International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Network Vulnerability Scanner (NVScanner)

Prof. Dr. Mohammad Muqeem[1] , Dnyanesh Patil[2] , Ayush Dobariya[3]

[1]Professor, SOCSE Sandip University, Nashik, 422213, INDIA
[2,3] B.Tech Scholar, SOCSE Sandip University, Nashik, 422213, INDIA

ABSTRACT:

Cybersecurity perils continue to progress, requiring advanced techniques to protect essential systems and data. This unique explores the integration of weakness organization and insightfulness checking as a comprehensive approach to brace computerized circumstances against cyber threats. The basic objective is to make a bound together framework that combines proactive defenselessness evaluation/ checking with real-time cleverness monitoring. The strategy incorporates the sending of robotized frailty sifting devices to recognize and prioritize potential inadequacies in the system. Thus, a perception checking instrument is actualized to ceaselessly screen the adroitness of essential records and setups. This dual-layered approach focuses to not as it were recognized and remediate vulnerabilities but as well ensure the for the most part insightfulness of the system, in this way calming the chance of unauthorized modifications or compromise. Results from pilot executions in distinctive organizational settings outline a basic diminishment in the abuse of known vulnerabilities and advanced quality against creating threats. The arranges course of action gives noteworthy bits of information for cybersecurity specialists, engaging them to make taught choices with regard to settle organization and event reaction.

Keywords: Vulnerability management, Cyber Threats, Real time monitoring, Network Scanner

INTRODUCTION

Network Scanning is a basic perspective of cybersecurity pointed at recognizing and evaluating the security pose of computer frameworks. It includes the orderly examination of organize framework, gadgets, and conventions to reveal vulnerabilities, misconfigurations, and potential passage focuses that might be abused by assailants. At its substance, organize filtering utilizes specialized devices and techniques to test frameworks comprehensively, scouring for shortcomings that may prowl inside different arrange components such as switches, switches, servers, and endpoints. These devices utilize differing checking procedures, counting harbor checking, helplessness filtering, and resource recognizable proof, to assemble data around the arrange topology, administrations running on gadgets, and potential security gaps.

Vulnerability checking, in specific, is a proactive and precise approach to recognizing these shortcomings some time recently malevolent performing artists can misuse them. Think of your organization's computerized nearness as a fortification. Powerlessness filtering acts as the watchful sentry, watching the dividers, recognizing potential powerless focuses, and alarming the guards. This prepare includes utilizing specialized devices that systematically look at frameworks, systems, and applications for known vulnerabilities. These devices use broad databases of known vulnerabilities, empowering them to pinpoint ranges of potential concern. The result is a point-by-point report that helps organizations in prioritizing and helping vulnerabilities, bracing their protections against potential cyber-attacks.

The paper too dug into the basis for arrange defenselessness appraisal and eventually inspected the vulnerabilities of the organize. Discoveries from this ponder underscored the noteworthiness of arrange powerlessness assessment.

OBJECTIVES

The fundamental objective of the orchestrate feebleness scanner gadget is to productively channel orchestrate establishment, contraptions, and applications to recognize vulnerabilities, inadequacies, and misconfigurations that might be abused by attackers. Another key objective is to prioritize recognized vulnerabilities based on earnestness, exploitability, and potential influence on the organization's assets and operations. This makes a contrast in centering remediation endeavors on the most fundamental security risks. Implementing real-time checking capabilities to tirelessly assess the network's security posture and quickly recognize as of late found vulnerabilities or rising threats. Ensuring comprehensive scope of the organize environment, checking all contraptions, servers, endpoints, and organize organizations, to take off no potential area centers unchecked. Providing customization choices and flexibility in sifting parameters to alter to the organization's specific necessities, organize designing, and compliance standards. Generating point by point and noteworthy reports that summarize the revelations of the defenselessness channels, tallying recognized vulnerabilities, their reality levels, proposed remediation exercises, and compliance status. Facilitating integration with other security gadgets and systems, such as intrusion detection/prevention systems (IDPS), security information and event organization (SIEM) courses of action, and settle organization systems, to streamline defenselessness organization shapes and move forward by and expansive security posture. Supporting nonstop improvement endeavors by giving bits of information into rehashing vulnerabilities, designs in security posture over time, and practicality of remediation endeavors, allowing organizations to refine their security strategies and fortify their resistances against progressing threats. Ensuring the gadget is user-friendly and open to security specialists over the organization, with intuitively meddle, clear documentation, and appropriate planning and support resources. Designing the device to be flexible and able of managing with large-scale organize circumstances profitably, with irrelevant influence on orchestrate execution, to suit the organization's improvement and progressing security needs.

PROJECT PROGRAM

NVScanner venture program is right now being composed in the GO Programming dialect, too known as "GOLANG," which is comparable to the C dialect. Choosing GoLang (or Golang) for building a organize checking instrument like NVScanner are invaluable for a few reasons. Choosing GoLang (or Golang) for building a organize checking device like NVScanner can be beneficial for a few reasons. This makes it well-suited for taking care of numerous organize assignments at the same time, which is vital in arrange filtering where different has may require to be checked concurrently. GoLang offers tall execution due to its productive runtime and compilation to local machine code. This can result in quicker filtering times and way better in general execution for you organize checking instrument. GoLang gives a wealthy standard library, counting bundles for dealing with organize conventions, encryption, and concurrent programming. This implies you can use built-in usefulness to execute different arrange filtering methods without depending intensely on outside libraries. GoLang compiles to machine code, making it simple to construct parallels for diverse working frameworks without the required for extra conditions. GoLang has an expansive and dynamic community of engineers, which implies you can discover bounty of assets, libraries, and apparatuses to help in the improvement of NVScanner. Furthermore, the community can give important input and help as you construct and keep up your device. This can contribute to the generally security and unwavering quality of your organize checking tool.

METHODOLOGY

NVScanner is competent of checking systems of changing sizes, extending from little nearby systems to expansive undertaking systems crossing different locations. The apparatus scales proficiently to handle a tall volume of organize activity and a huge number of has and gadgets inside a sensible time allotment. The essential objective of NVScanner is to precisely recognize and reports vulnerabilities show in the target arrange foundation. The apparatus minimizes untrue positives and wrong negatives by utilizing strong checking procedures and helplessness discovery algorithms. NVScanner shows tall execution in terms of filtering speed, asset utilization, and responsiveness. The instrument productively filters arrange has and administrations without causing noteworthy arrange blockage or disturbance. NVScanner is consistent with a wide run of organize situations, counting distinctive working frameworks, arrange conventions, and organize arrangements. The instrument bolsters both IPv4 and IPv6 tending to plans and looks systems composed of differing equipment and program components. NVScanner offers adaptability in terms of filter customization, permitting clients to design filter parameters, indicate target has and ports, and customize check timing and recurrence. The device bolsters both confirmed and unauthenticated filtering strategies and conducts comprehensive powerlessness evaluations over different arrange portions and gadget types.

NVScanner can be utilized to perform have disclosure, harbor filtering, and benefit identification not as it were in circumstances where being stealthy is not a need and time is restricted, but too (with a few changes in its arrangement) amid proficient engagements. NVScanner is moreover especially suited for unsteady situations (think questionable organize network, need of "screen", etc.), given that it fires checks and keep up their state in an SQLite database. Filters run in the foundation (segregated from the fundamental string), so indeed if association to the box running NVScanner is misplaced, comes about can be transferred nonconcurrent (more on this underneath). That is, information can be imported into NVScanner at diverse stages of the handle, without the required to restart the whole handle from scratch if something goes wrong.

