CYBER ODYSSEY: FROM FOOT PRINTING TO THREAT MITIGATION

P.S.S.Geethika[1], D.Vagbhat[2], V.Kiran Kumar[3], K.Venkata Pratap[4], S.Rakesh[5]

[1]Assistant Professor, Department of Computer Science and Engineering, Raghu Engineering College

[2,3,4,5] student, Department of Computer Science and Engineering, Raghu Engineering College

Abstract – **"Cybersecurity Odyssey: From Foot printing to Threat Mitigation" equips participants with a robust understanding of both theoretical knowledge with real world hands-on tasks to provide participants a solid understanding of the fundamentals of cyber security. The first step in this comprehensive educational journey is the reconnaissance techniques that helps the learners inacquiring intelligence same as the attackers to intelligence. The next steps include exploiting popular web application vulnerability like SQL injection and perform network scanning to identify potential vulnerabilities like open ports and services, enhancing knowledge of network security using tools like Nmap and Netcat. The program examines various tactics, such as password cracking techniques using Ophcrack on Windows 7, highlighting the importance of robust password policies and encryption methods andphishing attack simulations highlights risks associated with social engineering that deals with different tactics such as spear phishing and mass mailings. Exploiting popular web applications vulnerabilities like Cross Site Scripting (XSS) and SQL injection by using technologies like Damn Vulnerable Web Application (DVWA) and the Browser Exploitation Framework (BeEF) tools, participants will gain hands-on experience in identifying and exploiting vulnerabilities with great ease. Malware analysis and reverse engineering exercises improve threat detection and mitigation capabilities, and insider attack simulations using honeypots and intrusion detection systems (IDS) using Snort emphasize the value of strong internal security. Exploring the Remote Access Trojans (RATs) attack using VEIL, Metasploit framework and Meterpreter sheel and Man-in-the-Middle (MitM) attacks using ARP spoofing, Metasploit framework and Bettercap highlights the risks of unauthorized access and data collection. Simulations of DoS and DDoS attacks using LIOC tool, hping and Metasploit framework equip participants with effective mitigation strategies against service disruptions. Bringing theory and practice together, Studying Cyber Security enables participants to confidentlyand flexibly defend against various cyber threats and prepares them to navigate the ever-changing digital landscape.**

Keywords – **Foot printing, Threat Mitigation, Encryption methods, Malware analysis**

I. INTRODUCTION

In our increasingly interconnected world, cybersecurity has emerged as a critical concern, with cyber threats posing significant risks to individuals, organizations, and governments. Despite the growing demand for cybersecurity professionals, there exists a gap between theoretical knowledge and practical skills. This paper, "Cybersecurity Exploration: From Foot printing to Threat Mitigation," aims to address this gap by providing participants with hands-on experience in dealing with real-world cyber threats. Through a combination of theoretical concepts and practical exercises, participants will gain the skills needed to identify, assess, and mitigate cyber threats effectively. This introduction provides an overview of the paper's objectives, scope, and significance, setting the stage for a comprehensive exploration of cybersecurity principles and practices.

In today's digital age, where the reliance on technology is ubiquitous, cybersecurity has emerged as a critical concern. The proliferation of interconnected devices, the exponential growth of digitaldata, and the increasing sophistication of cyber threats have heightened the need for robust cybersecurity measures. From high-profile data breaches affecting millions of individuals to targeted cyber-attacks on critical infrastructure, the repercussions of inadequate cybersecurity practices are far-reaching and profound.

The central aim of this paper is to equip participants with practical cybersecurity expertise and insights, enabling them to adeptly tackle diverse cyber threats. Its specific objectives revolve around offering hands-on experience through practical exercises and simulations, enhancing comprehension of cybersecurity principles and methodologies, and arming participants with the capabilities to recognize, evaluate, and counter cyber threats across different contexts. Moreover, it seeks to cultivate a proactive culture of cybersecurity awareness and preparedness among all participants involved.

The significance of this paper lies in its potential to address the critical gap between theoretical knowledge and practical application in cybersecurity education and training. By providing participants with hands-on experience and immersive learning opportunities, this paper aims to empower them to become effective cybersecurity practitioners and advocates. Furthermore, by fostering a culture of proactive cybersecurity awareness and readiness, this paper seeks to contribute to the broader goal of enhancing digital resilience and security across individuals, organizations, and society as a whole.

