International Journal of Research Publication and Reviews

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

Port Capturer

Nanmaran M[1], Dr. B. Kalaiselvi[2]

[1]Final Year/ Cyber Security, [2]Associate Professor / CSE
[1,2] Mahendra Engineering College, Namakkal
Email: [1]maaran1314@gmail.com, [2]kalairs2003@gmail.com, [3]kalaiselvib@mahendra.info

ABSTRACT

In today's interconnected digital landscape, network security and efficient network management are paramount concerns. As networks continue to grow in complexity and importance, the need for robust tools to assess and monitor them becomes increasingly critical. This paper introduces the Port Capture Project, a comprehensive and versatile solution designed to address these challenges.

The Port Capture Project is an innovative tool developed to streamline the identification of open ports and the retrieval of MAC addresses on target systems. Open ports serve as potential entry points for unauthorized access or vulnerabilities, making their identification a fundamental aspect of network security. Concurrently, knowing the MAC addresses of network devices aids in device tracking, network optimization, and security monitoring. The Port Capture Project bridges these requirements by offering a user-friendly interface and a range of scanning options, catering to network administrators, security professionals, and organizations seeking to fortify their network defenses and efficiency.

1. INTRODUCTION:

In today's digitally interconnected world, network security and efficient network management are paramount concerns. As networks continue to grow in complexity and importance, the need for robust tools to assess and monitor them becomes increasingly critical. This paper introduces the TCP Port Capture Project, a comprehensive solution designed to address the fundamental challenges of TCP port scanning, service identification, and MAC address retrieval within network environments.

1.1 Background and Motivation:

The TCP (Transmission Control Protocol) serves as a cornerstone of network communication, facilitating the reliable and ordered exchange of data across interconnected devices. Ports within the TCP protocol are designated endpoints for communication, allowing for the efficient and organized transfer of information. The accessibility of these ports — whether they are open or closed — holds critical implications for network security and service availability.

Detecting open TCP ports and identifying the associated services on a target system are foundational tasks for network administrators and security professionals. Open ports represent potential entry points for unauthorized access or exploitation, while knowing the services running on these ports is essential for vulnerability assessment and service management.

Concurrently, network administrators often require the capability to retrieve the Media Access Control (MAC) address of network devices. The MAC address serves as a unique identifier for devices on a network, enabling precise device tracking, facilitating network optimization, and enhancing security monitoring.

1.2 Project Objectives:

The TCP Port Capture Project is designed with a tri-fold purpose:

To simplify and enhance the detection of open TCP ports on a target system, facilitating rapid assessment of potential vulnerabilities or services operating on that system.

To provide a means of identifying the services running on these open ports, aiding in service management and network optimization.

To offer an accessible means of retrieving the MAC address of the target system, aiding in device tracking and bolstering network management and security.

The TCP Port Capture Project represents a valuable contribution to the field of network security and management by offering a dedicated tool for TCP port scanning, service identification, and MAC address retrieval. Its user-friendly interface and focused functionality empower network administrators and security professionals with the means to enhance their network analysis capabilities, leading to improved security posture, efficient service management, and optimized network performance in TCP-based environments.

2. RELATED WORK:

In the realm of network security, TCP port scanning, service identification, and MAC address retrieval have been subjects of extensive research and tool development. Understanding the landscape of related work is essential to contextualize the contributions and innovations of the TCP Port Capture Project.

2.1 TCP Port Scanning:

TCP port scanning techniques have evolved significantly over the years. The primary goal of these techniques is to identify open ports on target systems. A few noteworthy approaches include:

2.2 Service Identification:

Service identification is a critical aspect of network analysis. Tools and techniques have been developed to not only identify open ports but also determine the services running on those ports. Prominent methods include:

Banner Grabbing: This technique involves connecting to a port and analyzing the initial banner or response from the service to identify it.

OS Fingerprinting: Some tools go a step further by attempting to identify the underlying operating system based on characteristics of the responses received.

2.3 MAC Address Retrieval:

Retrieving the MAC address of a network device is crucial for device tracking and network management. While MAC addresses can often be obtained through ARP (Address Resolution Protocol) requests, specialized tools have been developed to facilitate this process, particularly when ARP is not feasible.

2.4 Existing Tools:

Notable existing tools, such as Nmap, Wireshark, and Angry IP Scanner, offer varying degrees of functionality related to TCP port scanning, service identification, and MAC address retrieval. These tools have contributed significantly to the field, providing a foundation upon which the TCP Port Capture Project builds.

