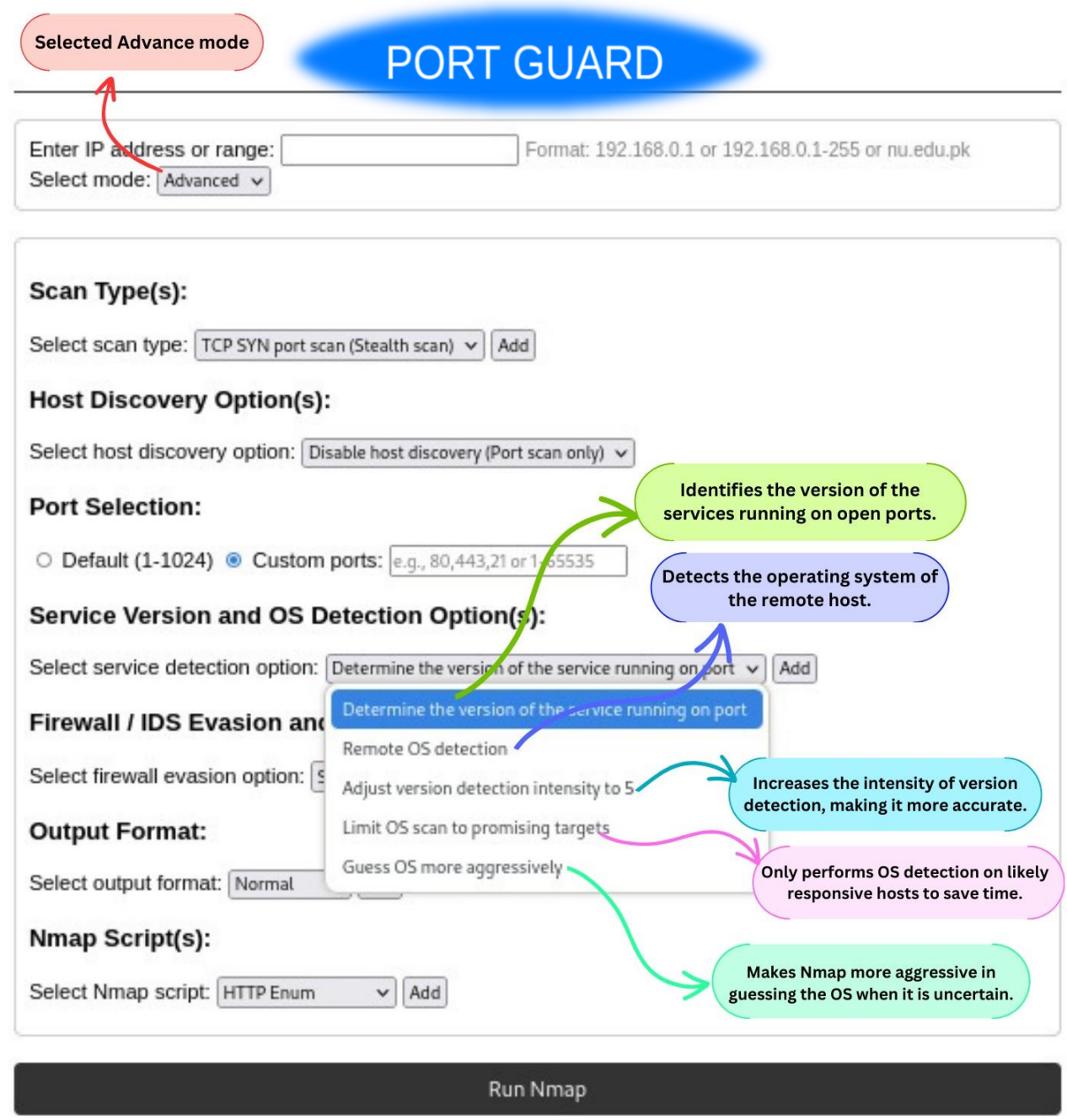
Visual Representation of Each Feature:

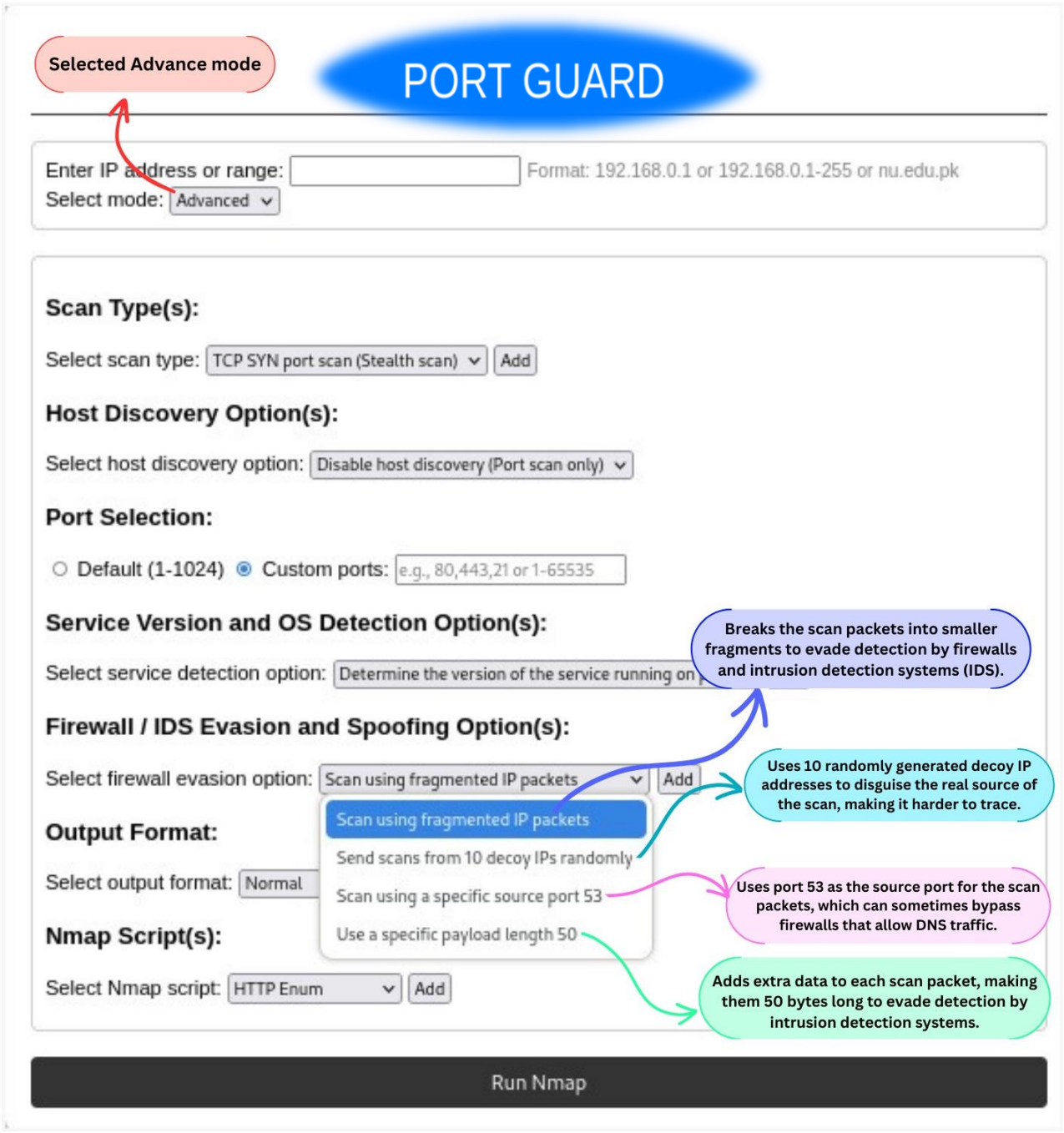


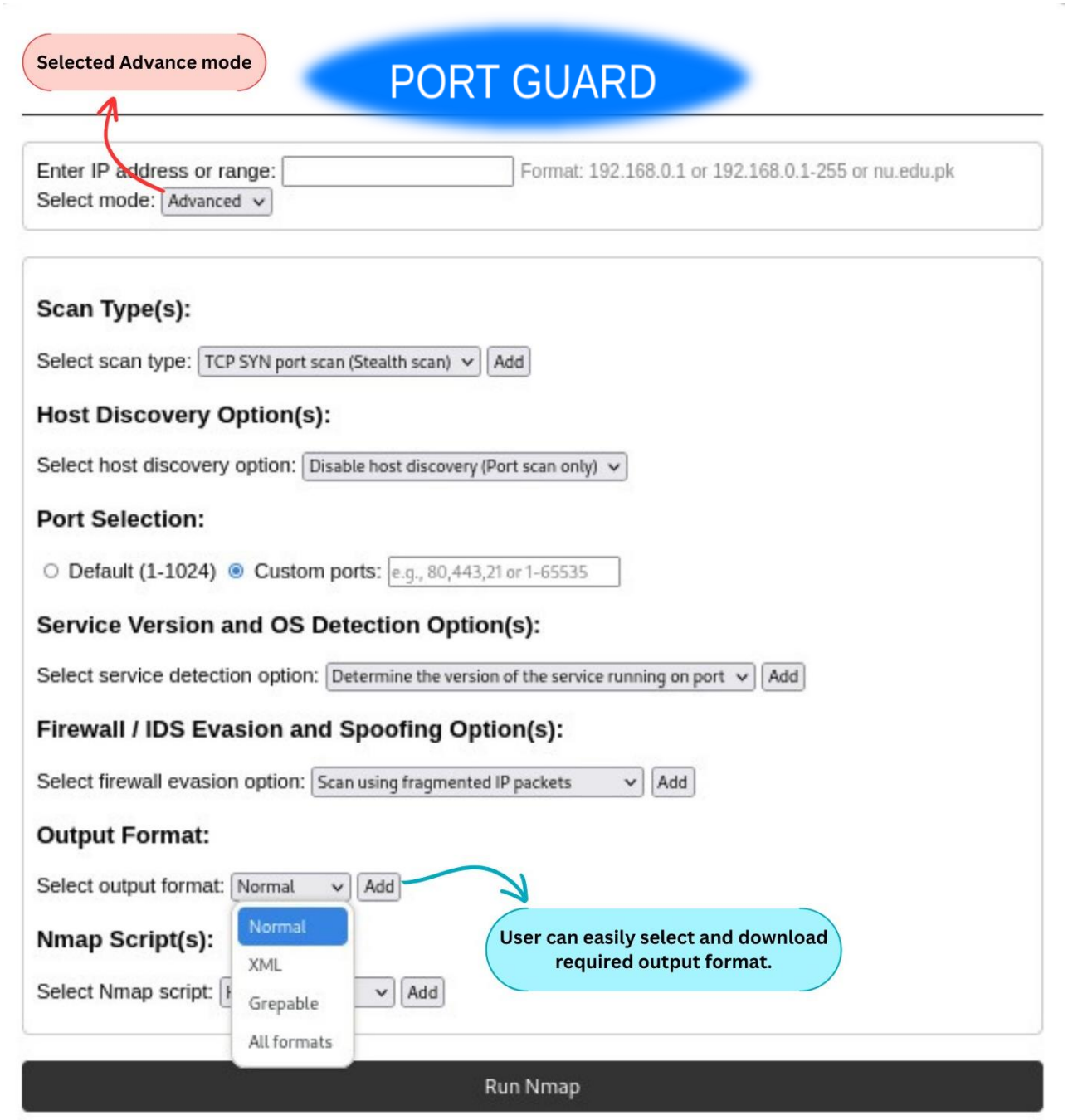

Selected Advance mode
PORT GUARD
Enter IP address or range:
Format: 192.168.0.1 or 192.168.0.1-255 or nu.edu.pk
Select mode: Advanced
Scan Type(s):
Select scan type: TCP SYN port scan (Stealth scan) Add
TCP SYN port scan (Stealth scan)
TCP connect port scan
UDP port scan
TCP ACK port scan
TCP Null scan
TCP FIN scan
TCP Xmas scan
ARP scan
Host Discover
Select host discov
Port scan only)
Port Selection
Default (1-102
1-65535
Service Versio
n(s):
Select service det
on of the service runi
Firewall / IDS Evasion and Spoofing Option(s):
Select firewall evasion option: Scan using fragmented IP packets
Output Format:
Select output format: Normal Add
Nmap Script(s):
Select Nmap script: HTTP Enum Add
Run Nmap
It detects open ports by sending SYN packets and observing responses without completing the handshake
It detects open ports by fully establishing and then terminating a TCP connection.
UDP port scan checks for open UDP ports by sending packets and analyzing responses to determine their status (open/closed).
TCP ACK port scan sends ACK packets to detect firewall rules and filtering without completing connections.
A TCP null scan sends packets with no flags set (null packets) to detect open ports by analyzing the lack of response, exploiting certain TCP/IP stack behaviors.
Open Port: If a port is open, it ignores the FIN packet, indicating its status by the lack of response.
Closed Port: If a port is closed, it responds with a TCP RST (reset) packet, indicating it is not in use.
The TCP XMAS scan uses the FIN, URG, and PSH flags in its packet.
URG (Urgent): Indicates that the packet contains urgent data.
PSH (Push): Requests that the data be pushed through to the receiving application immediately.
An ARP (Address Resolution Protocol) scan discovers devices on a network by sending ARP requests and mapping active devices using their MAC addresses.