II. RESEARCH METHODOLOGY

The literature on cybersecurity delves into evolving threats and defence strategies. Foundational techniques like foot printing offer insights into attackers' intelligence-gathering methods. Studies stress tools like WHOIS lookup, netcraft, Shodan.io, and DNSdumpster for vulnerability assessment. Web security concerns, especially SQL injection attacks, highlight the need for robust defenses. Research explores XSS vulnerabilities using tools like DVWA and BeEF, emphasizing understanding common flaws. Nmap aids in identifying entry points, underscoring the importance of regular scans. Password cracking with Ophcrack emphasizes strong policies. Phishing threats and malware analysis are significant areas of study. Insider attacks and defense mechanisms like honeypots and IDS are explored. In summary, cybersecurity literature highlightsdiverse threats and proactive defense strategies, essential for mitigating risks in today's digital landscape.

Cybersecurity has become an integral aspect of modern life, with individuals and organizations facing an increasing number of threats in the digital realm. The landscape of cybersecurity is constantly evolving, shaped by advancements in technology and the strategies employed by malicious actors. Understanding this landscape involves examining the various types of cyber threats, the motivations behind them, and the measures taken to mitigate risks. Foot printing serves as the initial phase of a cyber-attack, involving the collection of information about a target system or network. Techniques such as WHOIS lookup, netcraft, Shodan.io, and DNSdumpster are commonly used for reconnaissance purposes. By analyzing publicly available data, attackers can gain insights into the target's infrastructure, which forms the basis for subsequent stages of the attack.

Malware represents a pervasive threat in the cybersecurity landscape, encompassing a wide range of malicious software designed to infiltrate and disrupt systems. Analyzing malware behavior through techniques like static analysis with IDA Pro aids in identifying indicators of compromise and developing strategies for mitigation. Insider threats pose a significant risk to organizations, as authorized individuals may intentionally or inadvertently compromise security. Implementing measures such as honeypots and Intrusion Detection Systems (IDS) using tools like Snort helps detect and mitigate potential insider attacks. By monitoring network activity and identifying anomalous behavior, organizations can proactively defend against insider threats and safeguard sensitive data.

The cybersecurity landscape is constantly evolving, driven by advancements in technology and the evolving tactics of cybercriminals. Emerging trends such as the proliferation of Internet of Things(IoT) devices and the rise of artificial intelligence (AI) in cyber-attacks present new challenges for security professionals. Understanding these trends and anticipating future developments is essential for staying ahead of emerging threats and effectively protecting digital assets. Implementing best practices is crucial for building robust cybersecurity defenses and mitigating the risk of cyber-attacks. This includes measures such as regular software updates, network segmentation, access control, and incident response planning. Additionally, fostering a culture of cybersecurity awareness among employees through training and education helps create a strong human firewall against social engineering attacks.

III. SYSTEM ARCHITECTURE

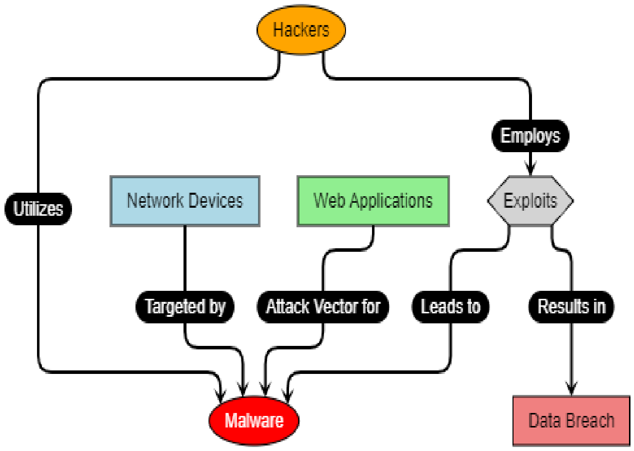
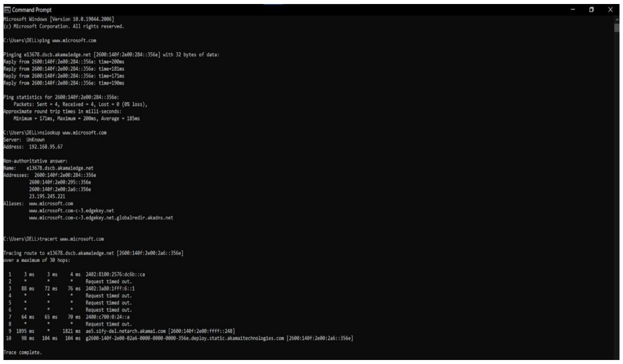