2.5 Limitations and Opportunities:

Existing solutions often excel in specific areas, but there is a continued need for comprehensive and user-friendly tools that combine TCP port scanning, service identification, and MAC address retrieval in a single interface. Additionally, advancements in network technology, the proliferation of IoT devices, and the evolving threat landscape present new challenges and opportunities for innovation in this field.

The TCP Port Capture Project aims to address these challenges by providing a unified and accessible solution that simplifies network analysis, enhances security, and aids in efficient network management. It leverages the lessons learned from related work to offer a comprehensive toolset for network administrators and security professionals, with a focus on TCP-based environments and service identification alongside MAC address retrieval.

3. METHODOLOGY:

The TCP Port Capture Project is designed as a command-line tool, providing network administrators and security professionals with a powerful yet straightforward means of TCP port scanning, service identification, and MAC address retrieval. This section outlines the key command-line instructions and processes that constitute the tool's methodology.

3.1 Command-Line Interface:

The TCP Port Capture Project's command-line interface allows users to customize their network analysis according to their specific requirements. Users can access the tool's functionalities by running the command-line executable and specifying relevant parameters.

3.2 TCP Port Scanning:

The tool offers various command-line options for TCP port scanning, catering to diverse network analysis needs:

3.2.1 Top 100 Ports:

Users initiate the "Top 100 Ports" scan by providing the appropriate command-line flag or parameter, specifying the target IP address.

The tool then iterates through the top 100 most commonly used TCP ports, attempting to establish connections and recording the results, including the state of each scanned port.

3.2.2 Top 1000 Ports:

The "Top 1000 Ports" scan is executed similarly, with users specifying the desired scan option and target IP address.

The tool extends the scanning range to the top 1000 TCP ports, providing a more comprehensive analysis.

3.2.3 All Ports:

For an exhaustive assessment, users can trigger the "All Ports" scan by selecting the corresponding command-line option.

The tool compiles a list of all possible TCP port numbers (0 to 65535) and scans each port, recording the results comprehensively.

3.2.4 Custom Ports:

Users with specific port ranges of interest can define custom scanning parameters, such as specifying the range or a list of ports to scan via command-line arguments.

3.3 Service Identification:

Service identification, a critical aspect of network analysis, is seamlessly integrated into the command-line interface:

3.3.1 Banner Grabbing:

The tool initiates connections to open ports detected during the scanning process.

Banner grabbing commands are sent to each open port, capturing the initial response from the service running on that port.

The tool identifies services based on these responses and records the results, associating them with the respective open ports.

3.4 MAC Address Retrieval:

Retrieving the MAC address of the target system is facilitated through command-line execution:

3.4.1 ARP Request:

Users can request the retrieval of the MAC address by specifying the target IP address and ARP request command-line parameters.

The tool sends ARP requests to the target IP address, capturing the response that includes the MAC address.

The retrieved MAC address is then displayed in the command-line output.

3.5 Data Output:

The tool provides clear and structured command-line output, presenting users with essential information about open ports, identified services, and retrieved MAC addresses.

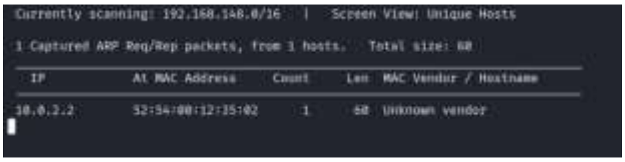
3.6 Ease of Use:

The command-line interface is designed for simplicity and ease of use, allowing users to customize their network analysis by invoking specific commands and parameters.

The TCP Port Capture Project's command-line methodology empowers users to efficiently conduct TCP port scanning, service identification, and MAC address retrieval, making it a valuable addition to network administrators' and security professionals' toolkit. Its flexibility, comprehensive scanning options, and user-friendly command-line interface ensure that it meets the needs of diverse network analysis scenarios.