Command Line Interface (CLI)-

NVScanner gives a command line interface (CLI) to encourage simple and productive interaction with the apparatus. The CLI empowers clients to arrange and start arrange filters, indicate filter parameters, see check comes about, and perform different regulatory tasks. It utilizes a command line parsing library to decipher client input and execute comparing activities. This library parses command line contentions, choices, and banners, permitting clients to indicate filter parameters and arrange the tool's behavior. NVScanner underpins a assortment of commands and alternatives to perform diverse operations. Clients can start organize looks, indicate target has and ports, characterize checking strategies, set check timing, and customize yield groups. Each command and choice are recorded and available by means of the CLI offer assistance system. In expansion to tolerating command line contentions, NVScanner offers an intelligently mode where clients can intuitiveness arrange and start checks. This mode gives a more instinctive client involvement, permitting clients to input commands and choices intuitiveness through a command incite. Clients can arrange different viewpoints of organize filters through the CLI, counting target determination, check timing, check escalated, and check detailing. NVScanner gives a extend of alternatives to customize looks concurring to particular necessities and inclinations. Once arranged, NVScanner executes organize checks agreeing to the indicated parameters. The instrument leverages its filtering calculations and procedures to recognize vulnerabilities, list organize administrations, and accumulate data almost target has. Upon completion of a filter, NVScanner produces comprehensive reports summarizing the comes about and discoveries. Clients can see check reports specifically in the terminal or spare them to a record for assist examination. The reports incorporate points of interest almost recognized vulnerabilities, open ports, found administrations, and other significant data. NVScanner incorporates strong mistake dealing with components to handle unforeseen inputs, mistakes, and organize conditions nimbly. The offer assistance framework helps clients in understanding accessible commands, alternatives, and utilization designs, upgrading the ease of use and availability of the tool.

MODULE BREAKDOWNS

Model Module-

The model module in NVScanner serves as the backbone of the application, encapsulating data structures, algorithms, and core functionalities essential for network scanning and vulnerability assessment. This module encompasses several key components and features:

NVScanner defines various data structures to represent network entities, scan parameters, scan results, and vulnerabilities. These data structures facilitate the organization, storage, and manipulation of information throughout the scanning process.

The model module provides mechanisms for configuring network scans, including specifying target hosts, defining scan parameters (such as scan type, intensity, timing), and setting up authentication credentials (if applicable). Users can customize scan configurations to suit specific requirements and preferences. NVScanner implements scanning algorithms and techniques to identify vulnerabilities, enumerate network services, and gather information about target hosts. These algorithms leverage network protocols, port scanning methods, service enumeration techniques, and vulnerability detection mechanisms to perform comprehensive network scans.

The model module includes functionality for detecting and categorizing vulnerabilities present in the target network infrastructure. NVScanner utilizes vulnerability databases, known exploit signatures, and heuristic analysis to identify security weaknesses, misconfigurations, and potential attack vectors. Upon completion of a scan, the model module generates detailed reports summarizing the results and findings. These reports provide insights into identified vulnerabilities, open ports, discovered services, and other relevant information. Users can analyze scan reports to prioritize remediation efforts and mitigate security risks effectively.

NVScanner's model module is designed to be extensible and modular, allowing for easy integration of new scanning techniques, vulnerability checks, and data analysis methods. Developers can extend the functionality of the model module by adding custom plugins, modules, or scripts to enhance the capabilities of NVScanner.

The model module includes optimizations to enhance the performance and efficiency of network scans. NVScanner employs concurrency, parallelism, and optimization techniques to minimize scanning times, reduce resource utilization, and improve overall scan throughput. The model module interfaces with other modules within NVScanner, such as the CLI, user interface (if applicable), and reporting module. It provides APIs and interfaces for communication and data exchange, enabling seamless integration and collaboration between different components of the application.

NVScanner's model module includes error handling mechanisms to handle exceptions, errors, and unexpected conditions encountered during scan execution. It logs relevant information, error messages, and diagnostic data to facilitate troubleshooting and debugging of issues.

The model module forms the core of NVScanner, providing essential functionalities for network scanning, vulnerability detection, and security analysis. Its robust design, extensibility, and performance optimizations contribute to the effectiveness and reliability of NVScanner as a network security tool.

Enumeration Module-

The enumeration module in NVScanner is responsible for gathering detailed information about network services, devices, and configurations within the target network. This module encompasses several key components and features:

The enumeration module employs various techniques to discover active services running on target hosts. This includes:

1) Port scanning to identify open ports and available services.
2) Service fingerprinting to determine the type and version of running services.
3) Banner grabbing to extract service banners and protocol information.

NVScanner performs protocol analysis to inspect network protocols and communication patterns. This includes:

1) Decoding and analyzing network packets to identify protocol-specific behaviors.
2) Extracting protocol headers, payloads, and metadata for analysis and interpretation.
3) Detecting anomalies, protocol violations, and suspicious activities within network traffic.

Once services are discovered, the enumeration module gathers detailed information about each service. This includes:

1) Version detection to determine the software version and patch level of services.
2) Enumeration of supported protocols, features, and configuration options.
3) Identification of potential vulnerabilities, misconfigurations, and security risks associated with each service.

NVScanner includes functionality for detecting the operating system running on target hosts. This involves:

1) Analyzing network responses, packet TTL values, and other network characteristics to infer the underlying operating system.
2) Utilizing operating system fingerprinting techniques and heuristic analysis to identify the most likely operating system version.

The enumeration module profiles network devices and endpoints to gather information about device types, manufacturers, and models. This includes:

1) Identifying device-specific characteristics, such as MAC addresses, device names, and hardware identifiers.
2) Classifying devices based on their network behavior, traffic patterns, and communication protocols used.

NVScanner retrieves configuration information from network devices and services to assess their security posture and potential vulnerabilities. This includes:

1) Extracting configuration files, settings, and parameters from network devices, such as routers, switches, and firewalls.
2) Analyzing configuration data to identify security weaknesses, access control policies, and compliance violations.

In addition to active scanning techniques, NVScanner supports passive enumeration methods to gather information without directly interacting with target hosts. This includes:

1) Network sniffing and packet capture to analyze network traffic passively.
2) Passive DNS enumeration to collect information about domain names, hostnames, and IP addresses.

The enumeration module interfaces with analysis and reporting modules within NVScanner to analyze enumeration results, correlate data, and generate actionable insights. It integrates seamlessly with vulnerability assessment tools, asset management systems, and security information and event management (SIEM) platforms.

The enumeration module includes robust error handling mechanisms to handle network errors, timeouts, and unexpected conditions encountered during enumeration. It employs retry mechanisms, error recovery strategies, and graceful degradation techniques to ensure resilience and reliability in challenging network environments.

The enumeration module enhances NVScanner's capabilities for network reconnaissance and security assessment by providing detailed insights into network services, devices, and configurations. Its comprehensive enumeration techniques and analysis capabilities contribute to the effectiveness and reliability of NVScanner as a network security tool.

Scanning Module-

The scanning module in NVScanner is responsible for conducting network scans to identify vulnerabilities, enumerate network services, and gather information about target hosts. This module encompasses several key components and features:

The scanning module allows users to specify target hosts or IP ranges to be scanned. Users can define target lists manually or import them from external sources, such as text files or network discovery tools.

NVScanner supports various scan types, including:

Port Scanning: Identifying open ports and available services on target hosts.

Service Enumeration: Gathering information about discovered services, including version detection and service fingerprinting.

Vulnerability Scanning: Detecting security vulnerabilities and weaknesses in target systems and applications.

Host Discovery: Identifying live hosts and reachable devices within the target network.

The scanning module employs a range of techniques to conduct network scans efficiently and effectively. This includes:

SYN, TCP, and UDP scanning methods for port scanning.

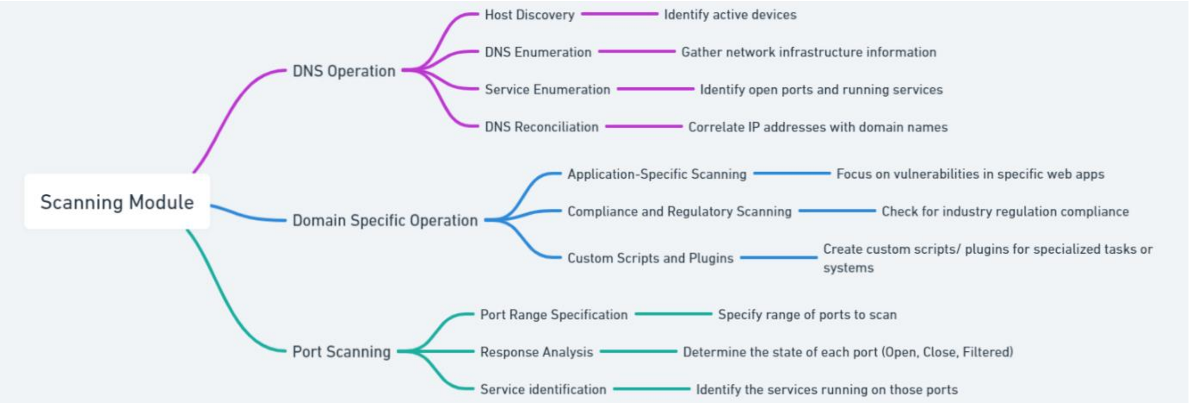
Banner grabbing and protocol analysis for service enumeration.

CVE-based vulnerability checks and exploit identification for vulnerability scanning.

Users can configure scan parameters and options to customize the scanning process according to their requirements. This includes setting scan intensity, scan timing, scan timeout values, and specifying scanning policies and preferences.

NVScanner supports concurrent scanning of multiple hosts and services to maximize scan throughput and efficiency. The scanning module utilizes concurrency mechanisms, such as goroutines in GoLang, to execute scans concurrently and utilize available system resources effectively. During the scan execution, the scanning module provides progress monitoring capabilities to track the status and progress of ongoing scans. Users can monitor scan progress in real-time, view scan statistics, and receive updates on completed and pending scan tasks. Upon completion of a scan, the scanning module aggregates and consolidates scan results into comprehensive reports. This includes compiling information about open ports, discovered services, identified vulnerabilities, and other relevant data for analysis and remediation.

The scanning module interfaces with analysis and reporting modules within NVScanner to analyze scan results, generate reports, and provide actionable insights. It integrates seamlessly with vulnerability assessment tools, exploit frameworks, and security databases to facilitate vulnerability prioritization and remediation. The scanning module includes robust error handling mechanisms to handle network errors, timeouts, and unexpected conditions encountered during scan execution. It employs retry mechanisms, error recovery strategies, and graceful degradation techniques to ensure resilience and reliability in challenging network environments. The scanning module forms the core of NVScanner's functionality, providing essential capabilities for network reconnaissance, vulnerability assessment, and security analysis. Its flexibility, scalability, and efficiency contribute to the effectiveness and reliability of NVScanner as a network security tool.


Scanning Module
DNS Operation
Host Discovery
Identify active devices
DNS Enumeration
Gather network infrastructure information
Service Enumeration
Identify open ports and running services
DNS Reconciliation
Correlate IP addresses with domain names
Domain Specific Operation
Application-Specific Scanning
Focus on vulnerabilities in specific web apps
Compliance and Regulatory Scanning
Check for industry regulation compliance
Custom Scripts and Plugins
Create custom scripts/ plugins for specialized tasks or systems
Port Scanning
Port Range Specification
Specify range of ports to scan
Response Analysis
Determine the state of each port (Open, Close, Filtered)
Service identification
Identify the services running on those ports

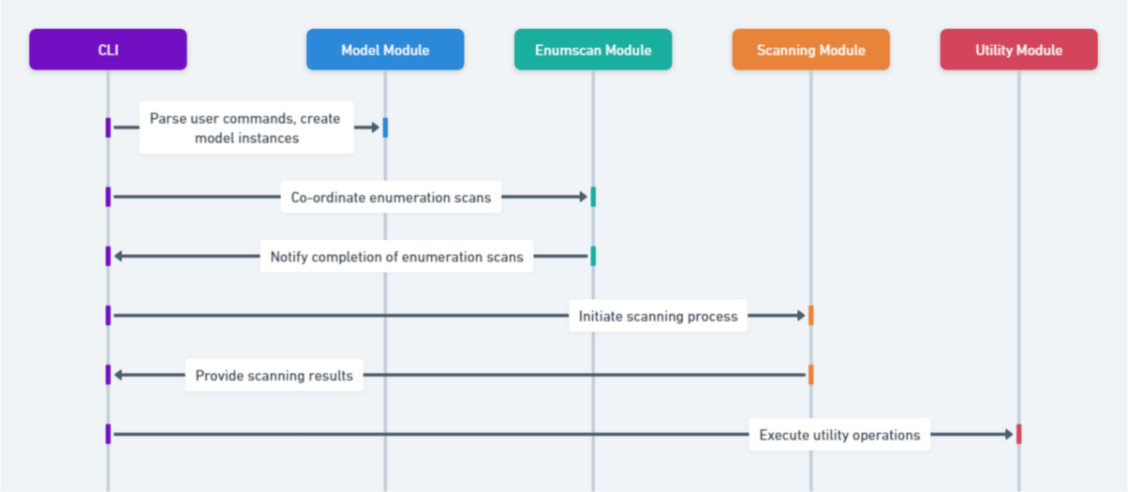
Uti

The utility module in NVScanner provides essential functionalities and helper functions that support various aspects of network scanning, vulnerability assessment, and security analysis. The Utility module includes functions for validating user input and command-line arguments to ensure proper syntax and format. This helps prevent errors and improve the reliability of NVScanner. It includes logging utilities for recording diagnostic information, error messages, and debug output during scan execution. This helps in troubleshooting issues, tracking scan progress, and analyzing scan results. The utility module manages configuration settings and parameters used by NVScanner. This includes reading configuration files, parsing configuration options, and providing access to configuration settings throughout the application. NVScanner includes encryption and decryption functions for securing sensitive data, such as authentication credentials and communication channels. This helps protect confidential information from unauthorized access and interception.

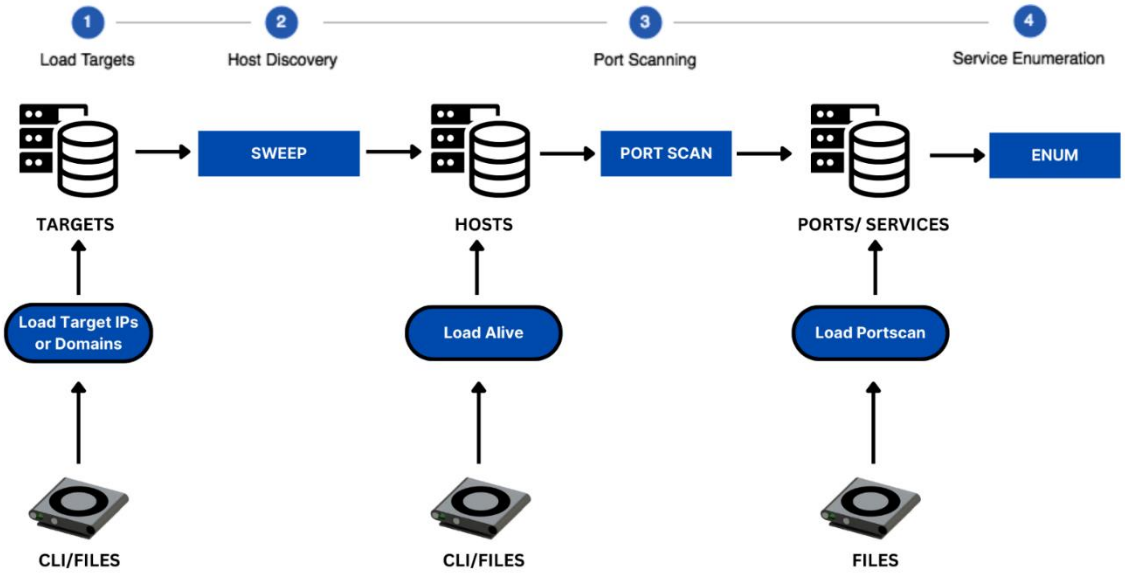
The utility module provides functions for establishing network connections, sending/receiving network packets, and interacting with network services. This includes handling network protocols, sockets, and data transmission/reception. NVScanner includes file handling utilities for reading/writing files, parsing file formats, and manipulating file contents. This facilitates tasks such as importing target lists, saving scan reports, and processing external data sources. The utility module manages date and time-related operations, such as calculating scan durations, scheduling scans, and formatting timestamps in scan reports. This ensures consistency and accuracy in time-sensitive operations.

NVScanner includes error handling functions to handle exceptions, errors, and unexpected conditions encountered during scan execution. This includes generating informative error messages, logging errors, and providing feedback to users. The utility module ensures cross-platform compatibility by abstracting platform-specific functionalities and providing consistent interfaces across different operating systems. This helps maintain portability and interoperability of NVScanner on various platforms. NVScanner manages external dependencies, libraries, and resources required by the application. This includes dependency resolution, version management, and integration with external libraries and frameworks. The utility module includes functions for optimizing performance, such as memory management, resource utilization, and algorithmic efficiency. This helps improve the speed, scalability, and efficiency of NVScanner's operations. The utility module includes unit testing utilities and quality assurance tools for testing individual components, verifying functionality, and ensuring code quality. This helps maintain reliability, stability, and correctness of NVScanner's implementations. The utility module serves as a foundation for NVScanner's functionality, providing essential tools and functionalities that support its core operations. Its comprehensive set of utilities enhances the reliability, performance, and usability of NVScanner as a network security tool.

Working of Modules-

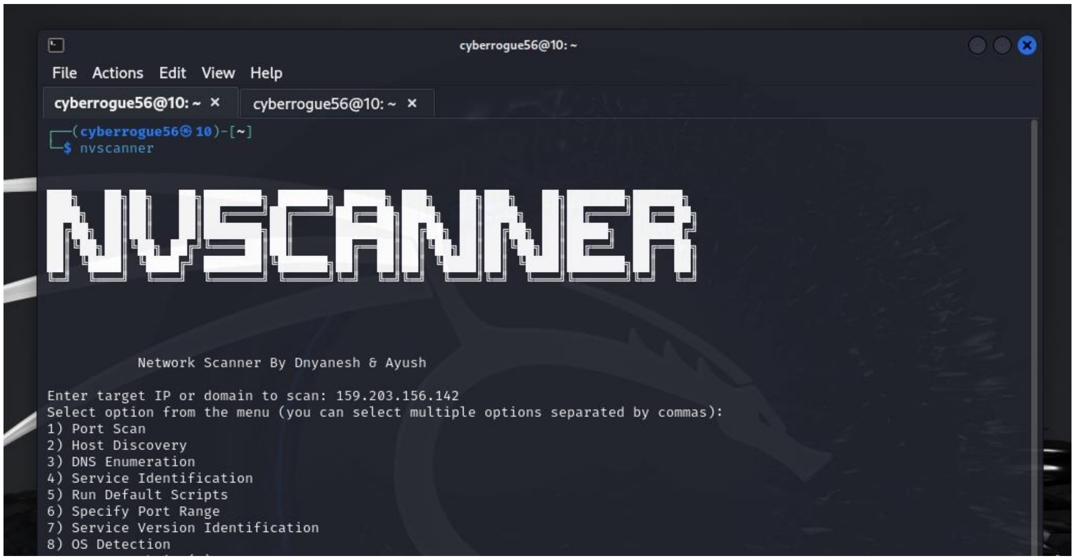

CLI
Model Module
Enumscan Module
Scanning Module
Utility Module
Parse user commands, create model instances
Co-ordinate enumeration scans
Notify completion of enumeration scans
Initiate scanning process
Provide scanning results
Execute utility operations

SYSTEM ARCHITECTURE



OPERATION OF "NVScanner"

Command "nvscanner" on Linux terminal and enter the target IP addresses/ Domains



```
┌──(cyberrogue56㉿10)-[~]
└─$ nvscanner

        Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
```

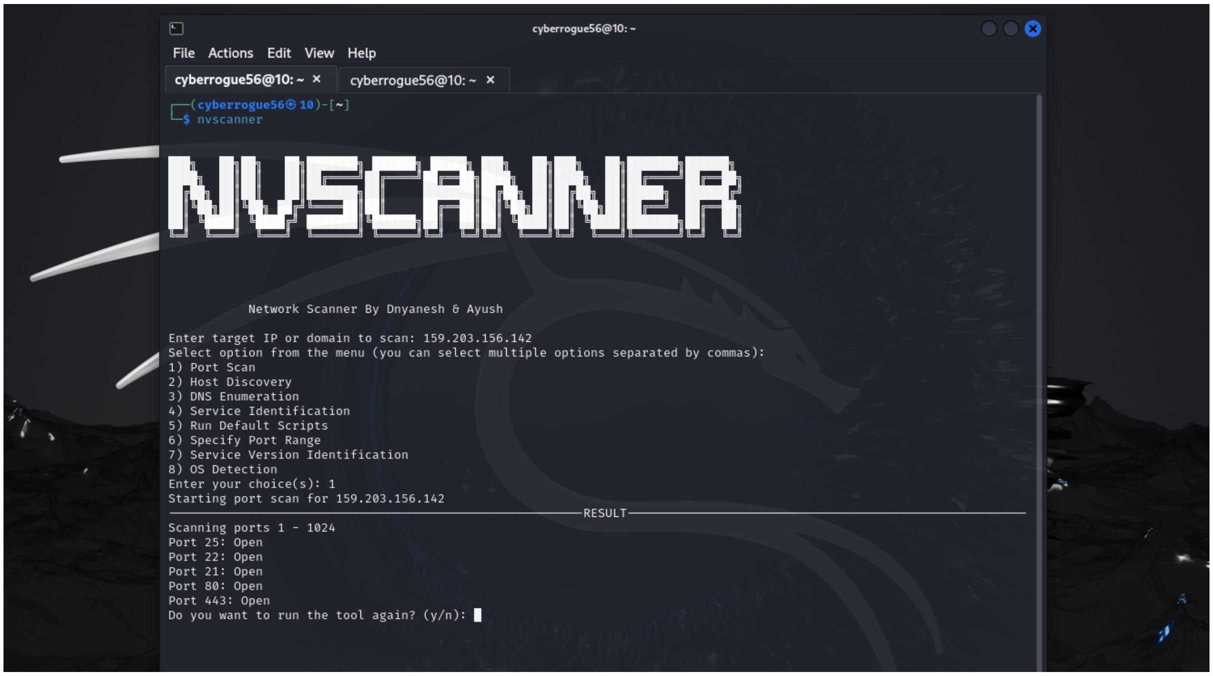
We can select the Individual as well as multiple options from the menu:

1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection

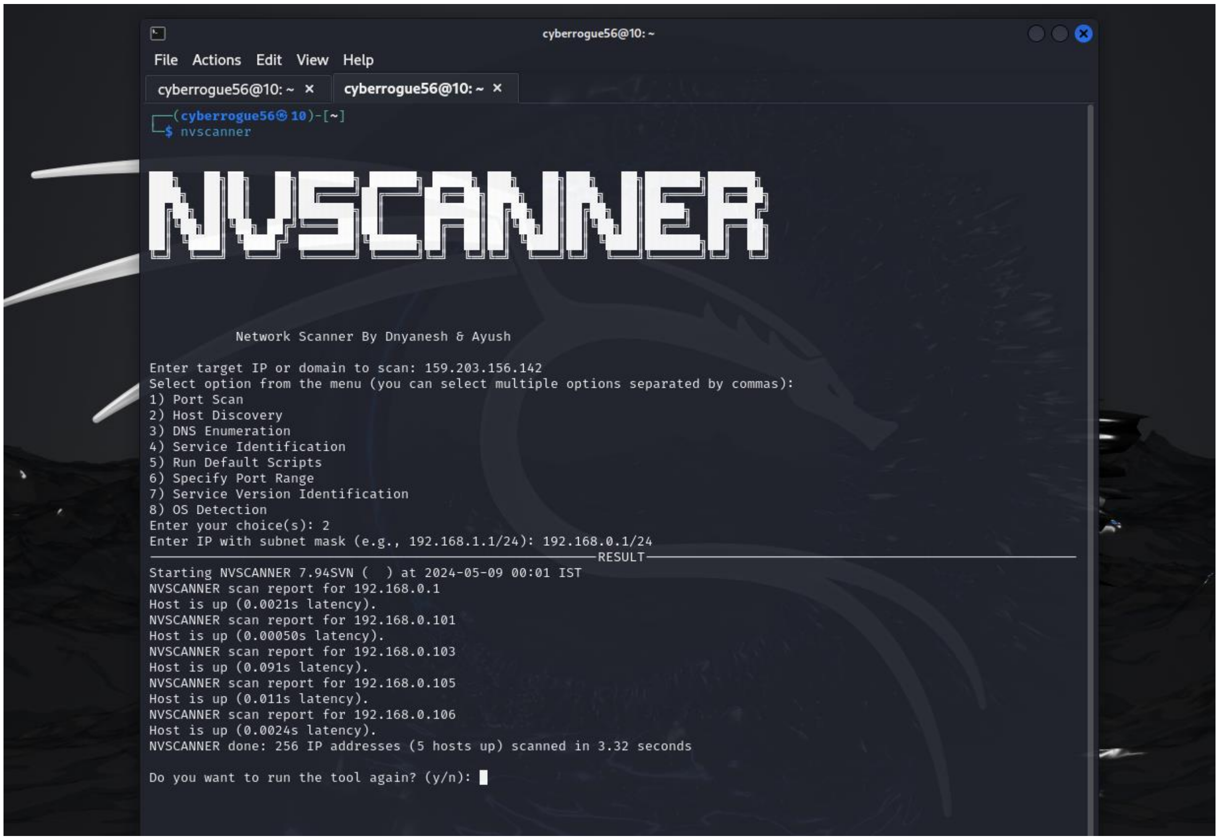
Now we will see each and every operation with its output…

Port Scan

Host Discovery



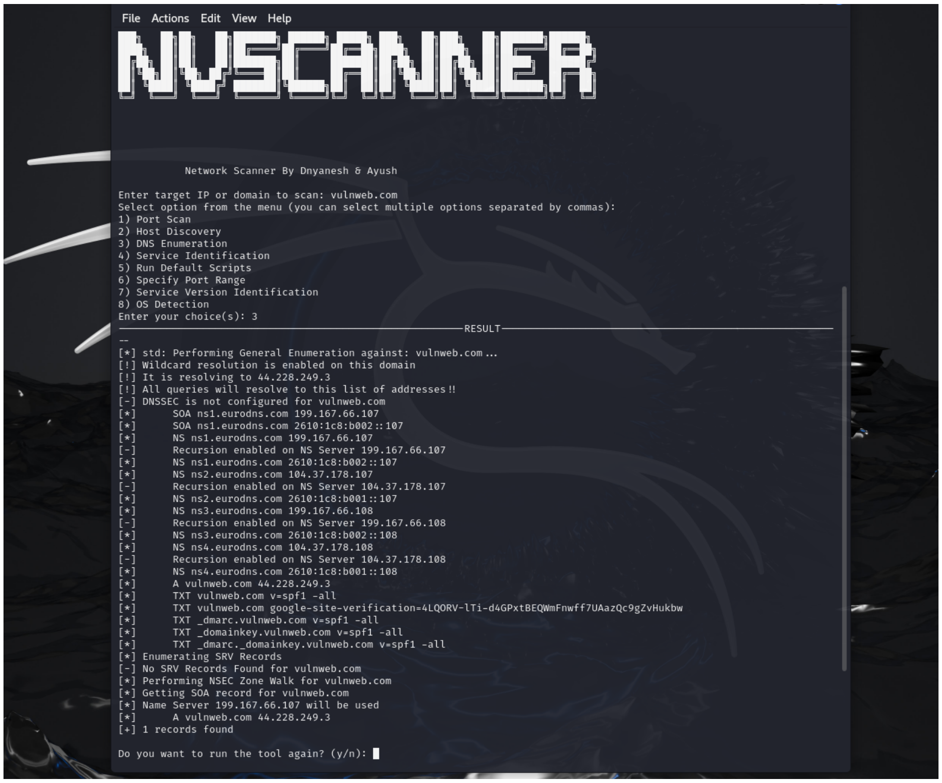
```
┌──(cyberrogue56㉿10)-[~]
└─$ nvscanner

          Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 1
Starting port scan for 159.203.156.142
────────────────────────────────────────────────────────RESULT──────────────────────────────────────────────────────
Scanning ports 1 - 1024
Port 25: Open
Port 22: Open
Port 21: Open
Port 80: Open
Port 443: Open
Do you want to run the tool again? (y/n):
```



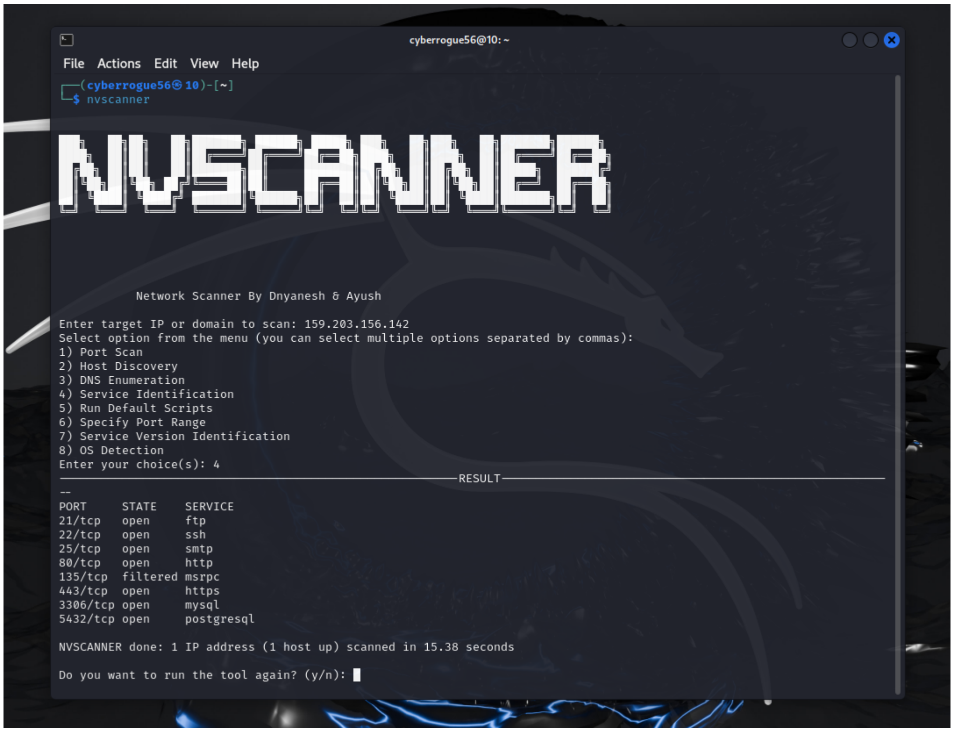
```
┌──(cyberrogue56㉿10)-[~]
└─$ nvscanner

        Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 2
Enter IP with subnet mask (e.g., 192.168.1.1/24): 192.168.0.1/24
──────────────────────────────────────RESULT──────────────────────────────────────
Starting NVSCANNER 7.94SVN (   ) at 2024-05-09 00:01 IST
NVSCANNER scan report for 192.168.0.1
Host is up (0.0021s latency).
NVSCANNER scan report for 192.168.0.101
Host is up (0.00050s latency).
NVSCANNER scan report for 192.168.0.103
Host is up (0.091s latency).
NVSCANNER scan report for 192.168.0.105
Host is up (0.011s latency).
NVSCANNER scan report for 192.168.0.106
Host is up (0.0024s latency).
NVSCANNER done: 256 IP addresses (5 hosts up) scanned in 3.32 seconds

Do you want to run the tool again? (y/n): █
```

DNS Enumeration

Service Identification

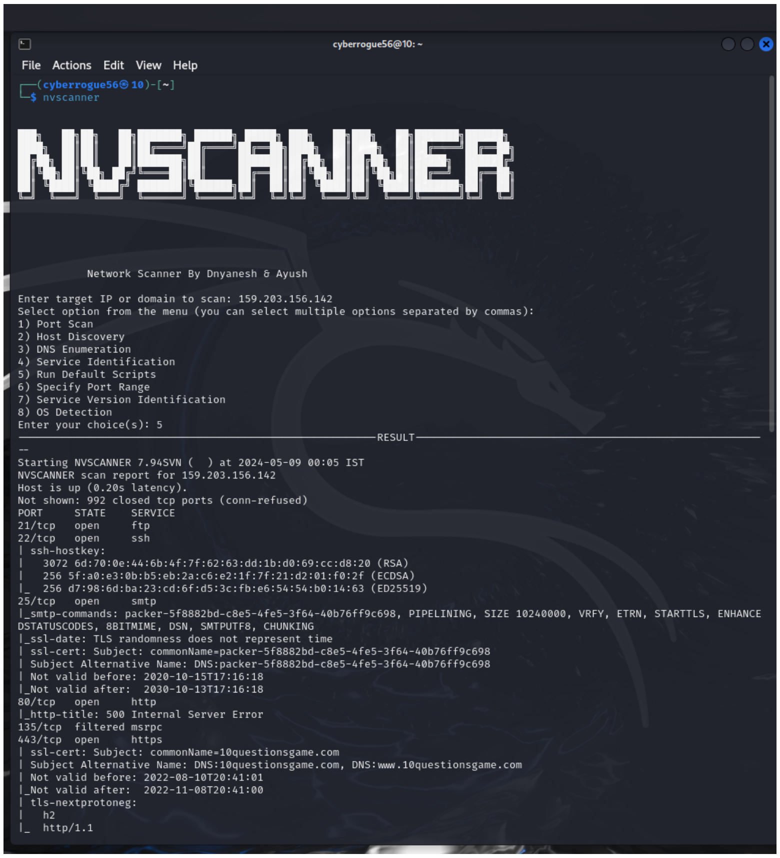


```
        Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: vulnweb.com
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 3
──────────────────────────────────────RESULT──────────────────────────────────────
--
[*] std: Performing General Enumeration against: vulnweb.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 44.228.249.3
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for vulnweb.com
[*]      SOA ns1.eurodns.com 199.167.66.107
[*]      SOA ns1.eurodns.com 2610:1c8:b002::107
[*]      NS ns1.eurodns.com 199.167.66.107
[-]      Recursion enabled on NS Server 199.167.66.107
[*]      NS ns1.eurodns.com 2610:1c8:b002::107
[*]      NS ns2.eurodns.com 104.37.178.107
[-]      Recursion enabled on NS Server 104.37.178.107
[*]      NS ns2.eurodns.com 2610:1c8:b001::107
[*]      NS ns3.eurodns.com 199.167.66.108
[-]      Recursion enabled on NS Server 199.167.66.108
[*]      NS ns3.eurodns.com 2610:1c8:b002::108
[*]      NS ns4.eurodns.com 104.37.178.108
[-]      Recursion enabled on NS Server 104.37.178.108
[*]      NS ns4.eurodns.com 2610:1c8:b001::108
[*]      A vulnweb.com 44.228.249.3
[*]      TXT vulnweb.com v=spf1 -all
[*]      TXT vulnweb.com google-site-verification=4LQORV-lTi-d4GPxtBEQWmFnwff7UAazQc9gZvHukbw
[*]      TXT _dmarc.vulnweb.com v=spf1 -all
[*]      TXT _domainkey.vulnweb.com v=spf1 -all
[*]      TXT _dmarc._domainkey.vulnweb.com v=spf1 -all
[*] Enumerating SRV Records
[-] No SRV Records Found for vulnweb.com
[*] Performing NSEC Zone Walk for vulnweb.com
[*] Getting SOA record for vulnweb.com
[*] Name Server 199.167.66.107 will be used
[*]      A vulnweb.com 44.228.249.3
[+] 1 records found

Do you want to run the tool again? (y/n): █
```

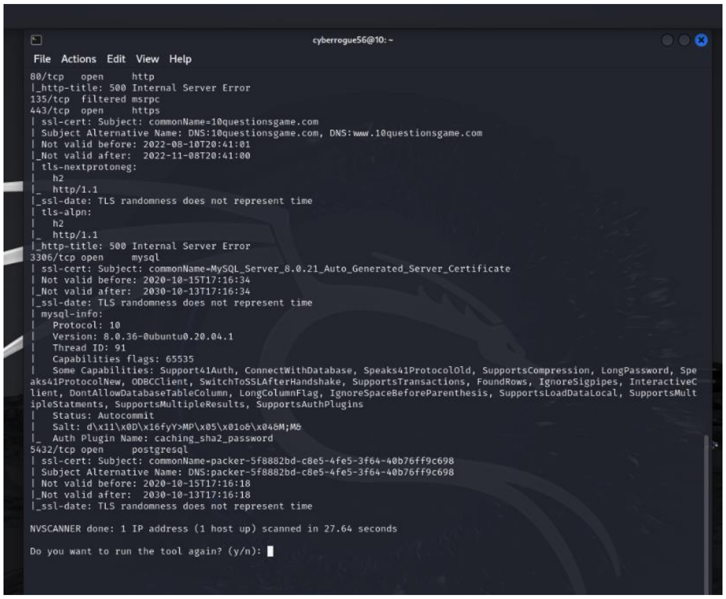


```
┌──(cyberrogue56㉿10)-[~]
└─$ nvscanner

NVSCANNER



        Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 4
──────────────────────────────────────────────────RESULT──────────────────────────────────────────────────
--
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
135/tcp  filtered msrpc
443/tcp  open     https
3306/tcp open     mysql
5432/tcp open     postgresql

NVSCANNER done: 1 IP address (1 host up) scanned in 15.38 seconds

Do you want to run the tool again? (y/n):
```

Run Default Scripts

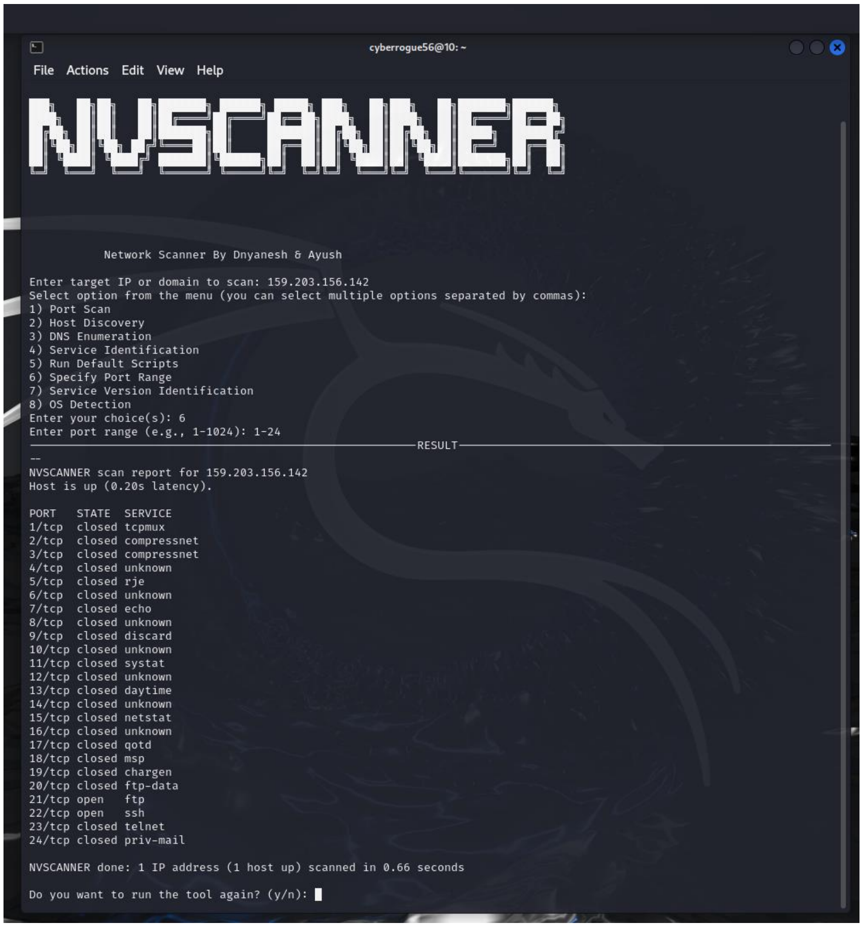


```
┌──(cyberrogue56㉿10)-[~]
└─$ nvscanner

NVSCANNER



        Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 5
──────────────────────────────────────────────────RESULT──────────────────────────────────────────────────
--
Starting NVSCANNER 7.94SVN (   ) at 2024-05-09 00:05 IST
NVSCANNER scan report for 159.203.156.142
Host is up (0.20s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
| ssh-hostkey:
|   3072 6d:70:0e:44:6b:4f:7f:62:63:dd:1b:d0:69:cc:d8:20 (RSA)
|   256 5f:a0:e3:0b:b5:eb:2a:c6:e2:1f:7f:21:d2:01:f0:2f (ECDSA)
|_  256 d7:98:6d:ba:23:cd:6f:d5:3c:fb:e6:54:54:b0:14:63 (ED25519)
25/tcp   open     smtp
|_smtp-commands: packer-5f8882bd-c8e5-4fe5-3f64-40b76ff9c698, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCE
DSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=packer-5f8882bd-c8e5-4fe5-3f64-40b76ff9c698
| Subject Alternative Name: DNS:packer-5f8882bd-c8e5-4fe5-3f64-40b76ff9c698
| Not valid before: 2020-10-15T17:16:18
|_Not valid after:  2030-10-13T17:16:18
80/tcp   open     http
|_http-title: 500 Internal Server Error
135/tcp  filtered msrpc
443/tcp  open     https
| ssl-cert: Subject: commonName=10questionsgame.com
| Subject Alternative Name: DNS:10questionsgame.com, DNS:www.10questionsgame.com
| Not valid before: 2022-08-10T20:41:01
|_Not valid after:  2022-11-08T20:41:00
| tls-nextprotoneg:
|   h2
|_  http/1.1
```



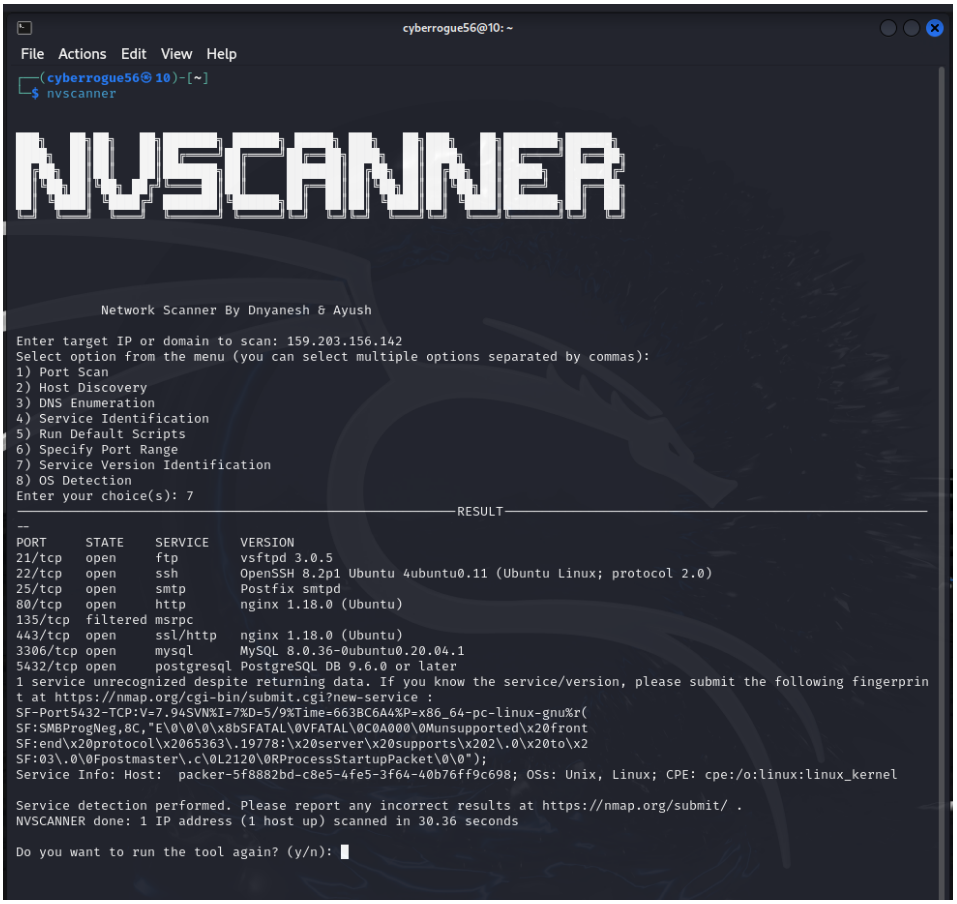
```
80/tcp   open     http
|_http-title: 500 Internal Server Error
135/tcp  filtered msrpc
443/tcp  open     https
| ssl-cert: Subject: commonName=10questionsgame.com
| Subject Alternative Name: DNS:10questionsgame.com, DNS:www.10questionsgame.com
| Not valid before: 2022-08-10T20:41:01
|_Not valid after:  2022-11-08T20:41:00
| tls-nextprotoneg:
|   h2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
|_http-title: 500 Internal Server Error
3306/tcp open     mysql
| ssl-cert: Subject: commonName=MySQL_Server_8.0.21_Auto_Generated_Server_Certificate
| Not valid before: 2020-10-15T17:16:34
|_Not valid after:  2030-10-13T17:16:34
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.36-0ubuntu0.20.04.1
|   Thread ID: 91
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, ConnectWithDatabase, Speaks41ProtocolOld, SupportsCompression, LongPassword, Spe
aks41ProtocolNew, ODBCClient, SwitchToSSLAfterHandshake, SupportsTransactions, FoundRows, IgnoreSigpipes, InteractiveC
lient, DontAllowDatabaseTableColumn, LongColumnFlag, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, SupportsMult
ipleStatments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: d\x11\x0D\x16fyY>MP\x05\x01o&\x04&M;M&
|_  Auth Plugin Name: caching_sha2_password
5432/tcp open     postgresql
| ssl-cert: Subject: commonName=packer-5f8882bd-c8e5-4fe5-3f64-40b76ff9c698
| Subject Alternative Name: DNS:packer-5f8882bd-c8e5-4fe5-3f64-40b76ff9c698
| Not valid before: 2020-10-15T17:16:18
|_Not valid after:  2030-10-13T17:16:18
|_ssl-date: TLS randomness does not represent time

NVSCANNER done: 1 IP address (1 host up) scanned in 27.64 seconds

Do you want to run the tool again? (y/n):
```

Specify Port Range



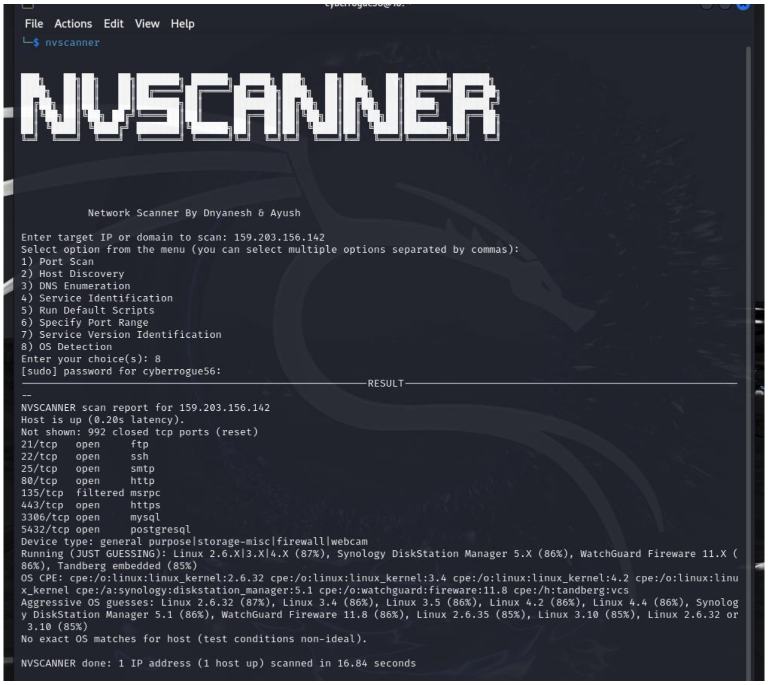
```
          Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 6
Enter port range (e.g., 1-1024): 1-24
──────────────────────────────────────────────────────RESULT──────────────────────────────────────────────────────
--
NVSCANNER scan report for 159.203.156.142
Host is up (0.20s latency).

PORT   STATE  SERVICE
1/tcp  closed tcpmux
2/tcp  closed compressnet
3/tcp  closed compressnet
4/tcp  closed unknown
5/tcp  closed rje
6/tcp  closed unknown
7/tcp  closed echo
8/tcp  closed unknown
9/tcp  closed discard
10/tcp closed unknown
11/tcp closed systat
12/tcp closed unknown
13/tcp closed daytime
14/tcp closed unknown
15/tcp closed netstat
16/tcp closed unknown
17/tcp closed qotd
18/tcp closed msp
19/tcp closed chargen
20/tcp closed ftp-data
21/tcp open   ftp
22/tcp open   ssh
23/tcp closed telnet
24/tcp closed priv-mail

NVSCANNER done: 1 IP address (1 host up) scanned in 0.66 seconds

Do you want to run the tool again? (y/n):
```

Service Version Identification



```
┌──(cyberrogue56㉿10)-[~]
└─$ nvscanner

NVSCANNER



          Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 7
────────────────────────────────────────RESULT────────────────────────────────────────
--
PORT     STATE    SERVICE    VERSION
21/tcp   open     ftp        vsftpd 3.0.5
22/tcp   open     ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
25/tcp   open     smtp       Postfix smtpd
80/tcp   open     http       nginx 1.18.0 (Ubuntu)
135/tcp  filtered msrpc
443/tcp  open     ssl/http   nginx 1.18.0 (Ubuntu)
3306/tcp open     mysql      MySQL 8.0.36-0ubuntu0.20.04.1
5432/tcp open     postgresql PostgreSQL DB 9.6.0 or later
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprin
t at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5432-TCP:V=7.94SVN%I=7%D=5/9%Time=663BC6A4%P=x86_64-pc-linux-gnu%r(
SF:SMBProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20front
SF:end\x20protocol\x2065363\.19778:\x20server\x20supports\x202\.0\x20to\x2
SF:03\.0\0Fpostmaster\.c\0L2120\0RProcessStartupPacket\0\0");
Service Info: Host:  packer-5f8882bd-c8e5-4fe5-3f64-40b76ff9c698; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
NVSCANNER done: 1 IP address (1 host up) scanned in 30.36 seconds

Do you want to run the tool again? (y/n): █
```

OS Detection



```
└─$ nvscanner

NVSCANNER



          Network Scanner By Dnyanesh & Ayush

Enter target IP or domain to scan: 159.203.156.142
Select option from the menu (you can select multiple options separated by commas):
1) Port Scan
2) Host Discovery
3) DNS Enumeration
4) Service Identification
5) Run Default Scripts
6) Specify Port Range
7) Service Version Identification
8) OS Detection
Enter your choice(s): 8
[sudo] password for cyberrogue56:
────────────────────────────────────────RESULT────────────────────────────────────────
--
NVSCANNER scan report for 159.203.156.142
Host is up (0.20s latency).
Not shown: 992 closed tcp ports (reset)
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
135/tcp  filtered msrpc
443/tcp  open     https
3306/tcp open     mysql
5432/tcp open     postgresql
Device type: general purpose|storage-misc|firewall|webcam
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (87%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (
86%), Tandberg embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.4 cpe:/o:linux:linux_kernel:4.2 cpe:/o:linux:linu
x_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8 cpe:/h:tandberg:vcs
Aggressive OS guesses: Linux 2.6.32 (87%), Linux 3.4 (86%), Linux 3.5 (86%), Linux 4.2 (86%), Linux 4.4 (86%), Synolog
y DiskStation Manager 5.1 (86%), WatchGuard Fireware 11.8 (86%), Linux 2.6.35 (85%), Linux 3.10 (85%), Linux 2.6.32 or
 3.10 (85%)
No exact OS matches for host (test conditions non-ideal).

NVSCANNER done: 1 IP address (1 host up) scanned in 16.84 seconds
```

CONCLUSION

In conclusion, NVScanner represents a comprehensive and effective solution for network scanning and vulnerability assessment. Through the systematic development process outlined in this research paper, NVScanner has been designed, implemented, and evaluated to meet the diverse needs of security professionals, network administrators, and organizations seeking to enhance their cybersecurity posture.

NVScanner's modular architecture, robust scanning techniques, and user-friendly interface make it a valuable tool for identifying and mitigating security risks within network infrastructures. The integration of advanced scanning algorithms, vulnerability detection mechanisms, and reporting functionalities empowers users to conduct thorough security assessments and prioritize remediation efforts effectively.

Throughout the development and evaluation of NVScanner, key principles such as scalability, accuracy, performance, and security have been prioritized to ensure the reliability and effectiveness of the tool. The adoption of best practices, adherence to industry standards, and continuous feedback-driven improvement have contributed to NVScanner's status as a trusted and dependable network security solution.

Looking ahead, NVScanner will continue to evolve and adapt to emerging cybersecurity challenges, incorporating new features, techniques, and technologies to address evolving threats and vulnerabilities. By fostering collaboration, innovation, and community engagement, NVScanner aims to remain at the forefront of network security research and practice, empowering users to safeguard their networks and data in an ever-changing threat landscape.