Fig. 1 Architecture

The system architecture for the cybersecurity exploration platform is designed to provide a scalable, reliable, and secure environment for students to learn and practice cybersecurity concepts.The architecture comprises multiple layers, each responsible for specific functionalities and interactions within the system.

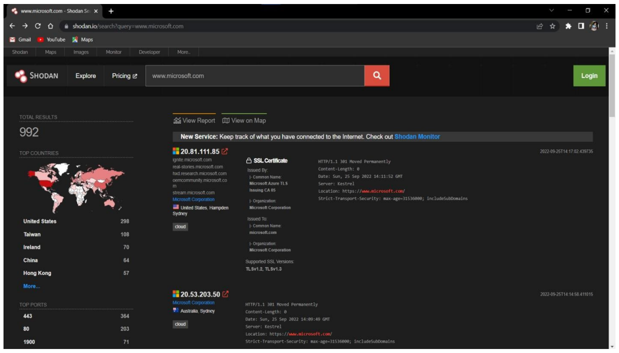
IV. Results

Foot printing on Microsoft Website: Foot printing means gathering information about a target system that can be used to execute a successful cyber-attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system. There are two types of foot printing as following below.



```
Command Prompt
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping www.microsoft.com

Pinging e13678.dscb.akamaiedge.net [2600:140f:2e00:284::356e] with 32 bytes of data:
Reply from 2600:140f:2e00:284::356e: time=200ms
Reply from 2600:140f:2e00:284::356e: time=181ms
Reply from 2600:140f:2e00:284::356e: time=171ms
Reply from 2600:140f:2e00:284::356e: time=190ms

Ping statistics for 2600:140f:2e00:284::356e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 171ms, Maximum = 200ms, Average = 185ms

C:\Users\DELL>nslookup www.microsoft.com
Server:  UnKnown
Address:  192.168.95.67

Non-authoritative answer:
Name:    e13678.dscb.akamaiedge.net
Addresses:  2600:140f:2e00:284::356e
          2600:140f:2e00:295::356e
          2600:140f:2e00:2a6::356e
          23.195.245.221
Aliases:  www.microsoft.com
          www.microsoft.com-c-3.edgekey.net
          www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net


C:\Users\DELL>tracert www.microsoft.com

Tracing route to e13678.dscb.akamaiedge.net [2600:140f:2e00:2a6::356e]
over a maximum of 30 hops:

  1     3 ms     3 ms     4 ms  2402:8100:2576:dc6b::ca
  2     *        *        *     Request timed out.
  3    88 ms    72 ms    76 ms  2402:3a80:1fff:6::1
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    64 ms    65 ms    70 ms  2400:c700:0:24::a
  8     *        *        *     Request timed out.
  9  1895 ms     *     1821 ms  ae5.sify-del.netarch.akamai.com [2600:140f:2e00:ffff::248]
 10    98 ms   104 ms   104 ms  g2600-140f-2e00-02a6-0000-0000-0000-356e.deploy.static.akamaitechnologies.com [2600:140f:2e00:2a6::356e]

Trace complete.
```

Fig. 2 Two types of foot printing



TOTAL RESULTS
992

TOP COUNTRIES

United States	298
Taiwan	108
Ireland	70
China	64
Hong Kong	57
More...	