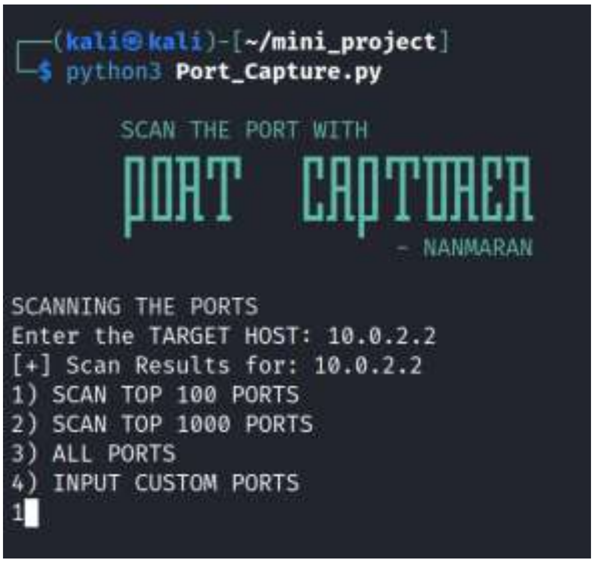
4. RESULT:

The IP available in my network:



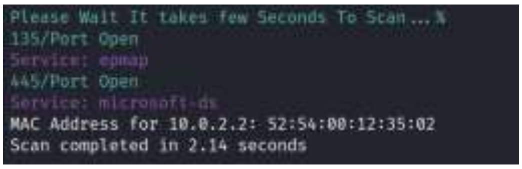
```
Currently scanning: 192.168.148.0/16   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 ______________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ______________________________________________________________________________
 10.0.2.2        52:54:00:12:35:02      1      60  Unknown vendor
```

Top 100 Ports:



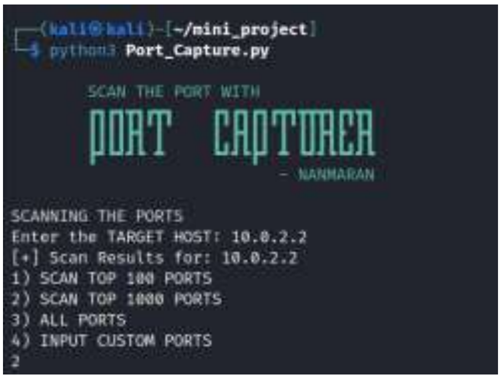
```
┌──(kali㉿kali)-[~/mini_project]
└─$ python3 Port_Capture.py

        SCAN THE PORT WITH
        PORT  CAPTURER
                        - NANMARAN

SCANNING THE PORTS
Enter the TARGET HOST: 10.0.2.2
[+] Scan Results for: 10.0.2.2
1) SCAN TOP 100 PORTS
2) SCAN TOP 1000 PORTS
3) ALL PORTS
4) INPUT CUSTOM PORTS
1
```

Scan Results:



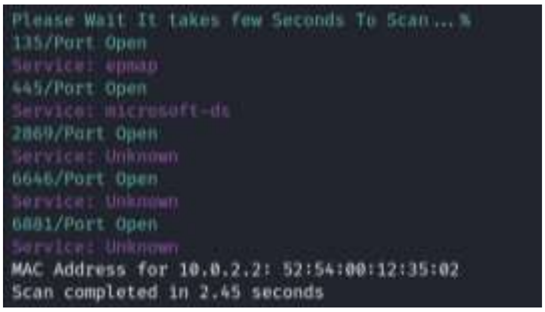
```
Please Wait It takes few Seconds To Scan ... %
135/Port Open
Service: epmap
445/Port Open
Service: microsoft-ds
MAC Address for 10.0.2.2: 52:54:00:12:35:02
Scan completed in 2.14 seconds
```

Top 1000 Ports:



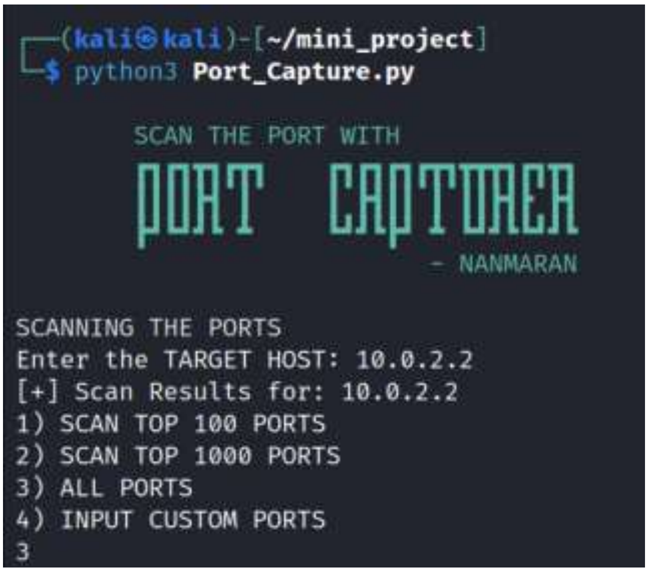
```
┌──(kali㉿kali)-[~/mini_project]
└─$ python3 Port_Capture.py

        SCAN THE PORT WITH
        PORT  CAPTURER
                        - NANMARAN

SCANNING THE PORTS
Enter the TARGET HOST: 10.0.2.2
[+] Scan Results for: 10.0.2.2
1) SCAN TOP 100 PORTS
2) SCAN TOP 1000 PORTS
3) ALL PORTS
4) INPUT CUSTOM PORTS
2
```