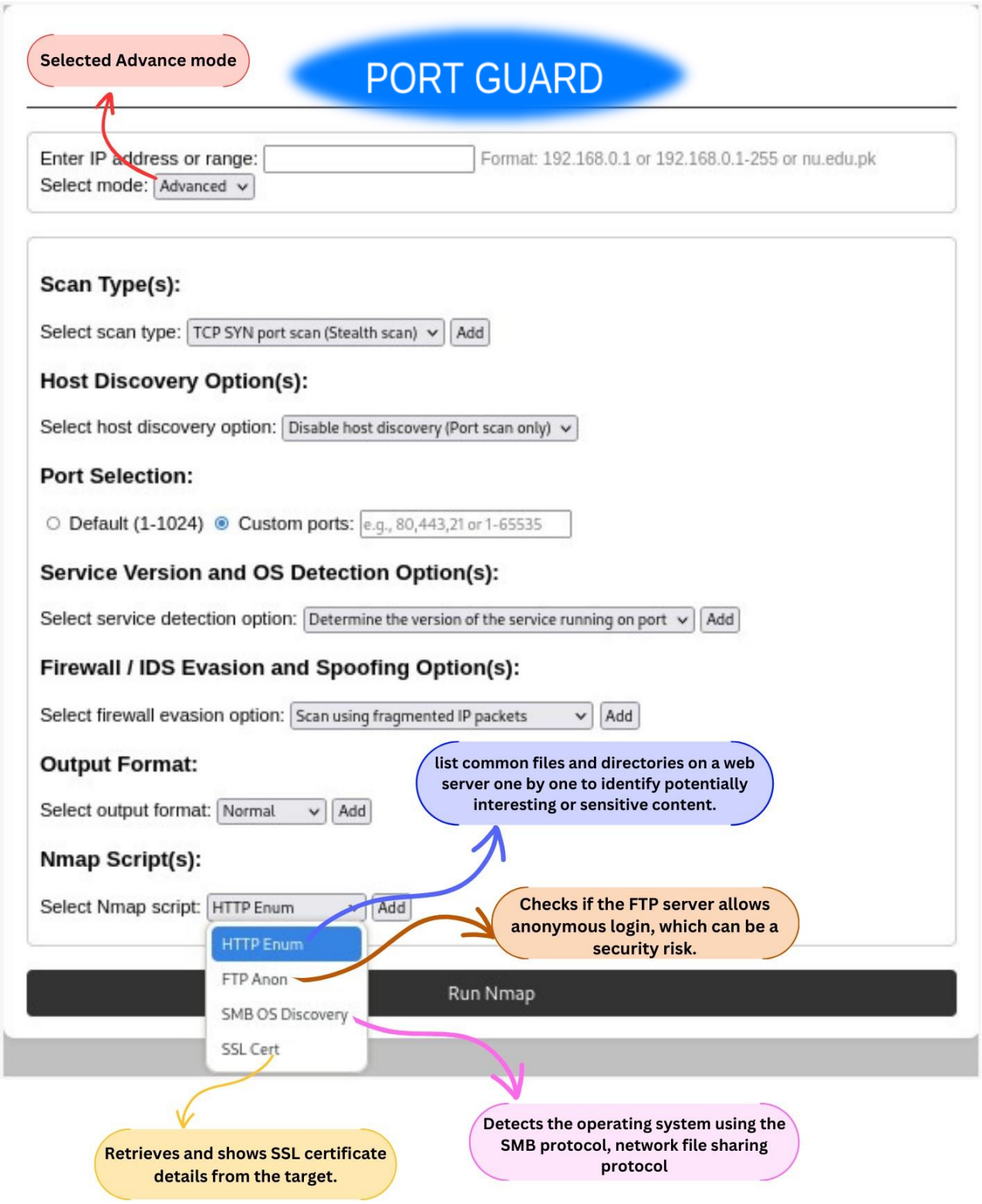

Selected Advance mode
PORT GUARD
Enter IP address or range:
Format: 192.168.0.1 or 192.168.0.1-255 or nu.edu.pk
Select mode: Advanced
Scan Type(s):
Select scan type: TCP SYN port scan (Stealth scan) Add
Host Discovery Option(s):
Select host discovery option: Disable host discovery (Port scan only)
Disable host discovery (Port scan only)
TCP SYN discovery on port 80
TCP ACK discovery on port 80
ARP discovery
UDP discovery
Port Selection:
Default (1-1024)
Service Version and OS
Select service detection optio
Firewall / IDS Evasion and Spoofing Option(s):
Select firewall evasion option: Scan using fragmented IP packets Add
Output Format:
Select output format: Normal Add
Nmap Script(s):
Select Nmap script: HTTP Enum Add
Run Nmap
It only scans for open ports without checking if hosts are active.
It sends SYN packets to port 80 to detect active hosts.
It sends ACK packets to port 80 to identify active hosts.
It uses ARP requests to discover active hosts on a local network.
It sends UDP packets to detect active hosts.


PORT GUARD
Enter IP address or range:
Format: 192.168.0.1 or 192.168.0.1-255 or nu.edu.pk
Select mode: Advanced
Scan Type(s):
Select scan type: TCP SYN port scan (Stealth scan) Add
Host Discovery Option(s):
Select host discovery option: Disable host discovery (Port scan only)
Port Selection:
Default (1-1024) Custom ports: e.g., 80,443,21 or 1-65535
Service Version and OS Detection Option(s):
Select service detection option: Determine the version of the service running on port Add