TOP PORTS

443	364
80	203
1900	71

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

20.81.111.85 2022-09-25T14:17:02.439735
ignite.microsoft.com
real-stories.microsoft.com
hxd.research.microsoft.com
oemcommunity.microsoft.com
stream.microsoft.com
Microsoft Corporation
United States, Hampden Sydney

SSL Certificate
Issued By:
|- Common Name: Microsoft Azure TLS Issuing CA 05
|- Organization: Microsoft Corporation
Issued To:
|- Common Name: microsoft.com
|- Organization: Microsoft Corporation
Supported SSL Versions: TLSv1.2, TLSv1.3

```
HTTP/1.1 301 Moved Permanently
Content-Length: 0
Date: Sun, 25 Sep 2022 14:11:52 GMT
Server: Kestrel
Location: https://www.microsoft.com/
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

20.53.203.50 2022-09-25T14:14:58.411015
Microsoft Corporation
Australia, Sydney

```
HTTP/1.1 301 Moved Permanently
Content-Length: 0
Date: Sun, 25 Sep 2022 14:09:49 GMT
Server: Kestrel
Location: https://www.microsoft.com/
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

Fig. 3 Whois website

Information from netcraft website: Using netcraft website we get some more extra information when compared to whois website. The information is below.

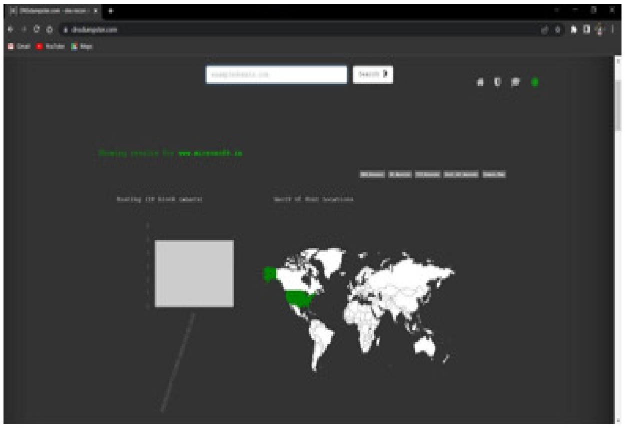
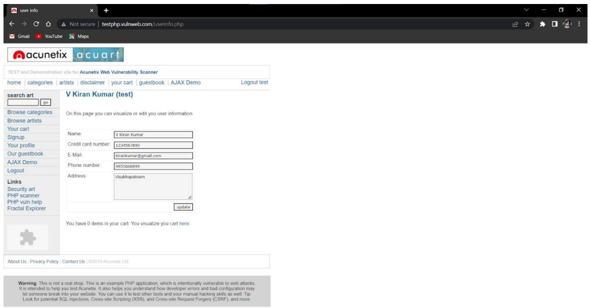


Fig. 4 Information using DNS dumpster website



user info
testphp.vulnweb.com/userinfo.php
Gmail
YouTube
Maps
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
update
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

V Kiran Kumar (test)

On this page you can visualize or edit you user information.

Name: V Kiran Kumar

Credit card number: 1234567890

E-Mail: kirankumar@gmail.com

Phone number: 9955668899

Address: Visakhapatnam

You have 0 items in your cart. You visualize you cart here.

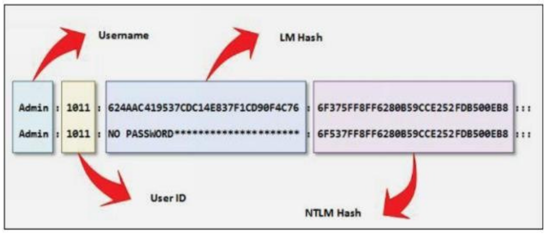
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Fig 5 SAM file

SAM File

- Security Accounts Manager (SAM) Database Security Account Manager SAM could be a database that stores credentials and other account parameters like passwords for the authentication process in a every Windows OS. Within Microsoft platform, SAM database contains passwords during a hashed form and other account information. Microsoft Windows save password in LM/ NTLM hashing format.

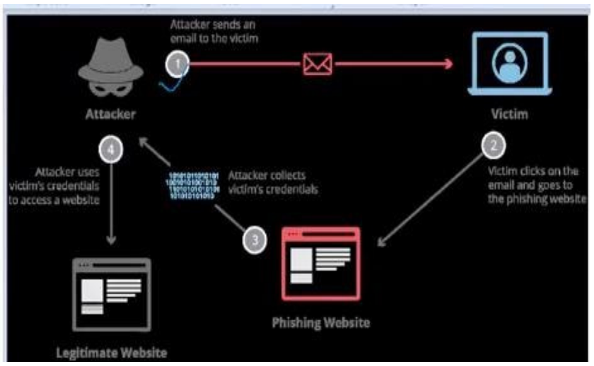
Fig.6 SAM database



```
Admin : 1011 : 624AAC419537CDC14E837F1CD90F4C76 : 6F375FF8FF6280B59CCE252FDB500EB8 :::
Admin : 1011 : NO PASSWORD********************* : 6F537FF8FF6280B59CCE252FDB500EB8 :::
```

PHISHING ATTACK:

Phishing may be a sort of social engineering attack often won't to steal user data including login credentials and master card numbers. It occurs when attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, the recipient is then tricked into clicking a maliciouslink.



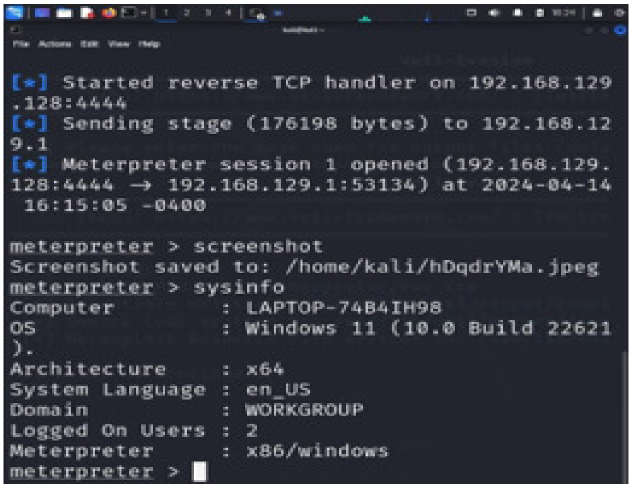
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
4
Attacker uses victim's credentials to access a website
Phishing Website
Legitimate Website

Fig.7 Phising Attack

Cisco monitoring shows about 37% of all malicious file extensions were archive files, like .zip and .jar, and 14% of the total were PDF files [9].

HONEYPOT:

A honeypot is a security mechanism used in cybersecurity to detect, deflect, or counteract attempts at unauthorized use of information systems. Essentially, it's a trap set up to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Imitation: A honeypot system imitates vulnerable or valuable resources, such as servers, networks, or services, to lure attackers into interacting with it.



```
[*] Started reverse TCP handler on 192.168.129
.128:4444
[*] Sending stage (176198 bytes) to 192.168.12
9.1
[*] Meterpreter session 1 opened (192.168.129.
128:4444 → 192.168.129.1:53134) at 2024-04-14
 16:15:05 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/hDqdrYMa.jpeg
meterpreter > sysinfo
Computer        : LAPTOP-74B4IH98
OS              : Windows 11 (10.0 Build 22621
).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

Fig.8 Honeypot

DoS and DDoS Attack:

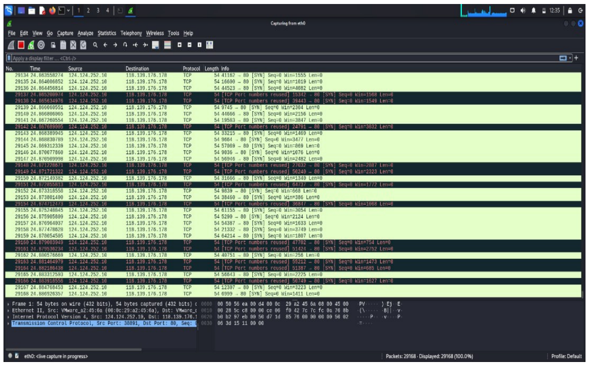


Fig.9 Dos and DDos attack

V. GRAPH ANALYSIS

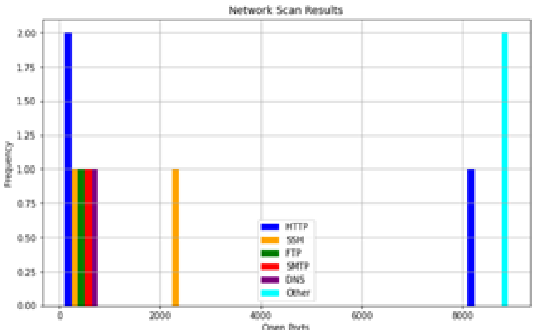


Fig.10 Phishing attack techniques distribution

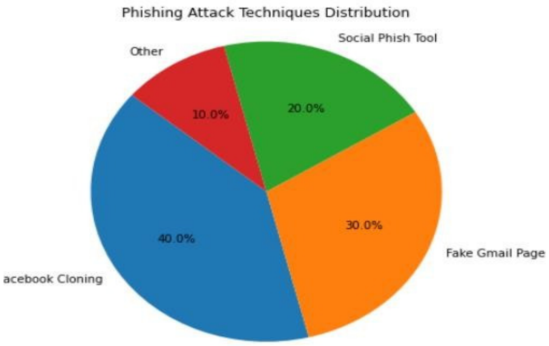


Fig.11 Distribution of vulnerabilities identified

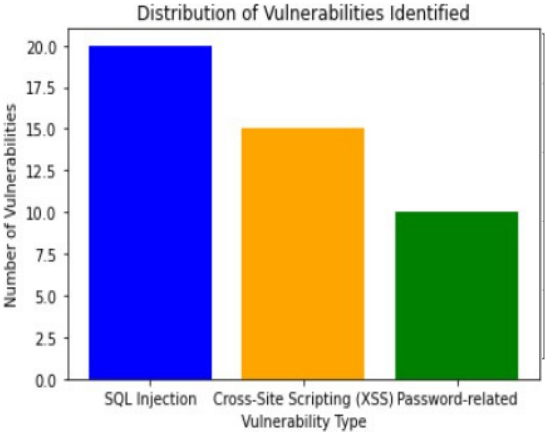


Fig.12 Malware analysis findings comparison

VI. Conclusion

In conclusion, the paper "Cybersecurity Exploration: From Foot printing to Threat Mitigation" offers a comprehensive journey through various aspects of cybersecurity, equipping students with valuable skills and knowledge to protect and defend computer systems and networks against a wide range of threats and attacks. Throughout the paper, participants engage in hands-on activities and exercises that cover fundamental reconnaissance techniques, paper such as foot printing and scanning, to advanced attack methodologies like SQL injection, phishing, and malware analysis. By utilizing a combination of industry-standard tools and frameworks, students gain practical experience in identifying vulnerabilities, exploiting weaknesses, and understanding attacker methodologies. The paper emphasizes the importance of robust security measures, such as implementing strong password policies, conducting regular vulnerability assessments, and deploying intrusion detection systems. Additionally, it underscores the significance of proactive defense strategies, including setting up honeypots to detect insider threats and deploying countermeasures against denial-of- service attacks. By exploring real-world scenarios and simulating cyber-attacks, students develop critical thinking skills and learn to diagnose and investigate cybersecurity events effectively. Furthermore, the paper promotes professional communication skills, fostering collaboration within teams to address information security issues and devise comprehensive defense strategies. In summary, "Cybersecurity Exploration: From Foot printing to Threat Mitigation" provides a dynamic and interactive learning experience, empowering students to become proficient cybersecurity practitioners capable of safeguarding digital assets and mitigating emerging threats in an increasingly complex threat landscape.

Fig.12 Network scan results

VII. Acknowledgment

- Future Scope: The paper "Cybersecurity Exploration: From Foot printing to Threat Mitigation" lays a strong foundation for future advancements and enhancements in the field of cybersecurity education. Integration of Advanced Attack Techniques: Incorporate more advanced attack techniques and methodologies, such as zero-day exploits, advanced persistent threats (APTs), and fileless malware attacks. This will provide students with exposure to cutting-edge cybersecurity threats and enhance their skills in detecting and mitigating sophisticatedattacks.

VIII. References

[1] Roumen Trifonov, Georgi Tsochev, Slavcho Manolov, Radoslav Yoshinov and Galya Pavlova, 2017. "A survey of artificial intelligence for enhancing the information security", International Journal of Development Research, 7, (11), 16866-16872.

[2] Roumen Trifonov, Slavcho Manolov, Radoslav Yoshinov, Georgi Tsochev, Galya Pavlova. (2017) Artificial Intelligence Methods for Cyber Threats Intelligence.
International Journal of Computers, 2, 129-135

[3] ENISA Threat Landscape Report 2018 [online]. Available: https://www.enisa.europa.eu/publications/enisa-threat- landscape-report-2018 [Accessed February 20 2020]

[4] 2019 Webroot Threat Report [online]. Available:https://wv

[5] Annual Report and Accounts 2018-19 - National CrimeAgency [online]. Available: https://nationalcrimeagency.gov.uk/who-we-are/publications/329-nca-annual-report-accounts-2018-19/file [Accessed April 25 2020]

[6] 2019 Cyberthreat Defense Report - Imperva [online]. Available: https://www.imperva.com/resources/reports/CyberEdge- 2019-CDR-Report-v1.1.pdf [Accessed April 25 2020]

[7] Symantec Internet Threat Report 2019 [online]. Available: https://docs.broadcom.com/doc/istr-24-2019-en[Accessed April 28 2020]

[8] Microsoft Security Intelligence Report 2019 [online]. Available: https://www.microsoft.com/security/blog/2019/02/28/micros oft-security-intelligence-report-volume-24-is-now-available/[Accessed April 28 2020]

[9] Cisco Cybersecurity Series 2019. Threat Report [Online] Available: https://www.cisco.com/c/dam/en/us/products/collateral/secu rity/2019-threats-of-the-year-cybersecurity-series-dec- 2019.pdf [Accessed February 15 2020]

[10] Oracle And Kpmg Cloud Threat Report 2019 [online]. Available: https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf [AccessedFebruary 5 2020]

[11] ENISA Threat Landscape Report 2017 [online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-

landscape-report-2017 [Accessed February 17 2020]

[12] ENISA Threat Landscape Report 2016 [online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 [Accessed February 17 2020]

[13] ENISA Threat Landscape Report 2015 [online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2015 [Accessed February 17 2020]

[14] ENISA Threat Landscape Report 2014 [online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2014 [Accessed February 17 2020]

[15] Valentin Hristov, Ivan Stankov, Kiril Slavkov, Investigation of 5G Mobile Networks, CAx Technologies Journal, issue 7, December 2019, ISSN 1314-9628

[16] Kaspersky Security Bulletin: Threat Predictions For 2019.

[17] The criminal cyberservices market 2018, Positive Technologies.

[18] Global Threat Intelligence Report, NTT Security, 2018.

[19] „State of the Internet - Security: Web Attacks “, Akamai, summer 2018.

[20] NETSCOUT Arbor's 14th Annual Worldwide Infrastructure Security Report, 2019. https://www.netscout.com/report/, accessed March 2019.

[21] Report. Kaspersky Security Bulletin 2018. Story of the year:miners.

[22] Discontinuation of Coinhive, https://coinhive.com/blog/en/discontinuation-of-coinhive, accessed March 2019.

[23] Public hacker test on Swiss Post's e-voting system, 07.02.2019, accessed March 2019. https://www.evoting-blog.ch/en/pages/2019/public-hacker-test-on-swiss-post-s-e-voting-system

[24] Nourhene Ellouze, et al. "Powerless security for Cardiac Implantable Medical Devices: Use of Wireless Identification and Sensing Platform, Journal of Network and Computer Applications", Volume 107, 2018, Pages 1-21, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.01.009.

[25] ForgotDoor: Routers in Singapore accidentally give complete access to potential IoT attackers, NewSky Security, 28 May 2018.

[26] McAfee Labs Threats Report, September 2018.

[27] Tracking the People Behind Botnets: A List of Top 20 IoT Blackhat Hackers, NewSky Security, 30 October 2018.

[28] State of the Internet - Security: Credential Stuffing Attacks,
Akamai, volume 4, issue 4, 2018

[29] IBM X-Force Threat Intelligence Index 2019, p. 12.

[30] AV-TEST Institute, Statistics, https://www.av-test.org/en/statistics/malware/, accessed March 2019.

[31] APT Report - Operation ShadowHammer, SecureList, March2019.

[32] Cyber Threatscape Report 2018, Accenture Security.

[33] Internet Security Threat Report, volume 23, Symantec, 2018.