Scan Results:



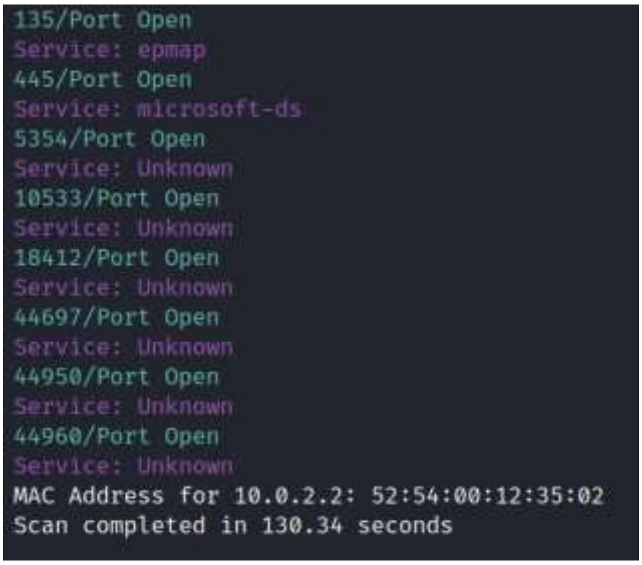
```
Please Wait It takes few Seconds To Scan...%
135/Port Open
Service: epmap
445/Port Open
Service: microsoft-ds
2869/Port Open
Service: Unknown
6646/Port Open
Service: Unknown
6881/Port Open
Service: Unknown
MAC Address for 10.0.2.2: 52:54:00:12:35:02
Scan completed in 2.45 seconds
```

All Ports [0-65365]:



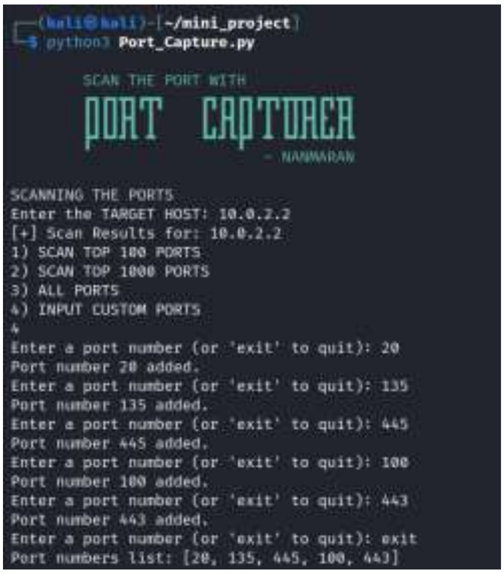
```
┌──(kali㉿kali)-[~/mini_project]
└─$ python3 Port_Capture.py

        SCAN THE PORT WITH
        PORT  CAPTURER
                          - NANMARAN

SCANNING THE PORTS
Enter the TARGET HOST: 10.0.2.2
[+] Scan Results for: 10.0.2.2
1) SCAN TOP 100 PORTS
2) SCAN TOP 1000 PORTS
3) ALL PORTS
4) INPUT CUSTOM PORTS
3
```

Scan Results:



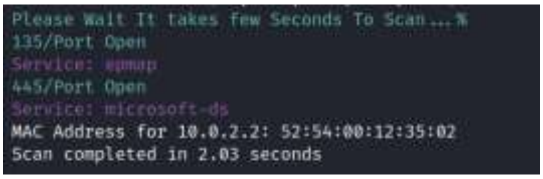
```
135/Port Open
Service: epmap
445/Port Open
Service: microsoft-ds
5354/Port Open
Service: Unknown
10533/Port Open
Service: Unknown
18412/Port Open
Service: Unknown
44697/Port Open
Service: Unknown
44950/Port Open
Service: Unknown
44960/Port Open
Service: Unknown
MAC Address for 10.0.2.2: 52:54:00:12:35:02
Scan completed in 130.34 seconds
```

Custom Ports:



```
┌──(kali@kali)-[~/mini_project]
└─$ python3 Port_Capture.py

        SCAN THE PORT WITH
        PORT  CAPTURER
                        - NANMARAN

SCANNING THE PORTS
Enter the TARGET HOST: 10.0.2.2
[+] Scan Results for: 10.0.2.2
1) SCAN TOP 100 PORTS
2) SCAN TOP 1000 PORTS
3) ALL PORTS
4) INPUT CUSTOM PORTS
4
Enter a port number (or 'exit' to quit): 20
Port number 20 added.
Enter a port number (or 'exit' to quit): 135
Port number 135 added.
Enter a port number (or 'exit' to quit): 445
Port number 445 added.
Enter a port number (or 'exit' to quit): 100
Port number 100 added.
Enter a port number (or 'exit' to quit): 443
Port number 443 added.
Enter a port number (or 'exit' to quit): exit
Port numbers list: [20, 135, 445, 100, 443]
```

Scan Results:



```
Please Wait It takes few Seconds To Scan....%
135/Port Open
Service: epmap
445/Port Open
Service: microsoft-ds
MAC Address for 10.0.2.2: 52:54:00:12:35:02
Scan completed in 2.03 seconds
```

5. DISCUSSION

5.1 Practical Applications:

The TCP Port Capture Project has a wide range of practical applications across various domains:

Network Security: It serves as a vital tool for identifying open ports and understanding the services running on them. Network administrators can leverage this information to bolster their security measures, promptly addressing potential vulnerabilities.

Device Tracking: The ability to retrieve MAC addresses aids in precise device tracking. Organizations can monitor the movement and activity of devices on their networks, enhancing asset management and security.

Network Optimization: By identifying services running on open ports, network administrators can optimize network resources and ensure the efficient delivery of services to end-users.

5.2 Implications:

The implications of the TCP Port Capture Project extend beyond immediate network analysis:

Enhanced Security Posture: Accurate port scanning and service identification contribute to a more robust security posture, enabling organizations to proactively address potential threats.

Streamlined Network Management: The project simplifies device tracking and network optimization, resulting in more efficient network management.

5.3 STRENGTHS AND LIMITATIONS:

Strengths: The project's modular design, user-friendly command-line interface, and comprehensive scanning options make it a valuable tool for network professionals. Its combination of TCP port scanning, service identification, and MAC address retrieval sets it apart from many existing tools.

Limitations: The project focuses exclusively on TCP scanning, and while this is a common protocol, there may be scenarios where UDP port scanning or other protocols are required. Additionally, the accuracy of service identification relies on known service banners, and the tool may encounter challenges in identifying proprietary or less common services.

5.4 Future Enhancements:

The TCP Port Capture Project lays a solid foundation for further development and improvement:

Protocol Expansion: Future versions could expand support to include UDP scanning and other protocols, broadening the tool's applicability.

Machine Learning Integration: Incorporating machine learning techniques may enhance service identification accuracy, particularly for identifying proprietary or non-standard services.

Scalability and Performance: Enhancements in scalability and performance can ensure the tool remains effective in large and complex network environments.

6. CONCLUSION

The TCP Port Capture Project presents a valuable solution for network administrators and security professionals, offering a unified and user-friendly command-line tool for TCP port scanning, service identification, and MAC address retrieval. By simplifying and streamlining these critical network analysis tasks, the project contributes to enhanced network security, efficient device tracking, and network optimization.

As networks continue to evolve and grow in complexity, the need for versatile and accessible tools like the TCP Port Capture Project becomes increasingly evident. Its modular design, range of scanning options, and potential for future enhancements position it as a valuable asset for those responsible for securing and managing networks in today's interconnected world.

In conclusion, the TCP Port Capture Project underscores the importance of innovation in network analysis tools, offering a tangible contribution to the ever-evolving field of network security and management. It empowers professionals with the means to navigate the challenges of modern networks, ultimately leading to safer, more efficient, and better-managed network environments.

7. REFERENCES

Books

[1] Nmap Network Scanning: The Official Nmap Project Guide by Gordon Lyon (2009)

[2] Hacking: The Art of Exploitation by Jon Erickson (2008)

[3] Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers by TJ O'Connor (2015)

Links

[4] Nmap website: https://nmap.org/

[5] Official Nmap documentation: https://nmap.org/docs.html

[6] Nmap tutorial: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

[7] Port scanning tutorial: https://nmap.org/book/port-scanning-tutorial.html

Blogs

[8] Nmap blog: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

[9] Security Onion blog: https://blog.securityonion.net/

[10] SensePost blog: https://sensepost.com/blog/

[11] PacketStorm Security blog: https://packetstormsecurity.com/