Firewall / IDS Evasion and Spoofing Option(s):
Select firewall evasion option: Scan using fragmented IP packets Add
Output Format:
Select output format: Normal Add
Nmap Script(s):
Select Nmap script: HTTP Enum Add
Run Nmap
It will scan all reserved or well known ports.
User can select custom port scans.


Selected Advance mode
PORT GUARD
Enter IP address or range:
Format: 192.168.0.1 or 192.168.0.1-255 or nu.edu.pk
Select mode: Advanced
Scan Type(s):
Select scan type: TCP SYN port scan (Stealth scan) Add
Host Discovery Option(s):
Select host discovery option: Disable host discovery (Port scan only)
Port Selection:
Default (1-1024) Custom ports: e.g., 80,443,21 or 1-65535
Service Version and OS Detection Option(s):
Select service detection option: Determine the version of the service running on port Add
Determine the version of the service running on port
Remote OS detection
Adjust version detection intensity to 5
Limit OS scan to promising targets
Guess OS more aggressively
Firewall / IDS Evasion and
Select firewall evasion option:
Output Format:
Select output format: Normal
Nmap Script(s):
Select Nmap script: HTTP Enum Add
Run Nmap
Identifies the version of the services running on open ports.
Detects the operating system of the remote host.
Increases the intensity of version detection, making it more accurate.
Only performs OS detection on likely responsive hosts to save time.
Makes Nmap more aggressive in guessing the OS when it is uncertain.


Selected Advance mode
PORT GUARD
Enter IP address or range:
Format: 192.168.0.1 or 192.168.0.1-255 or nu.edu.pk
Select mode: Advanced
Scan Type(s):
Select scan type: TCP SYN port scan (Stealth scan) Add
Host Discovery Option(s):
Select host discovery option: Disable host discovery (Port scan only)
Port Selection:
Default (1-1024) Custom ports: e.g., 80,443,21 or 1-65535
Service Version and OS Detection Option(s):
Select service detection option: Determine the version of the service running on
Firewall / IDS Evasion and Spoofing Option(s):
Select firewall evasion option: Scan using fragmented IP packets Add
Scan using fragmented IP packets
Send scans from 10 decoy IPs randomly
Scan using a specific source port 53
Use a specific payload length 50
Output Format:
Select output format: Normal
Nmap Script(s):
Select Nmap script: HTTP Enum Add
Breaks the scan packets into smaller fragments to evade detection by firewalls and intrusion detection systems (IDS).
Uses 10 randomly generated decoy IP addresses to disguise the real source of the scan, making it harder to trace.
Uses port 53 as the source port for the scan packets, which can sometimes bypass firewalls that allow DNS traffic.
Adds extra data to each scan packet, making them 50 bytes long to evade detection by intrusion detection systems.
Run Nmap


Selected Advance mode
PORT GUARD
Enter IP address or range:
Format: 192.168.0.1 or 192.168.0.1-255 or nu.edu.pk
Select mode: Advanced
Scan Type(s):
Select scan type: TCP SYN port scan (Stealth scan) Add
Host Discovery Option(s):
Select host discovery option: Disable host discovery (Port scan only)
Port Selection:
Default (1-1024) Custom ports: e.g., 80,443,21 or 1-65535
Service Version and OS Detection Option(s):
Select service detection option: Determine the version of the service running on port Add
Firewall / IDS Evasion and Spoofing Option(s):
Select firewall evasion option: Scan using fragmented IP packets Add
Output Format:
Select output format: Normal Add
Normal
XML
Grepable
All formats
Nmap Script(s):
Select Nmap script: Add
User can easily select and download required output format.
Run Nmap


Selected Advance mode
PORT GUARD
Enter IP address or range:
Format: 192.168.0.1 or 192.168.0.1-255 or nu.edu.pk
Select mode: Advanced
Scan Type(s):
Select scan type: TCP SYN port scan (Stealth scan) Add
Host Discovery Option(s):
Select host discovery option: Disable host discovery (Port scan only)
Port Selection:
Default (1-1024) Custom ports: e.g., 80,443,21 or 1-65535
Service Version and OS Detection Option(s):
Select service detection option: Determine the version of the service running on port Add
Firewall / IDS Evasion and Spoofing Option(s):
Select firewall evasion option: Scan using fragmented IP packets Add
Output Format:
Select output format: Normal Add
Nmap Script(s):
Select Nmap script: HTTP Enum Add
HTTP Enum
FTP Anon
SMB OS Discovery
SSL Cert
Run Nmap
list common files and directories on a web server one by one to identify potentially interesting or sensitive content.
Checks if the FTP server allows anonymous login, which can be a security risk.
Retrieves and shows SSL certificate details from the target.
Detects the operating system using the SMB protocol, network file sharing protocol

Contributors:

Find us on following social accounts:

Profiles:
https://github.com/arslanjv

https://github.com/sirzaighamabq
https://www.linkedin.com/in/zaigham-a-2a2891269/

License: