# Cybersecurity Operation and Digital Forensics Implementation Project

**Supervised by**

**Dr. Rubaiyat Islam**

Associate Professor

Department of Software Engineering, Daffodil International University

**Submitted By:**

**Md. Badiujjaman Badhon**
ID: 221-35-1041

Department of Software Engineering, Daffodil International University

## APPROVAL

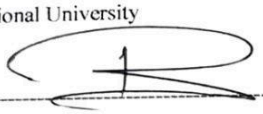
This Industry based Project titled on "**Cybersecurity Operation and Digital Forensics Implementation Project**", submitted by **Md. Badiujjaman Badhon (ID: 221-35-1041)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

## BOARD OF EXAMINERS

---

**Chairman**

**Dr. A. H. M. Saifullah Sadi**
**Professor**
Department of Software Engineering
Faculty of Science and Information Technology Daffodil International University



---

**Internal Examiner 1**

**Dr. Rubaiyat Islam**
**Associate Professor**
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

---

**Internal Examiner 2**

**Dr. Md. Abdul Kader**
**Associate Professor**
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

---

**Internal Examiner 3**

**Nuruzzaman Faruqui**
**Assistant Professor**
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

---

**External Examiner**

**Md. Mostafiz Khan**
**Managing Director**
Tecognize Solutions Limited

# DECLEARATION

I completed this internship and wrote this report under the sole guidance of **Dr. Rubaiyat Islam**, Associate Professor, Department of Software Engineering, Faculty of Science and Information Technology, Daffodil International University. I confirm that I have not previously submitted this internship experience or any part of this report for academic credit, award, or evaluation at any other institution or for any other purpose.

Badiujjaman

**Md. Badiujjaman Badhon**

ID: 221-35-1041

Department of Software Engineering,

Daffodil International University

**Certified by**

**Dr. Rubaiyat Islam**

**Associate Professor**

Department of Software Engineering,
Faculty of Science and Information Technology,
Daffodil International University

## GLOSSARY OF TERMS

**APT (Advanced Persistent Threat)** - A sophisticated, continuous cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period.

**CVSS (Common Vulnerability Scoring System)** - A framework for rating the severity of security vulnerabilities in software.

**DFIR (Digital Forensics and Incident Response)** - The field involving the investigation of cyber incidents and recovery from security breaches.

**EDR (Endpoint Detection and Response)** - A cybersecurity solution that continuously monitors end-user devices to detect and respond to cyber threats.

**IDS/IPS (Intrusion Detection System/Intrusion Prevention System)** - Security technologies that monitor network traffic for malicious activity.

**MFA (Multi-Factor Authentication)** - A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.

**NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)** - A framework for improving critical infrastructure cybersecurity.

**OWASP (Open Web Application Security Project)** - A nonprofit foundation that works to improve the security of software.

**PSK (Pre-Shared Key)** - A shared secret that was previously shared between the two parties using some secure channel before it needs to be used.

**SIEM (Security Information and Event Management)** - Solutions that provide real-time analysis of security alerts generated by applications and network hardware.

**SOC (Security Operations Centre)** - A centralised unit that deals with security issues on an organisational and technical level.

**VAPT (Vulnerability Assessment and Penetration Testing)** - A Security testing service used to identify and address cybersecurity vulnerabilities.

**WAF (Web Application Firewall)** - A firewall that monitors, filters, and blocks HTTP traffic to and from a web application.

**WPA/WPA2 (Wi-Fi Protected Access)** - Security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

**XSS (Cross-Site Scripting)** - A security vulnerability typically found in web applications that enables attackers to inject client-side scripts into web pages viewed by other users.

## LIST OF ABBREVIATIONS

**API** - Application Programming Interface
**ARP** - Address Resolution Protocol
**BSSID** - Basic Service Set Identifier
**CVE** - Common Vulnerabilities and Exposures
**DMZ** - Demilitarised Zone
**DoS** - Denial of Service
**GDPR** - General Data Protection Regulation
**HTTP** - Hypertext Transfer Protocol
**HTTPS** - Hypertext Transfer Protocol Secure
**ICMP** - Internet Control Message Protocol
**ICT** - Information and Communication Technology
**IDOR** - Insecure Direct Object Reference
**IoT** - Internet of Things
**IP** - Internet Protocol
**IT** - Information Technology
**KRI** - Key Risk Indicator
**MAC** - Media Access Control
**OS** - Operating System
**PMK** - Pairwise Master Key
**RDP** - Remote Desktop Protocol
**SDLC** - Software Development Life Cycle
**SLA** - Service Level Agreement
**SMTP** - Simple Mail Transfer Protocol
**SQL** - Structured Query Language
**SQLi** - SQL Injection
**SSH** - Secure Shell
**SSID** - Service Set Identifier
**TCP** - Transmission Control Protocol
**UDP** - User Datagram Protocol
**USB** - Universal Serial Bus
**VNC** - Virtual Network Computing
**VPN** - Virtual Private Network
**WEP** - Wired Equivalent Privacy
**WIDS** - Wireless Intrusion Detection System
**WPA3** - Wi-Fi Protected Access 3

This concludes the comprehensive internship report on my transformative journey through cybersecurity domains at Backdoor Private Limited. The experience has equipped me with both the technical expertise and professional mindset to contribute meaningfully to the field of cybersecurity.

# ACKNOWLEDGEMENTS

Acknowledgements, I wish to extend my greatest thanks to everyone who has helped me during the period of this internship and in writing this report.

To begin with, I am grateful to the authorities of **Backdoor Pvt.Ltd** for giving me this immense opportunity to gain real-world professional experience in cybersecurity. Having confidence in me to do real-world security has been so crucial in my journey as a security professional.

I owe a special thanks to my mentors at **Backdoor Private Limited – Ms Tahsina Sadia Meem** and **Mr Shuvo Sarkar**. Your inspiration, patience, guidance and knowledge are overwhelming. You have not just trained me technically, but developed in me the work ethic and attitude for this domain.

I am indebted to **Daffodil International University** and my academic supervisors for their valuable support and cooperation during my period of study and the internship. It also allowed me to take full advantage of this practical experience given by the theoretical background provided by the university.

I would also like to thank the whole team of **Backdoor Pvt Ltd** for creating a very helpful and learning environment. The professionalism and camaraderie I've witnessed have set a very high standard for my future career.

Finally, I would like to thank my family and friends for their continual understanding, support and encouragement throughout this challenging learning process.

I am grateful for all those that have made this internship successful and impactful, as it has been a life-altering summer.

# EXECUTIVE SUMMARY

Beep Report on Technical Internship experience as a Technical Executive at **Backdoor Pvt. Ltd** (3 Months) This lengthy report describes the professional knowledge and technical skills I acquired through my three-month internship as a Technical Executive in Backdoor Private Limited which is a leading cybersecurity company in Bangladesh. Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, Security OperationsCentrer (SOC) monitoring, etc. were some very sensitive domains of Cybersecurity that I got exposed to during the internship from **16th October 2025 to 16th December 2025**. The report systematically details operational experience with the most common cybersecurity tools and techniques. The report summarises hands-on experience with cybersecurity tools and methodologies that are commonly used in industry. Some of the technical aspects covered include network discovery using Nmap and Zenmap, vulnerability scanning with Nessus and OpenVAS, digital forensics with Oxygen Forensic, Autopsy and FTK Imager, security testing using GoPhish and Hydra frameworks. Conducting comprehensive security assessments, forensic data recovery, simulating targeted phishing and assisting with organisational vulnerability management were all significant professional achievements. The internship helped to cultivate important professional skills such as writing technical documents, working in teams to find solution andpractisingg ethical security. While there were operational limitations surrounding the testing of offensive exploitation, this experience imparted significant practical understanding of defensive capabilities and proactive risk reduction actions. This internship effectively connected the dots between theoretical academic learning and real-world demand, providing a sound technical basis to work in cybersecurity while offering a real-world context of present-day security issues. Critical success factors can now be readily defined and realised through the identification, closure and remediation of key vulnerabilities in client infrastructures; effective forensic investigations for incident response requirements; and tangible enhancements to security awareness within the organisation by running simulated phishing campaigns.

## *Table of Contents:*

# CHAPTER 1
# INTRODUCTION

## 1.1 Internship Overview

My internship at Backdoor Private Limited was a major milestone in my academic and professional journey. It gave me a real-world environment to apply my cybersecurity knowledge and see how things work in practice. As a Technical Executive Intern, I gained hands-on experience in security operations, especially in VAPT, Digital Forensics, and SOC monitoring.

This real-world experience helped me improve my ability to analyze and respond to digital threats. Working with the security team was rewarding, as I took part in activities like security posture assessments, breach reviews, and helping implement security protocols.

Furthermore, the experience also included some widely-adopted industry tools and adherence to established security best practice, all of which should be skills in a proficient working in today's threat environment."

## 1.2 Objectives and Purpose

The objective of the internship was to establish a link between the theoretical knowledge and practical challenges, within the context of Cyber defense through deep immersion in current sectoral trends and day-to-day work practices. They carefully designed the program with specific goals such as:

- Developing high-level tools, hardware, and procedure skills.
- Learn more about corporate security assessment processes and compliance requirements.
- Learning practical application in how to collect, preserve and analyse digital evidence.
- Enhance the capacity to generate well-crafted reports and official documents from cyber security reviews and findings.
- Enhancing the collaborative skills and collective analysis capabilities in a live cyber-defence scenario.
- Good understanding of ethical and legal rules of "engagement" for cyber-defence missions.
- Growing industry connections and exposure to the wider cyber-defence market.

Ultimately, this program was planned to serve as a means for me to be able to convert academic knowledge into more practical skills that could prepare me with the essential occupational expertise and professional judgement needed when entering into an entry-level position within the field of cybersecurity.

## 1.3 Organisational Context

Backdoor Private Limited is a premier cyber defence and technology solutions firm in Bangladesh offering holistic digital protection services to public sector, financial institutions, and corporate houses. The aim of the company had been to bring in a robust digital ecosystem in the country and turned out to be a reliable partner for businesses that traversed across a number of industries.

As the authorised partner of world-leading cyber defence companies, Backdoor Private Limited, delivers technological advanced solutions and local expertise to ensure the clients are protected from more sophisticated cyber attacks. Its team of certified cyber defense experts is dedicated to monitoring threats and ensuring that its customers remain in compliance with regulations and are adhering to best practices when it comes to strengthening their most important critical infrastructures. Furthermore, the company has a whole department focusing on innovation and development always monitoring what's new regarding threats to adapt accordingly to keep its protective technologies efficient and updated.

## 1.4 Professional Benefits

The Internship The internship was a eclectic and fertile ground of experience which resulted in my upgrading substantially on the occupational and technological fronts in several directions:

**Technical Skill Enhancement:**

- Gained practical, in the hand, experience with professional LAN cyber defense tools and systems.
- Acquired knowledge in the application of practical tools for vulnerability analysis and risk management.
- Learned about procedures and standards in digital investigations.
- Contributed to the success of cyber surveillance and incident response efforts.
- Learned statutory and corporate compliance.

**Professional Skill Enhancement**

- Enhanced capability to produce comprehensive technical reports for security audits and investigations.
- Enhanced articulation of vocational content and learned co-operation skills in group situation.
- GAINED experience with the flows of operations in Corporate Security, best practices and standard functions.
- Involved in client interaction, gained experience of requirement clarification in a professional environment.
- Acquired project management and time management competencies with tasks completed in a timely and effectual manner.

**Career Advancement Opportunities**

- Established industry relationships in the cybersecurity sector; further expanded my base of specialists and advisers.
- Learned about possible career paths in cyber defense from a niche perspective.
- Honed my career profile by documenting work experience and hard achievements.
- "I moved my career by learning the same level of practical skills, necessary for sector demands and relevant.
- Familiarised himself with the corresponding accreditations and strategic career moves within the profession.

## 1.5 Learning Objectives

The internship was based on explicit and measurable educational objectives, consequently, it was both a hands-on program, as well as a career-development one.

**Primary Objectives**

The main objective for this report is to learn how to use the fundamental instruments and operational concepts used in a cyber defense assessment. Get intimate with the Vuln Management cycle. Learn to generate, collect and analyze digital evidence. With it, become fluent in writing polished security assessment reports. Know the ethics and legalities related to security assessments.

**Secondary Objectives**

I. To gain effective communications to communicate with specialists and executives.
II. To learn about corporate architectures and operational interactions in the cyber defense organization.
III. "Try to make the most of your opportunities, within whatever legal or moral screen you are operating."
IV. To strengthen temporal arranging, assignment coordinating and initiative planning.
V. Build professional connections and networking with the cybersecurity community at largeStrengthen communicative skills to communicate successfully with technical staff as well as corporate leadership.

## 1.6 Program Schedule and Duration

The intern rotation occurred from **September 16, 2025 to December 16, 2025**. It adhered to a very disciplined institutional architecture that was optimize for the learning and experience soak.

- **Total Program Length:** 12 weeks (3 months)
- **Weekly Time Table:** Sunday - Thursday, from 10:00 to 18:00.
- **Total Time on the Job:** Over 480 hours of hands-on work.

**Step-by-Step Training Stages:**

1. **Introduction and Tool Familiarisation (Weeks 1–2):** Becoming acquainted with company policies, cybersecurity applications, and operational procedures.
2. **Supervised Practice (Week 3–6):** Application of the theory in real professional cases.
3. **PROJECT DEMONSTRATION (Weeks 7–10):** The cyber security projects are to be delivered using the necessary problem solving and decision making as specified.
4. **Documentation and Reporting (Weeks 11 -12):** Composing technical reports with an accompanying professional documentation of internship activities.

This well-considered approach aimed to progress from the most basic supporting input to unsupervised task performance, balancing guidance and independent application.

# CHAPTER 2

# ORGANIZATIONAL PROFILE

## 2.1 Company Overview

Backdoor Private Ltd is one of the leading companies in Bangladesh focusing on cyber security where we offer a plethora of services. With the expertise of a team of cybersecurity professionals are certified who have diverse experience in work fields such as network security, digital forensics, vulnerability management and security awareness programme. As a result of the firm's alliance with global technology and software organisations, they have access to the tools and 'Threat intelligence' which allows them to deliver high level security solutions. The organization is structurally divided into 5 groups as above, such as the vulnerability assessment team, digital forensics team, security operations and R&D(team). This means that the company maintains deep technical expertise in each and have holistic service delivery. Backdoor Private Limited is strongly committed to the ongoing professional development of its employees, and is prepared to invest heavily in training and qualifications for its personnel so that our team remains current with new threats and their related latest technology.

## 2.2 Strategic Vision

*"To be a known leader in digital security and to make sure that Backdoor becomes a recognized brand achieving customer requirements with accuracy, and confidentiality & transparency."*

This vision underscores the company's dedication to excellence, trust and client-centric focus, thus setting a clear path towards growth of the organisation and continued deliverance of quality cybersecurity services.

## 2.3 Mission Statement

*"To offer market leading information security consultancy and customer solutions, improving organisational digital security profile – empowering clients with understanding and awareness of the threat landscape as it evolves."*

The mission reflects the company's commitment to both providing technical excellence and promoting client education, which Gliederer says is a big part of human factors in continuing to keep organisations secure.

## 2.4 Service Portfolio

Backdoor Private Limited offers a full range of cybersecurity services developed to meet the various protection needs of today's companies.

**Security Assessment Services:**

Yes We audit to prevent an attack. Our ability to provide assessments that go deeper than any in the industry identify your vulnerabilities before you are attacked.

- Vulnerability assessment and penetration testing (VAPT)
- Security Testing and Verification of Web Apps
- Network Infrastructure Security Evaluation
- Mobile Application Security Assessment
- Cloud Security Configuration Review
- IoT Testing and Security

**Digital Forensic Services:**

- Seizure and examination of digital evidence
- Incident response and investigation management
- Mobile device forensic examinations
- Support for cybercrime investigations
- Data recovery and correlation analysis
- Drafting of advocate's reports and pleadings

**Managed Security Services:**

- Control and control by the SOC
- Threat intelligence collection and analysis
- Security incident handling and response
- Compliance monitoring and regulatory reporting
- 24/7 security monitoring operations
- Proactive threat hunting and mitigation

**Security Awareness Services:**

- Phishing tests and employee training plan
- Development and Enactment of Training information on security policies is followed.
- Employee security awareness initiatives
- Social engineering testing and assessment
- Assessment and facilitation of an organisational security culture
- Custom designed and delivered cyber security training formats

**2.5 Client Ecosystem**

Backdoor Private Limited extends our know-how to a wide spectrum of companies business types; from the most crucial sectors. These range from government bodies and banks to big businesses and infrastructure suppliers. Through careful customization of these offering to each individual customer, the company ensures strong protection & further strengthens the overall digital resilience across all Forthnet client base.

**Financial Services Sector:**

- Modhumoti Bank Limited
- Several other commercial banks and financial institutions
- Insurance and assurance providers
- Microfinance organisations and cooperatives

**Government Entities:**

- Bangladesh Police – Anti-Terrorism Unit
- Police Bureau of Investigation (PBI)
- Rapid Action Battalion (RAB)
- ICT Division, Government of Bangladesh
- Various ministries and government departments

**Corporate Organisations:**

- Spectra Engineering Limited
- Bangladesh Shipping Corporation Limited (BSCL)
- BD Link Communication
- Multiple companies and critical infrastructure you
- Educational institutions and academic organisations
- Healthcare providers and medical institutions

This diverse client base demonstrates the expertise of Backdoor Private Limited in providing customised security solutions for different sectors and solidifies its status as a reliable and complete security solution provider.

# CHAPTER 3
# INTERNSHIP LEARNING

## 3.1 Internship Learning Outcome:

At Backdoor Private Limited, I was a Technical Executive intern and gained hands-on experience in cybersecurity and IT service operations. This was a pivotal experience that greatly assisted me in the quest to come down from the ivory tower and apply my academic theoretical knowledge in industry settings.

I further developed my skills on various Critical Cybersecurity tools such as Nmap, Oxygen Forensic, Autopsy, FTK Imager, Nessus, OpenVAS and Zenmap. Proficiently leveraged these instruments for a variety of tasks including network reconnaissance, digital forensics analysis, and full-scope vulnerability assessments. Using these apps, I really felt my understanding increased over host identification, port analysis and data extraction - to advanced threat ID.

This internship not only enhanced my technical skill set significantly, it honed my team work, communication and critical problem-solving skills in a live IT environment. I was involved in key activities such as system maintenance, defect fixes and real-time security projects under supervision of the seniors. Working hand in hand with industry professionals and making real contributions which mattered to projects did not just Improve my ability for effectively applying IT concepts but also developed my strategic thinking abilities of SWOT analysis. This holistic exposure has molded me to be confident in operating and flourishing in the rough tides of cybersecurity.

## 3.2 Learning to Internship:

### 3.2.1 Nmap Tools:

Nmap is a very powerful, flexible and well known open source tool for network exploration, security scanning and vulnerability auditing. Developed by Gordon Lyon, better known as Fyodor, the tool enables knowledgeable security professionals, digital security experts and network administrators to map out an entire network and find security holes.

It works by sending tailored data packets to specific machines that are then very carefully interpreted in the replies. This intelligent methodology brings critical information to users, such as live devices in an infrastructure, available communication channels and their hosting service specifics and platform details.

The utility supports several inspection states such as TCP SYN, TCP Connect, and UDP scans. It also provides advanced features such as OS and service fingerprinting and NSE (Nmap Scripting Engine) script scanning.

Nmap is really a wonder tool for so many purposes: even in simulated cyber attacks, for inventory management, perimeter defense readouts- the list goes on and on just like. It provides the detail you need to see what's really going on, from detailed information about each packet to entirely customizable reports that help you make sense of your network vulnerabilities.

**Installation (Debian / Ubuntu)**

To install Nmap on a Debian or Ubuntu system:

sudo apt update
sudo apt install -y nmap
After installation, Nmap can be executed directly from the terminal.
**Nmap Tools Using Real Life:**
**3.2.1.1 Host Discovery**

Host Discovery is first step of network reconnaissance. Its main purpose is to determine what devices or systems are active and/or available on a network. Although Nmap has many efficient ways of performing this important task. That capability, meanwhile, enables cybersecurity professionals to effectively determine which targets should receive more thorough scanning and full vulnerability assessments.

**Command / Option:** -sL
**Full Command:** nmap -sL 192.168.68.0/24
**Description:** Lists all potential targets without sending packets. Useful for verifying scope.

**Screenshot:**

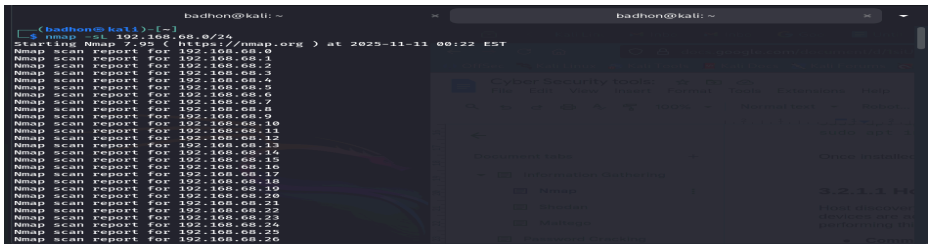



***Figure 1:*** **Lists all potential targets without sending packets**

**My Work:** Listed all IP addresses in the local subnet without scanning.

**Command / Option:** -sn
**Full Command:** nmap -sn 192.168.68.0/24
**Description:** Performs a ping scan to identify which hosts are online.

**Screenshot:**

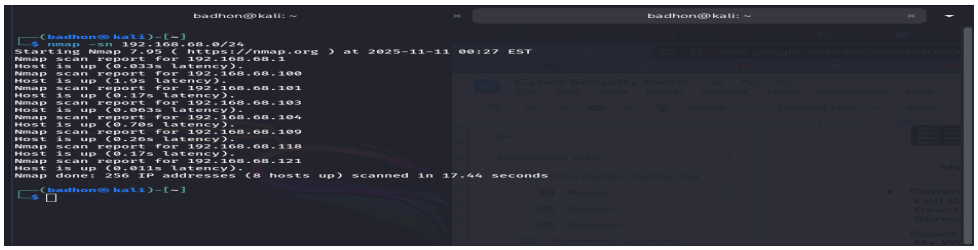



***Figure 2:*Performs a ping scan to identify which hosts are online**

**My Work:** Found all active devices on the company's internal network.

**Command / Option:** -Pn
**Full Command:** nmap -Pn 192.168.68.115
**Description:** Treats all hosts as online, bypassing ping checks.

**Screenshot:**

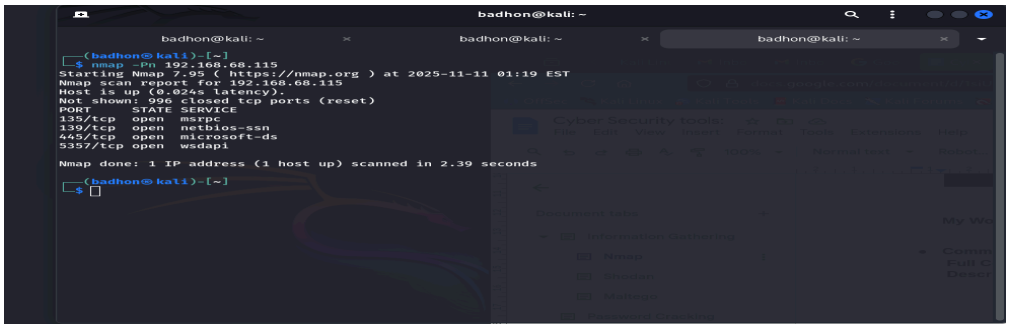



***Figure 3:* Treats all hosts as online, bypassing ping checks.**

**My Work:** Detected active host and identified open ports (135, 139, 445, 5357) even when ICMP ping requests were disabled.

**Command / Option:** -PS/PA/PU/PY
**Full Command:** nmap -PS80,443 192.168.68.0/24
**Description:** Uses TCP SYN, TCP ACK, UDP, or SCTP packets for host discovery.

**Screenshot:**

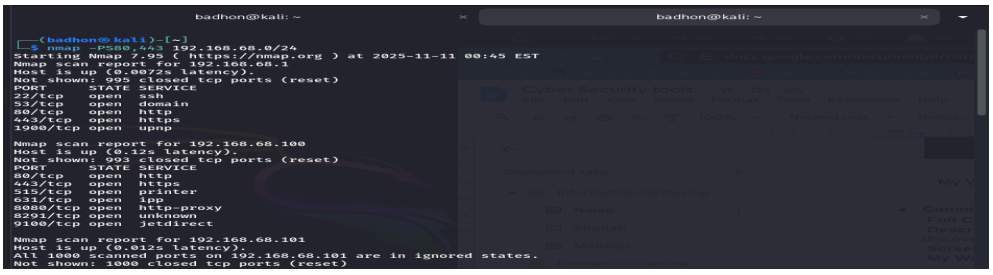



***Figure 4:* Uses TCP SYN, TCP ACK, UDP, or SCTP packets for host discovery**

**My Work:** Discovered 11 active hosts on the 192.168.68.0/24 subnet and identified multiple open web and network service ports (e.g., 22, 80, 443, 445, 9100), confirming responsive devices through SYN probes on ports 80 and 443.

**Command / Option:** -PE/PP/PM
**Full Command:** nmap -PE 192.168.68.0/24
**Description:** Uses ICMP Echo, Timestamp, or Netmask requests to find live hosts.

**Screenshot:**

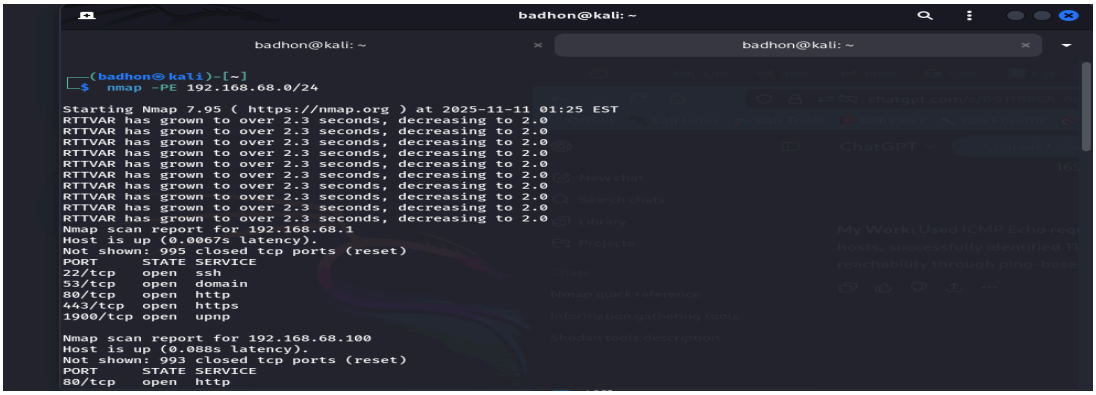



***Figure 5:*** **Uses ICMP Echo, Timestamp, or Netmask requests to find live hosts.**

**My Work:** Revealed devices that responded to ICMP echo requests across the subnet, confirming 11 active hosts and their open network services.

**Command / Option:** --traceroute
**Full Command:** nmap --traceroute 192.168.68.115
**Description:** Traces the path packets take to reach the host.

**Screenshot:**

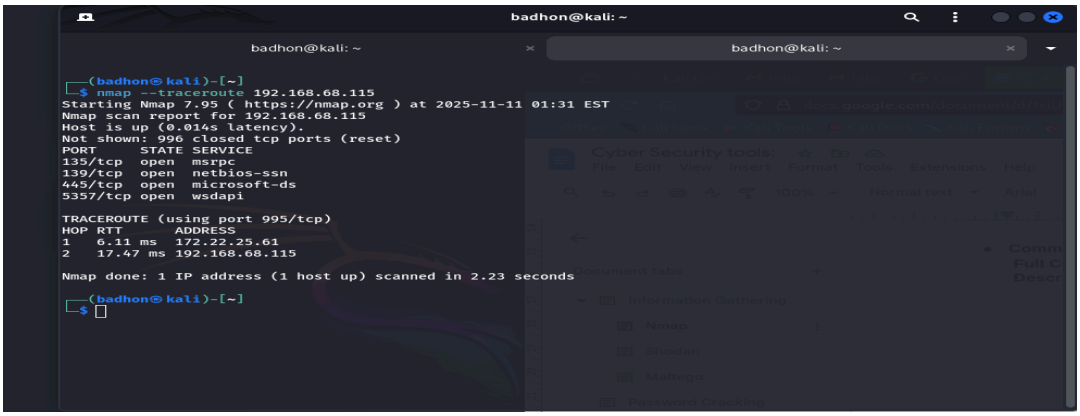



***Figure 6:*** **Traces the path packets take to reach the host.**

**My Work:** Traced the network path to the target host and identified two hops (gateway 172.22.25.61 → host 192.168.68.115) along with open ports 135, 139, 445, and 5357 on the destination system.

**Summary:**Host discovery efficiently identifies live devices and optimises subsequent scanning.

### 3.2.1.2 Scan Techniques

Scanning techniques are used to detect open ports, running services, and potential security risks. Each method differs in speed, stealth, and accuracy.

**Command / Option:** -sS
**Full Command:** nmap -sS -p 1-1000 192.168.68.115
**Description:** Performs a stealthy TCP SYN scan, sending SYN packets but not completing the connection.

**Screenshot:**

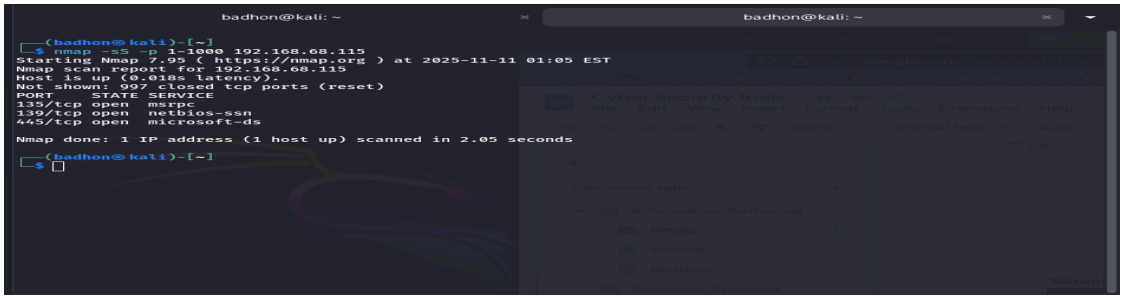



***Figure 7:*** **Performs a stealthy TCP SYN scan**

**My Work:** Performed a stealthy SYN scan on ports 1–1000 and detected open ports 135, 139, and 445, confirming active Windows network services on the target host.

**Command / Option:** -sT
**Full Command:** nmap -sT -p 1-1000 192.168.68.115
**Description:** Conducts a full TCP connect scan using system calls.

**Screenshot:**

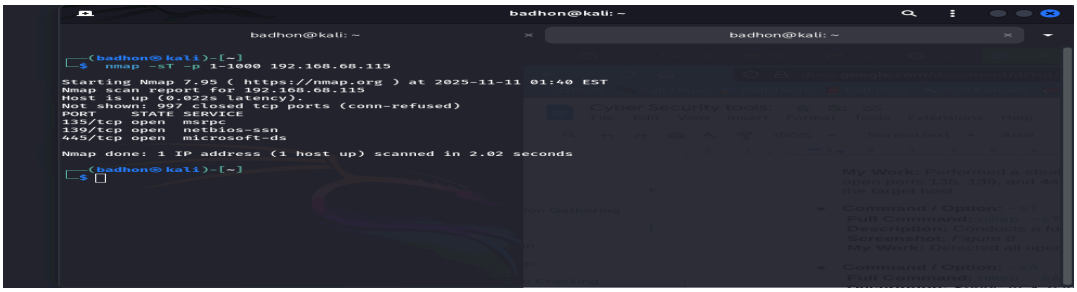



***Figure 8:*** **Conducts a full TCP connect scan using system calls**

**My Work:** Performed a TCP Connect scan (-sT) on ports 1–1000 and confirmed open ports 135, 139, 445, validating active Windows networking services on the target.

**Command / Option:** -sA
**Full Command:** nmap -sA -p 1-1000 192.168.68.115
**Description:** Sends ACK packets to determine if ports are filtered by a firewall.

**Screenshot:**


***Figure 9***

**My Work:** Conducted a TCP ACK scan (-sA) on ports 1–1000, which showed all ports as **unfiltered**, indicating no active firewall blocking and confirming direct accessibility to the host.

**Command / Option:** -sU
**Full Command:** nmap -sU -p 53,67,123 192.168.68.115
**Description:** Scans for open UDP ports used by services like DNS and NTP.

**Screenshot:**


***Figure 10:*Scans for open UDP ports used by services like DNS and NTP.**

**My Work:** UDP ports 53, 67, and 123 on 192.168.68.115 are closed.

**Summary:**Different scanning methods reveal various aspects of network exposure. Combining multiple scan types ensures a complete assessment.

### 3.2.1.3 Script Scanning

The **Nmap Scripting Engine (NSE)** automates advanced tasks such as vulnerability detection and service analysis.

**Command / Option:** -sC
**Full Command:** nmap -sC 192.168.68.115
**Description:** Runs Nmap's default safe scripts for general system information.

**Command / Option:** --script
**Full Command:** nmap --script=http-title,ftp-anon 192.168.68.115
**Description:** Executes specific Lua scripts for deeper analysis.

**Command / Option:** --script-help
**Full Command:** nmap --script-help=http-title
**Description:** Provides details about specific scripts.

**My Work:**I used NSE for vulnerability and information-gathering scans, identifying software versions, exposed services, and potential weaknesses.

### 3.2.1.4 Port Scanning

Port scanning identifies which services are available and running on target systems.

**Command / Option:** -p
**Full Command:** nmap -p 22,80 192.168.68.115
**Description:** Scans specific ports such as SSH and HTTP.

**Screenshot:**

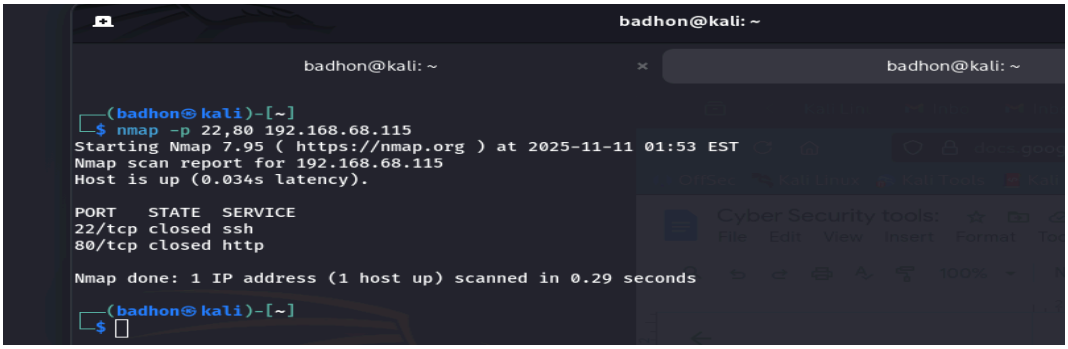



***Figure 11:*** **Scans specific ports such as SSH and HTTP.**

**My Work:** Scanned ports 22 and 80 — both found closed, indicating no active SSH or HTTP services on the host.

**Command / Option:** -p 1-65535
**Full Command:** nmap -p 1-65535 192.168.68.115
**Description:** Scans all 65,535 ports for a full security overview.

**Screenshot:**

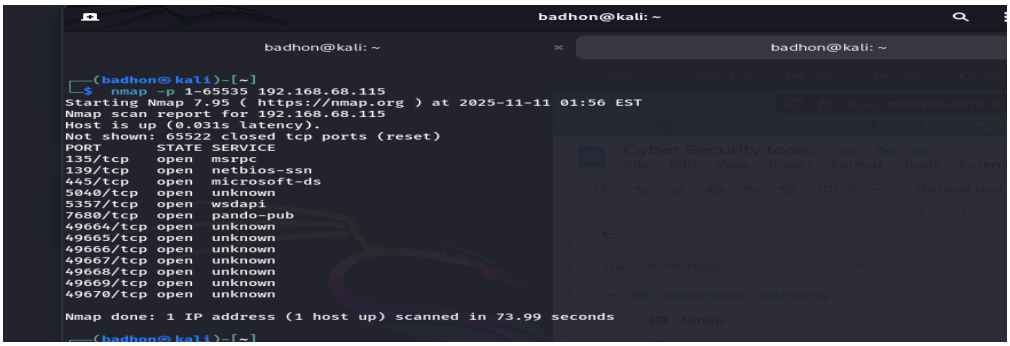



***Figure 12:*** **Scans all 65,535 ports for a full security overview.**

**My Work:** Performed a full TCP port scan (1–65535) and identified multiple open ports, revealing various active services on the host.

**Command / Option:** -F
**Full Command:** nmap -F 192.168.68.0/24
**Description:** Performs a fast scan on the most common ports.

**Screenshot:**


***Figure 13:*** **Performs a fast scan on the most common ports.**

**My Work:** Performed a fast scan (-F) across the network to quickly identify active hosts and commonly used open ports within the subnet.

**Command / Option:** --top-ports 100
**Full Command:** nmap --top-ports 100 192.168.68.115
**Description:** Scans the top 100 most frequently used ports.

**Screenshot:**

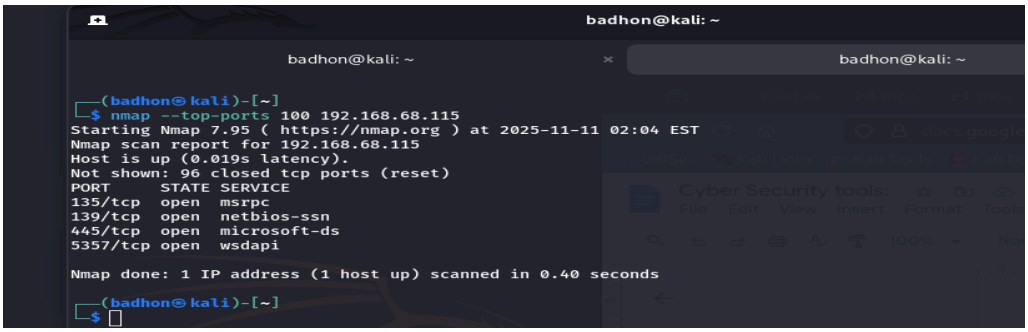



***Figure 14:*** **Scans the top 100 most frequently used ports.**

**My Work:** Discovered critical services running on common ports.

**Command / Option:** --exclude-ports
**Full Command:** nmap --exclude-ports 22,80 192.168.68.115
**Description:** Excludes selected ports to reduce noise or avoid sensitive Services.

**Screenshot:**

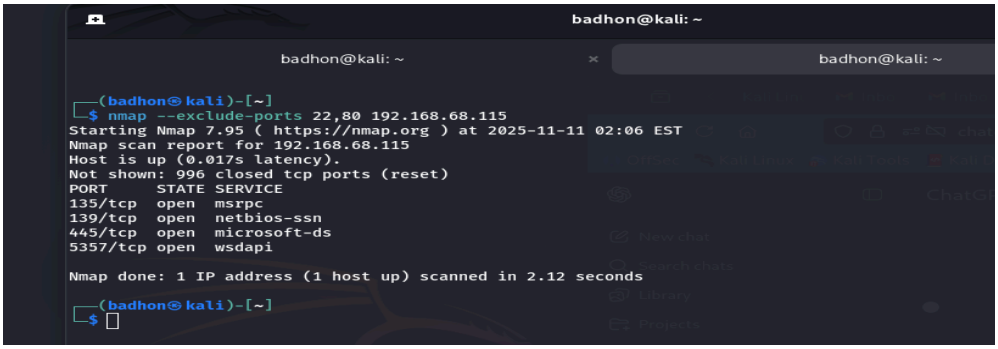



***Figure 15:*** **Excludes selected ports to reduce noise or avoid sensitive Services.**

**My Work:** Scanned all other ports except SSH and HTTP for cleaner results.

**Summary:**Port scanning provides a clear view of available services and potential vulnerabilities, helping to prioritise security actions.

### 3.3 Whois Command:

**Description:** Whois is an important command-line tool which can be used to query public databases and obtain information about domain names, IP addresses, or Autonomous System Numbers (ASNs). It delivers critical visibility, helping you thoroughly understand your network and prevent attacks. Whois is often used by users to obtain information for a variety of purposes (e.g., the registrar that holds the domain, when the domain was created, when the domain will expire, what are associated name servers or contacts related to some domains are doing so websites), commonly using command such as target ”whois google.com”). com”). This flexible utility also provides advanced options for performing qualified searches. e.g.: it is possible to specify custom whois servers (ex:“whois -h whois. ripe. org 193.0.6.135”) or send requests to provided communication port (example: “whois -h whois. verisign-grs. com -p 43 example. com”). In the end Whois has done a world of good in determining who actually owns domains/networks. It greatly supports early stages of security analysis and penetration testing by providing valuable intelligence on target digital infrastructures.

**Command: whois [options] [domain|IP|ASN]**

| Option | Example | Description |
|---|---|---|
| Basic | whois example.com | Queries the default WHOIS server for domain info. |
| -h <host> | whois -h whois.verisign-grs.com example.com | Manually specify the WHOIS server to query. |
| -p <port> | whois -h whois.verisign-grs.com -p 43 example.com | Specifies a custom port (default is 43). |
| --verbose | whois --verbose example.com | Outputs detailed debug/connection info. |
| --help | whois --help | Displays help information for the command. |

**Table 1:Common WHOIS Command Options provide this table**

#### 3.3.1 Example WHOIS Lookups

**Domain Name Lookup**
Example: whois google.com

**Scan Screenshot:**

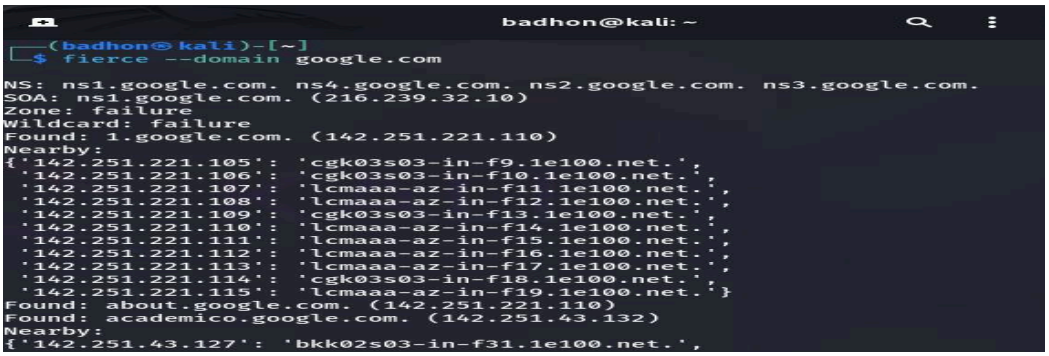



***Figure 16: Domain name lookup***

Description: Retrieves registrar, registration dates, name servers, and contact info.

**IP Address Lookup**

Example: whois 8.8.8.

Description: Displays the network owner, ASN, and CIDR range (usually from ARIN, RIPE, etc.).

**Specify WHOIS Server**

Ex: whois -h whois.ripe.net 193.0.6.135

Description: Queries RIPE (European registry) directly for an IP.

**Lookup Using Custom Port**

Example: whois -h whois.verisign-grs.com -p 43 example.com

Description: Uses a specific port for the WHOIS server.

**ASN Lookup**

Example: whois AS15169

Description: Shows owner and routing info for the Autonomous System.

### 3.4 Fierce

**Description**: Fierce Fierce is a reconnaissance tool which can help locate non-contiguous IP space and hostnames against the target. It assists penetration testers and cybersecurity researchers by revealing critical data in the early stages of an engagement.

The script uses targeted DNS queries to identify subdomains and network blocks not visible to the public, but present in the zone file if they exist. This can make Fierce an especially practical tool when fingerprinting a target's external attack surface, and looking for systems that deserve more scrutiny.

**Command: fierce** --domain [target-domain]
**Example: fierce --domain** google.com

**Scan Screenshot:**

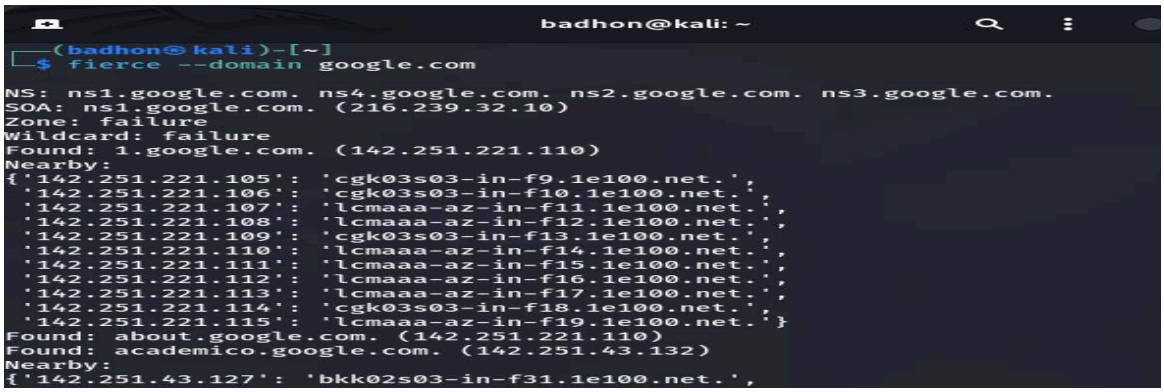



*Figure 17: Target Domain fierce*

**I did work:** The command above describes the DNS map of google. com. It detects subdomains and IP addresses may be potential attack vectors or network information leak points. We replied to a lot of little ip address and DNS service is tomein google. com.

### 3.5 Dnsenum

**Description:** This command collects details of the example. com along with its DNS records, subdomains and all associated data.

**Command**: **dnsenum example.com Example**: **dnsenum backdoor.com.bd**

**Scan Screenshot:**


*Figure 18:* **DNS records**

**I did work:** The command grasps DNS-related information on backdoor. com. bd, revealing subdomains, servers. We found backdoor. com. BD Hosts server, DNS Server and Mail Server.

### 3.6 DnsMap

**Description:** DNSMap is a open source repository and network information gathering tool that was originally released 10-June-2017 making it yet another addition to the If you are familiar with penetration testing tools, then you should know the name or even might have used the Network Mapping and Enumerator like nmap. It assists hackers and Security professionals in helping you discover hidden domains related to a target domain. Released in 2006 by Paul Craig as a real-world application of the fictitious work described in his novel *"The Thief No One Saw,"* this utility was created with the express purpose of discovering sub-domains which no ordinary DNS client would ever list.

It does that by doing DNS queries based on a user-supplied dictionary file. Bye includes a standard wordlist with popular English and spanish words like *ns1, firewall, smtp..* etc., as well custom wordlists to make the developement project-specific.

In an effort to give the scan more coverage, DNSMap has all these goodies:

- Filtering the IP to filter out real positives and negatives.
- Modifying query delays to avoid detection
- Saving out in a read-able format, rather then back to CSV.

For massive enumeration efforts, this tool also hands you **dnsmap-bulk.** sh to give users the ability to do scan multiples of domains at once faster.

**Command: dnsmap example.com**

**Example: dnsmap backdoor.com.bd**
**Scan Screenshot:**

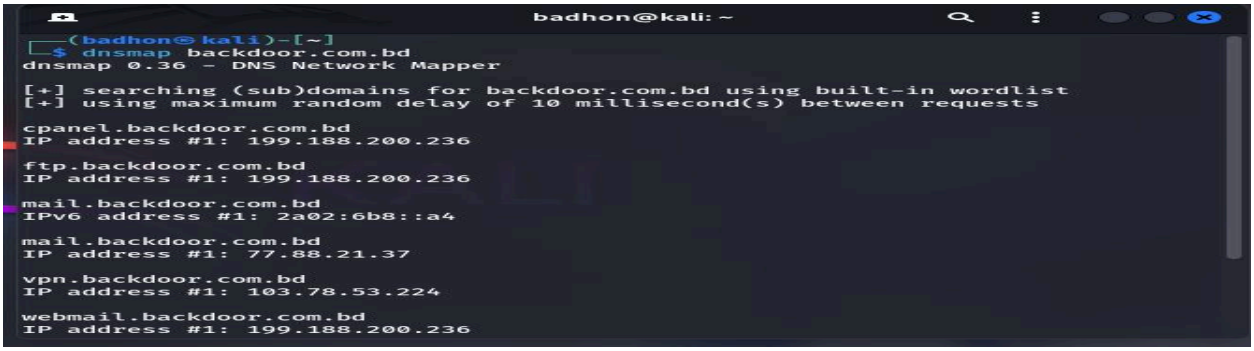



***Figure 19:*** **Dnsmap-bulk**

**I did work:** From the command we can see accpetable subdomains of backdoor. com. bd brute-force helping map the attack surface or network presence of the domain. We discovered ftb server, web mail, mail server and server IP address.

### 3.7 Spiderfoot

**Description:** SpiderFoot is a reconnaissance tool that automatically queries over 100 public data

sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names and more.

While interning at **Backdoor Pvt Ltd**, I utilized SPIDERFOOT to automate the process of gathering information about targets such as domain names, hostnames and subnets. The tool uses in excess of 200 modules to perform tasks such as data correlation, domain footprinting and active/passive scanning.

SpiderFoot's interface is easy to use using the command line or web-based dashboards. For instance, you might include on the command line

**python3 sf.py -l 127.0.0.1:500**

It also allows to create custom scan profiles (e.g. Passive, Investigate, Footprint) and to export results in the CSV/JSON/GEXF file formats. Superiority! API integrations make it even more powerful as it now allows integration with premium data sources.

SpiderFoot is a very promising tool for both offensive penetration testing as well as defensive purposes including security professionals can search relationships between entities, expose additional nodes and relationship indicating potential vulnerabilities in the network. But it may work only when you have some API keys for premium sources and enough resources to scan large scale.

**Command: spiderfoot -l 127.0.0.1:5001**

**Screenshot:**


***Figure 20: Spiderfoot Starting on web***

**Open a web Browser:**

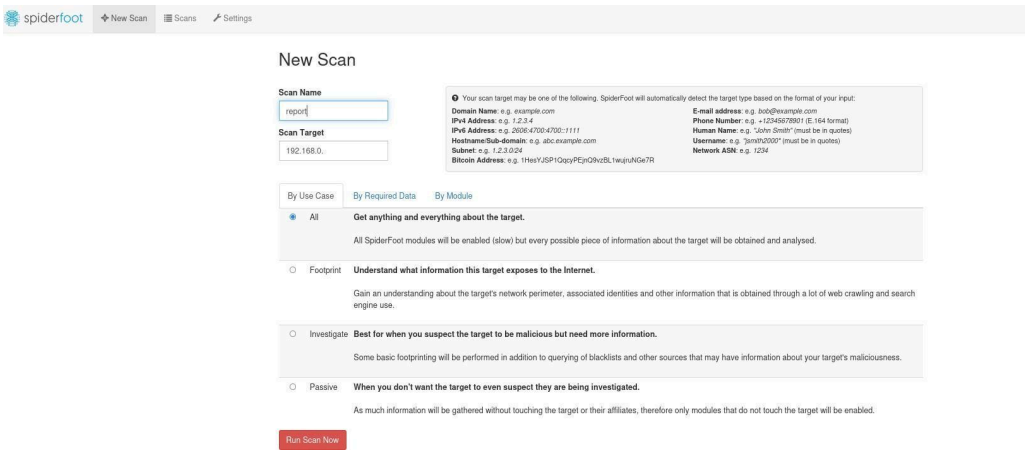



***Figure 21: Open Springfoot web Browser***

## 3.8 Nessus Tools:

**Description:** Nessus is a top Vulnerability scanner released by Tenable Serving which could detect vulnerabilities around the networked systems, databases & various other application. Used in Kali Linux this tool isolates vulnerability searching, going through the hundred of tools available after its GUI via an web page matahari interface. The recipe has you downloading and installing the Nessus Debian package, bootstrapping the service, creating scans through a web interface (served on https://localhost:8834), as well configuring your targets and scan policies. Nessus scans for vulnerabilities, configuration issues, and compliance violations and provides detailed sharing information including severity scores, solution information with research references, and html or pdf output. Some notable features include a large up to date plug ins database, the ability to provide custom scan templates and web app scanning as well as compliance checking and integration with Kali toolset – perfect for security professionals. Up-to-date plugins, thoughtful target choices, and an easy time management of vulnerabilities confirmed being capable in handling more than a single virtual machine in kali but doesn't run as smooth with all targets off the included Kali version.

### 3.8.1 Work Process of Nessus on Kali Linux

**Open Nessus in this terminal:**

**Open in browser:** https://localhost:11127 (any local browser)

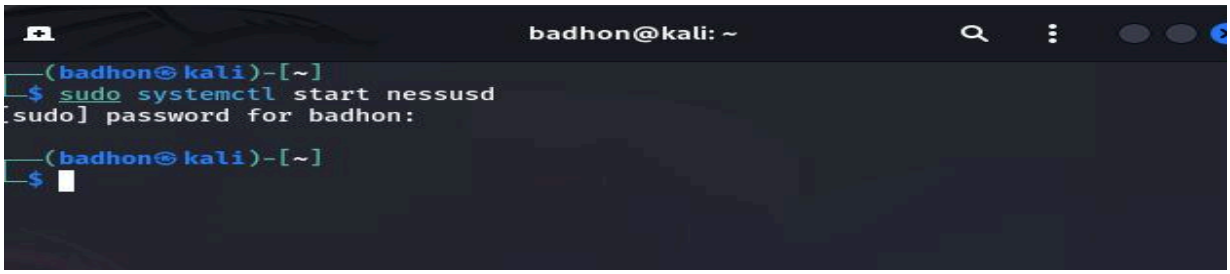



*Figure 22 : Open Nessus Terminal command*

**I did work:** We command in the terminal and run Nessusd

**Log in interface:**

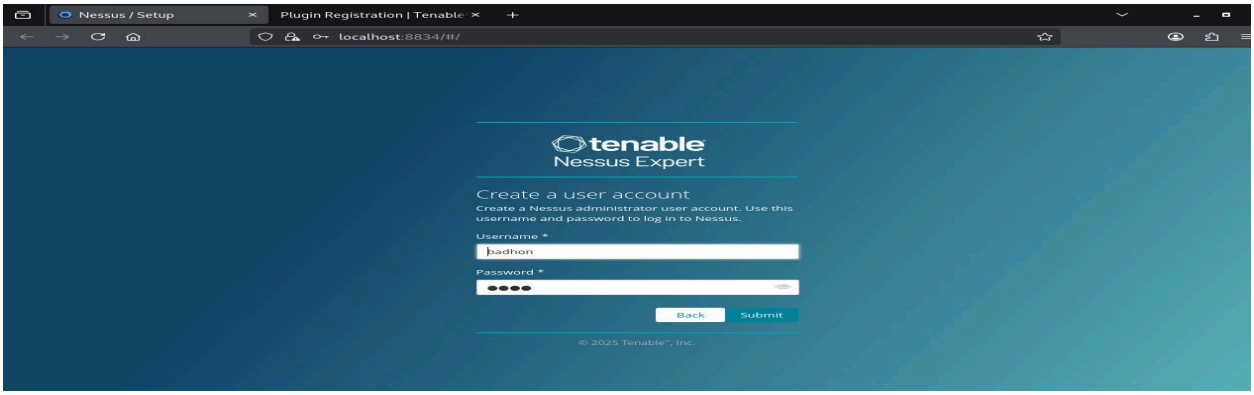



*Figure 23: Nessus Open in terminal*

**I did work:** We login the Nessus website using Username & Password

**Plug in the software:**

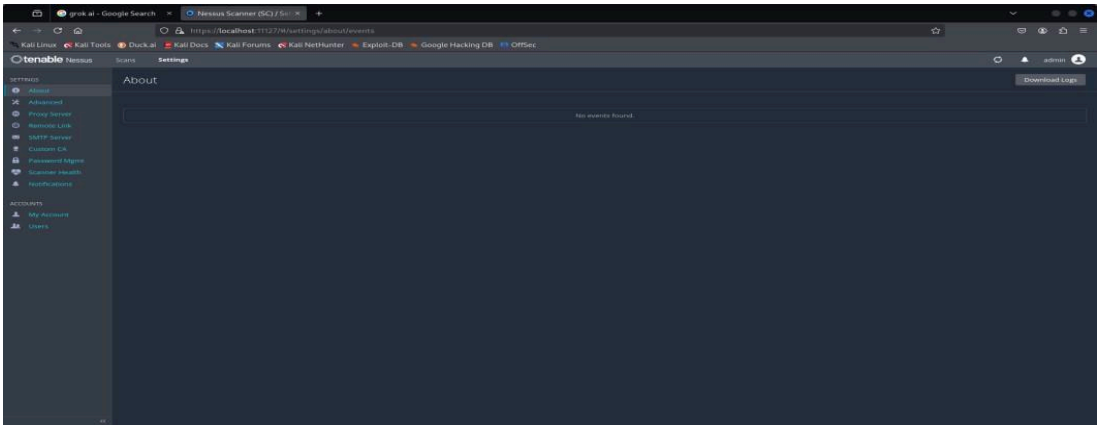



***Figure 24: Plug in Software***

**I did work:** Plugin all services in Nessusd

**Nessus Home page:**

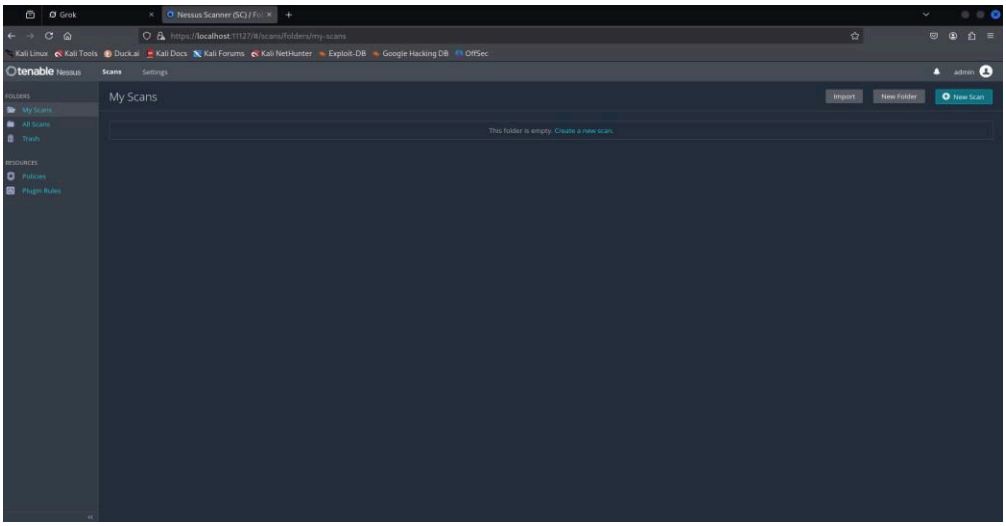



***Figure 25: Nessus home page***

**Scan Templates:**

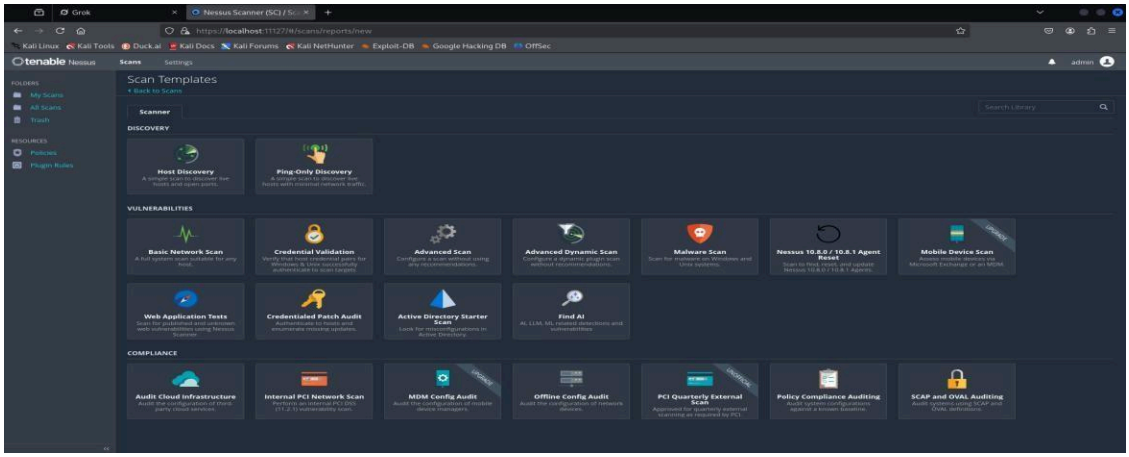



*Figure 26 : Scan Terminal*

**New Scan for Host Discovery:**

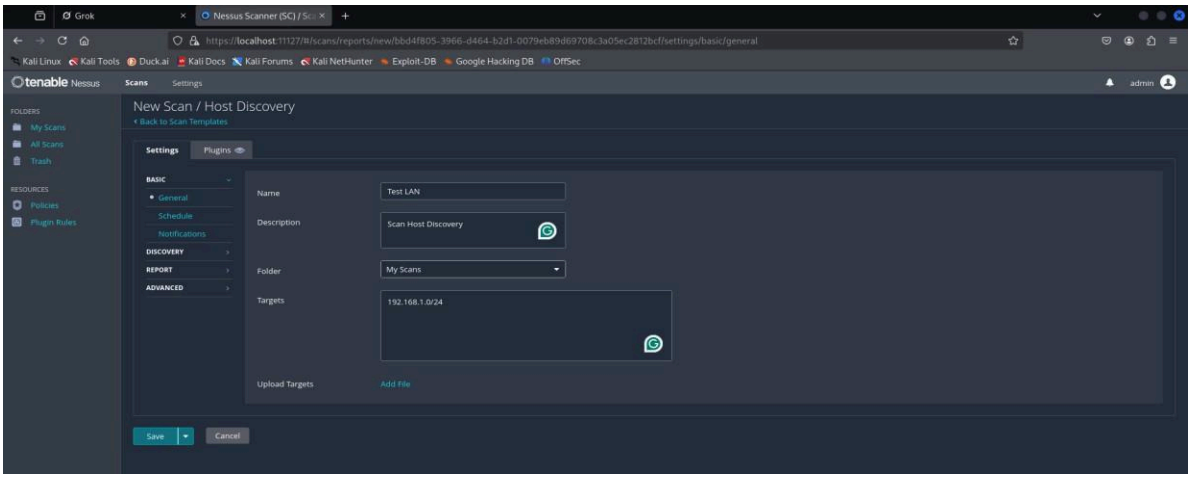



*Figure 27 : New Scan for Host Discovery*

**I did work:** We started a new scan for host discovery. We set up the scan technique.

**Save Scan**

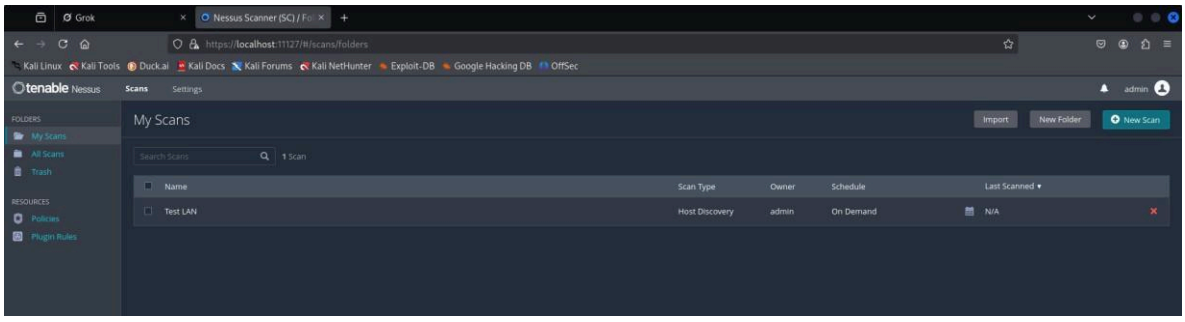



*Figure 28: Save scan*

**I did work:** Save the scan for scanning host discovery.

**Lunch the Scanning:**

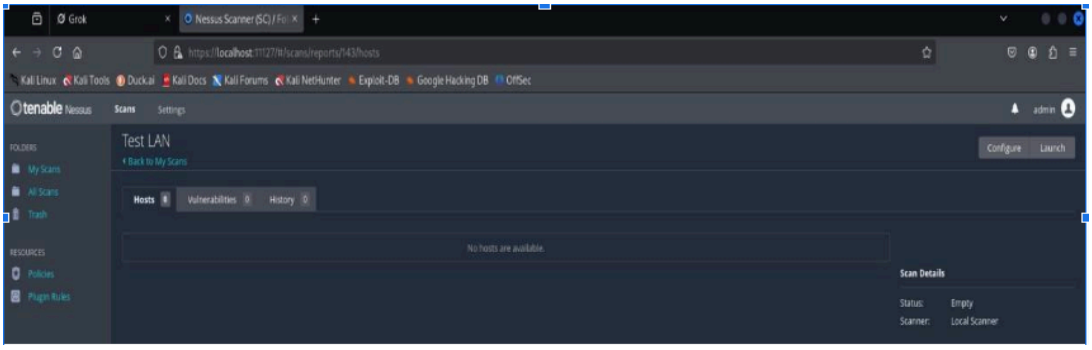



***Figure 29: Lunch the host discovery Scanning***

**I did work:** Lunch, the host discovery scanning

**Start Scanning:**

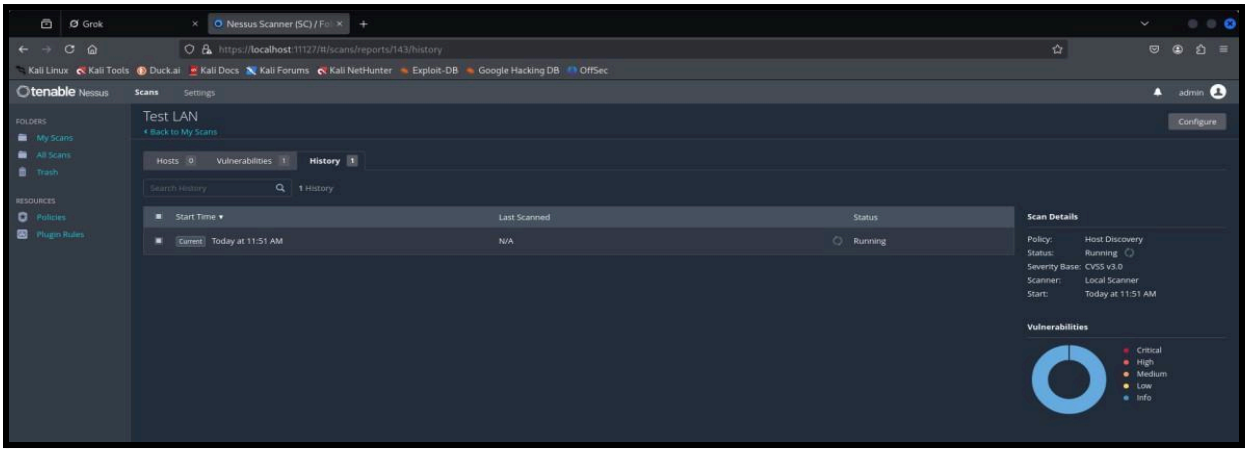



***Figure 30: Start Scanning***

**Scanning Complete:**

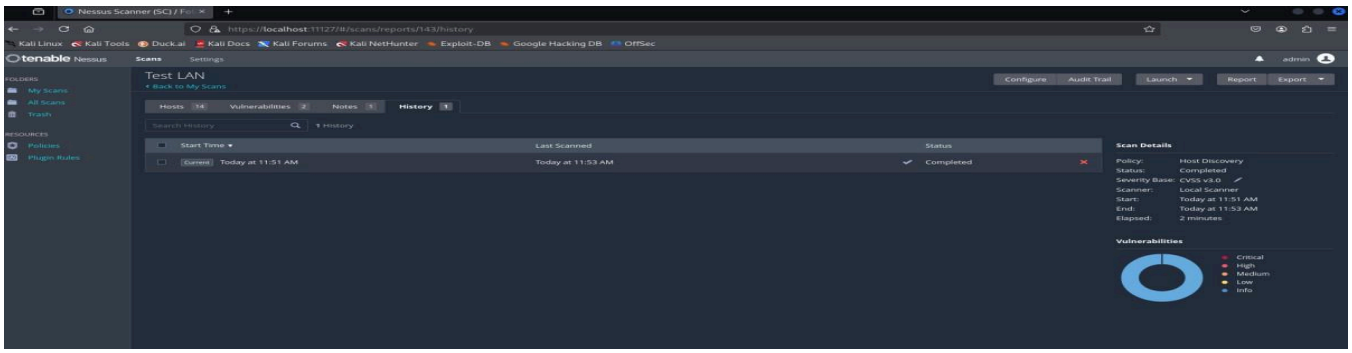



***Figure 31: Host directory scanning complete***

**Host Discovery after scanning:**


*Figure 32: After Host directory Scanning*

**Vulnerability Find After scanning:**

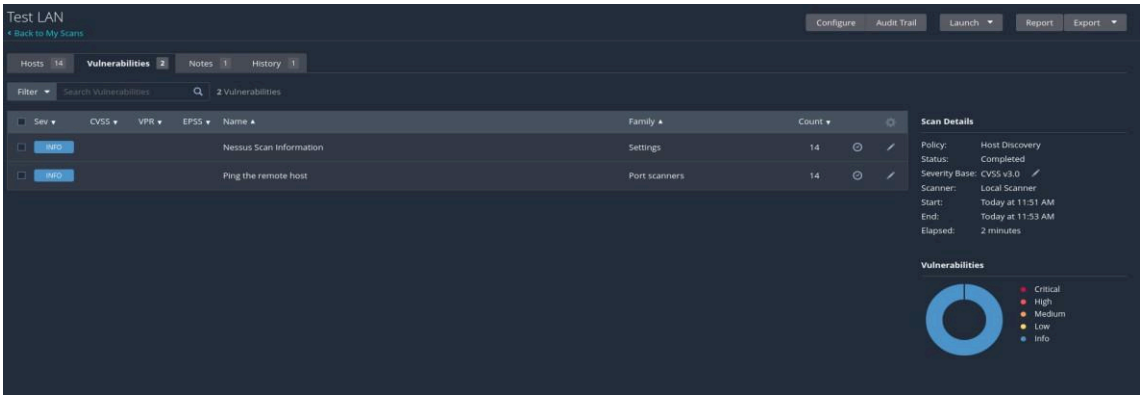



*Figure 33: Vulnerability found after scanning*

**Generate Scanning:**

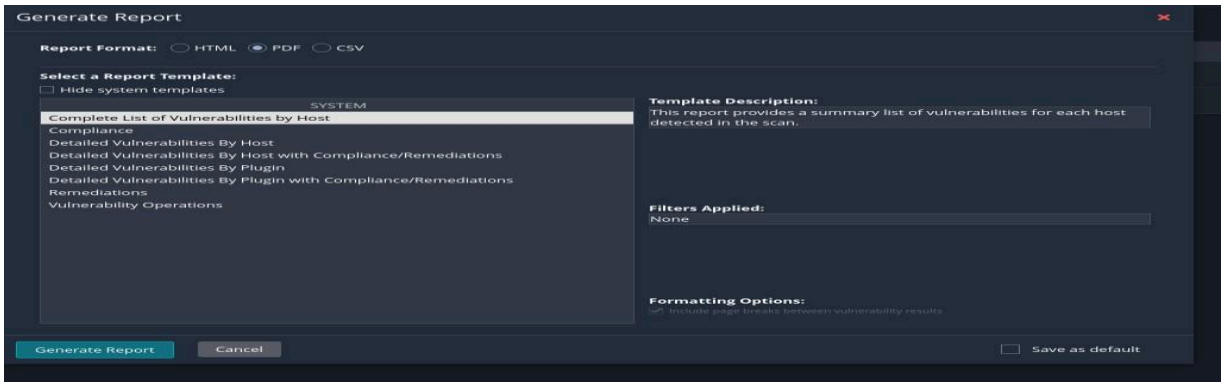



*Figure 34: Generate Scanning*

### 3.9 OpenVAS:

**Description:** The free and open source software, OpenVAS (Open Vulnerability Assessment System), was a fork of the Nessus project after it became a proprietary tool, and after spending some time in versions 2.x of the software, it eventually saw an editor rewritten as version 3.0 until today Greenbone has published its own direct successor for the popular scanner on GitHub. It uses a collection of some 50,000 Network Vulnerability Tests (NVTs) to detect threats affecting network services, servers, and all connected devices that are updated regularly. OpenVAS provides support for authenticated and unauthenticated testing, and industrial protocols as well as high- and low-level internet protocols allowing for a flexible optimal tool capable of conducting cybersecurity assessments. It delivers detailed results based on Common Vulnerability Scoring System (CVSS) severity and has the capability to tune for very high-volume scans. It includes a web-based interface, the Greenbone Security Assistant which is available at https://localhost:9392 and provides access to various tools like scan configurations, report management and others in an easy to use web application for security tester. OpenVAS is Resource-hungry, it uses around 5GB of RAM and an average CPU load of 20%, so its well suited for penetration testers and companies that are looking for a free vulnerability management solution.

#### 3.9.1 Work Process:

**Open OpenVAS in Terminal:**

**Command:** "sudo gvm-start"

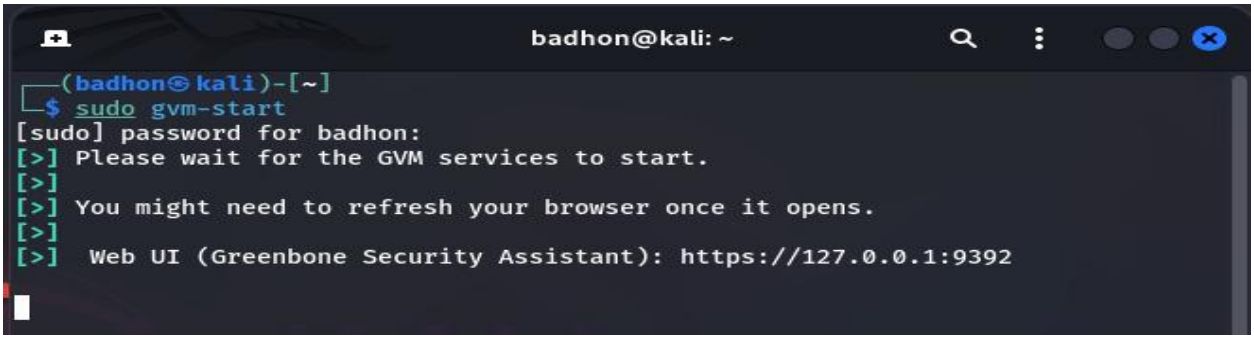



***Figure 35: Start OpenVAS command***

**Open a browser,** open this link https://localhost:9392

**Open Greenbone Security Login page:** log in with Greenbone Security username & password

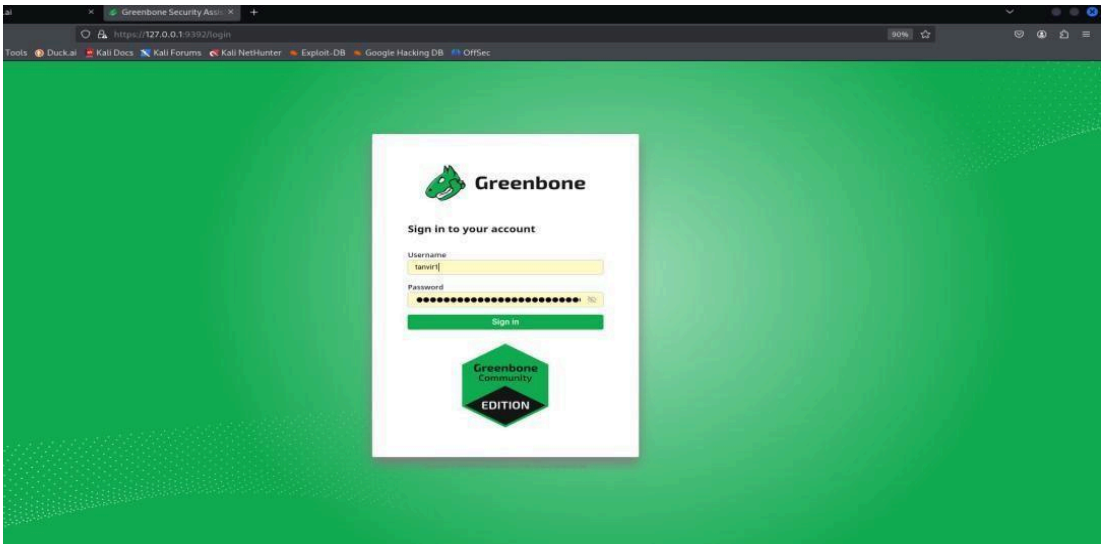



*Figure 36: OpenVAS Website login page*

**Open Dashboard:**

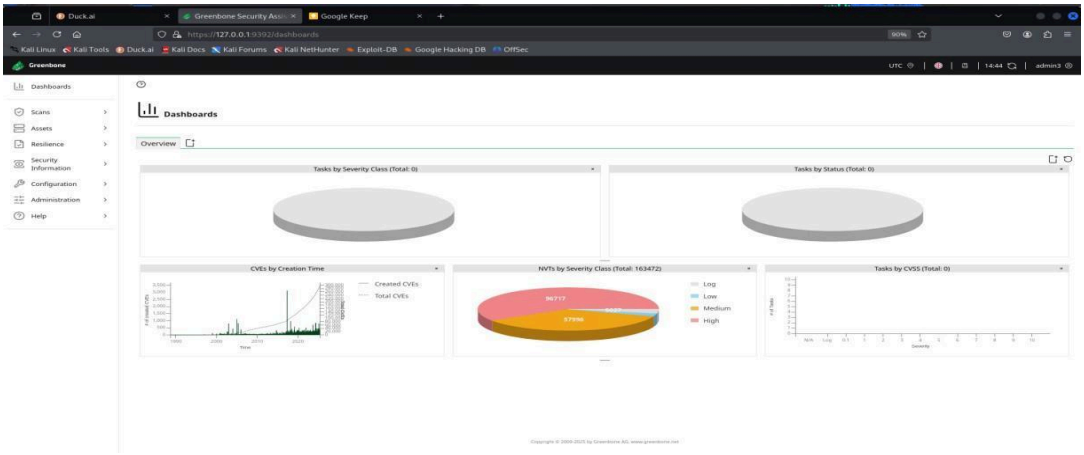



*Figure 37: Show Dashboard*

**Scan Task :**


*Figure 38: Scan given task*

**Lunch the scanning:**

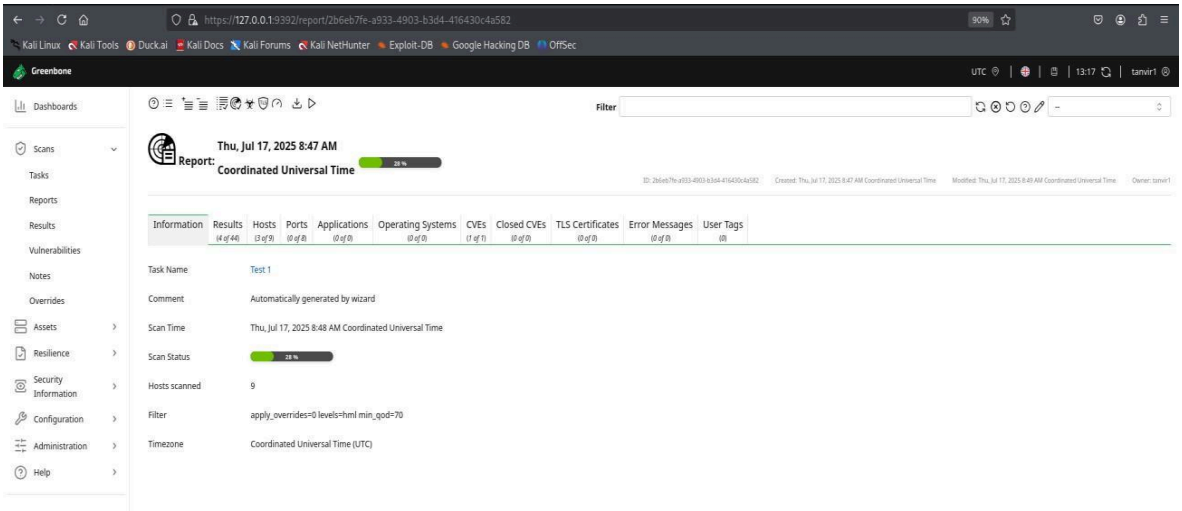



***Figure 39: Lunch the scanning***

**Complete Scanning:**

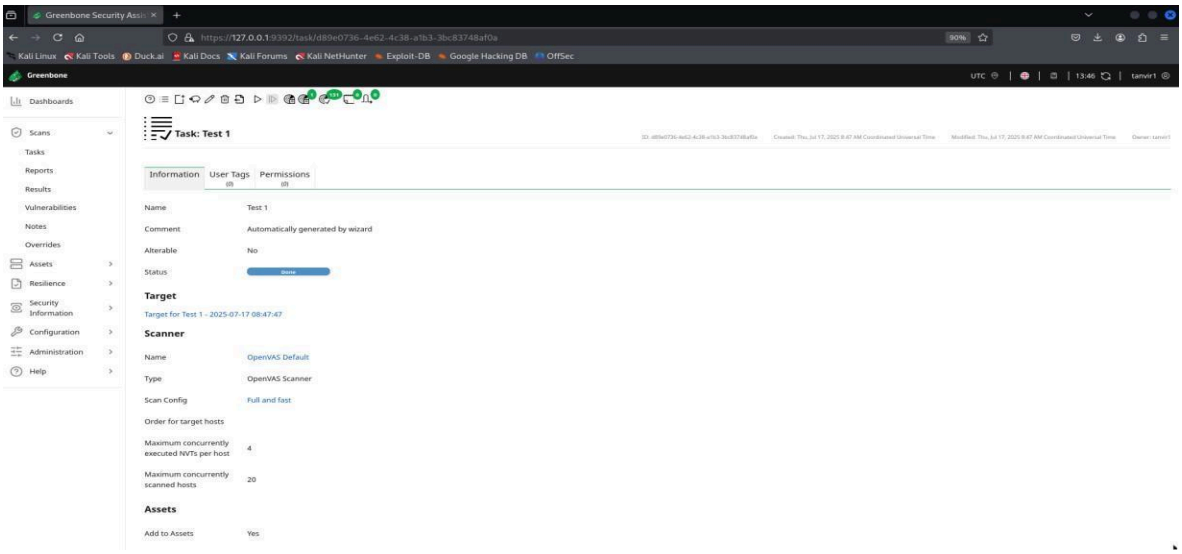



***Figure 40: Complete this scanning***

**Stop Openvas in Terminal: “ sudo systemctl stop gvmd ”**

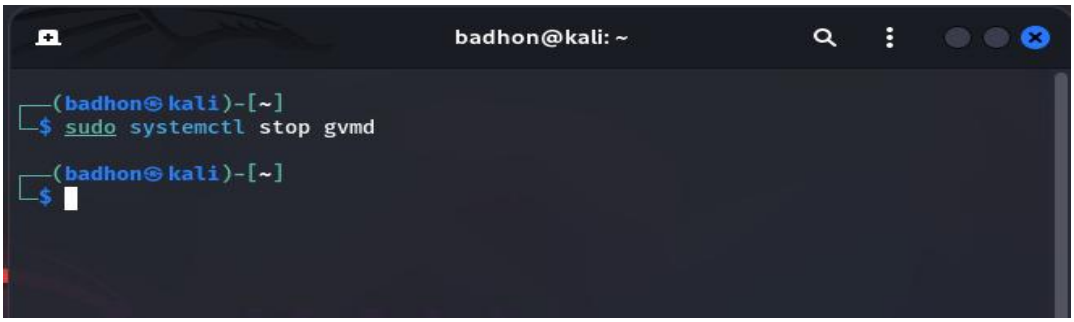



*Figure 41: Stop command for OpenVAS*

### 3.10 Znmap

**Description:** The graphical interface to the official implementation of Nmap is known as Zenmap. It's a great open-source tool to explore the network and perform security audits. It works in Linux, Windows and MacOS, among other platforms. Zenmap makes Nmap easy to use on the command line. This makes it a little easier for beginners to use, but still gives experience users all the advanced tools they need. Network scanning can be used to find hosts, open ports, services and operating systems. They can also store their commonly used scans as profiles for use later on. Zenmap also offers a command creator that can be used to create and share Nmap commands, a topology map showing connections between hosts in your scan, as well as a searchable database for storing and comparing scan results. Network administrators and cybersecurity professionals love Zenmap for projects such as penetration testing and vulnerability assessments, due to the wealth of information it gives about network configurations and problems.

#### 3.10.1 Work Process:

**Open Zenmap**

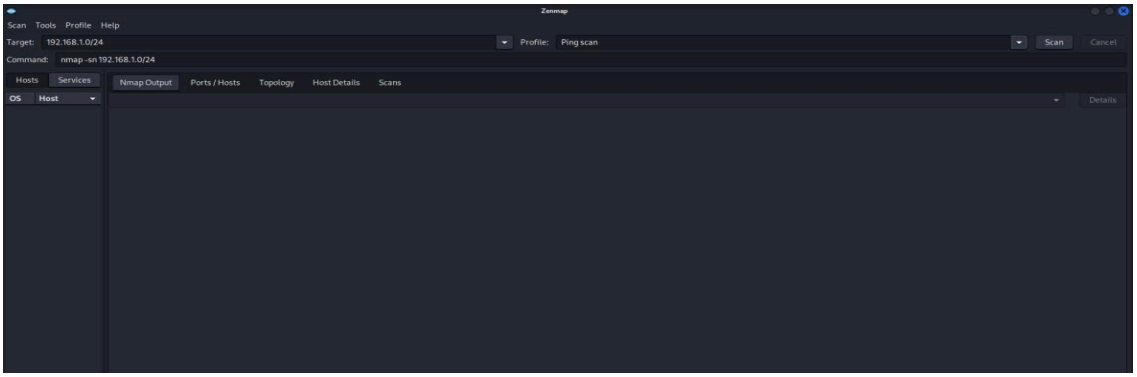



*Figure 42: Open Zenmap*

**Zenmap home page:**

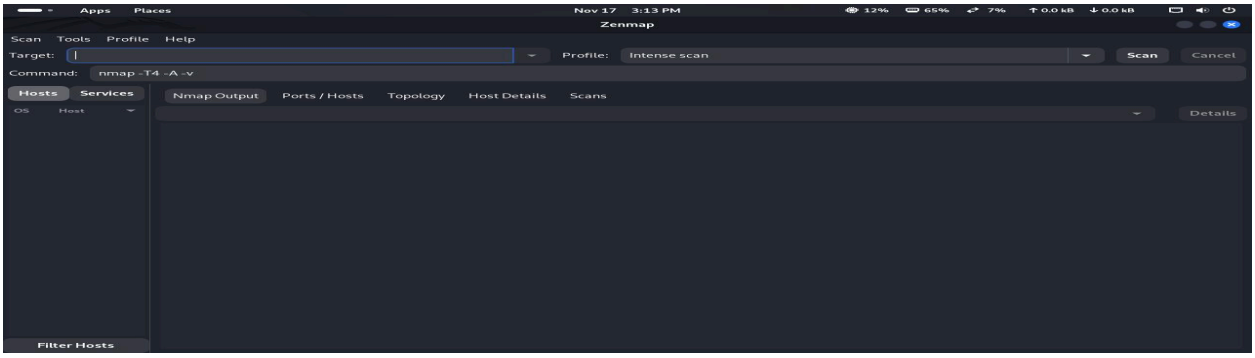



*Figure 43: Zenmap Home page*

**Set the target IP and press scan:**
**Complete scanning:**

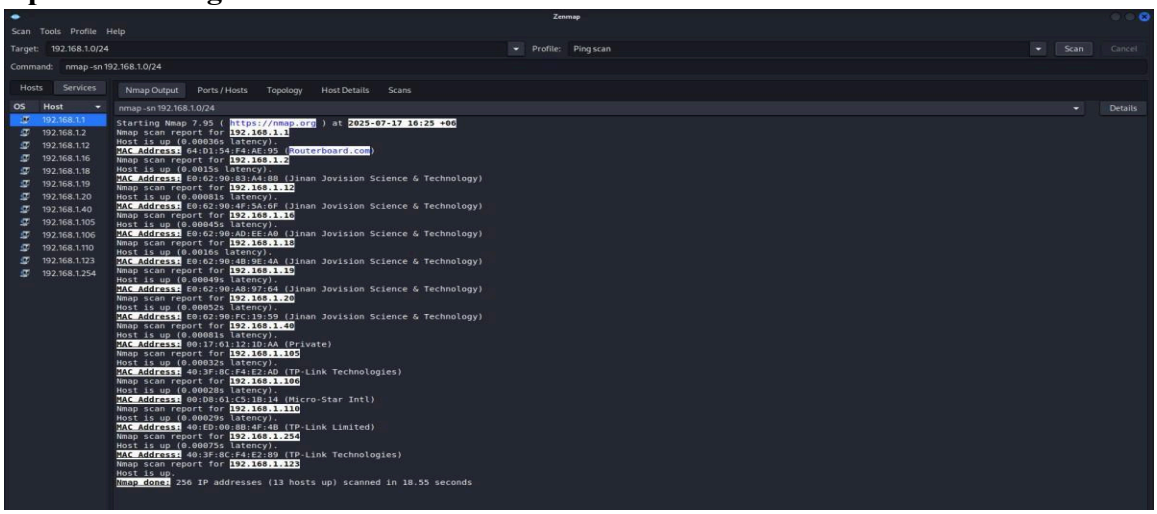



*Figure 44: Set the target ip and complete scanning*

**Digital Forensic**

**3.11 Oxygen Forensic**

**Description:**About Oxygen Forensics Detective An advanced, all-in-one tool based on a cloud approach dedicated for a variety of digital investigations including mobile [devices? types], device data and IoT analysis. It is very good at defeating security locks being used and parsing data from over 2,000+ applications as well as many other system files too!Parsing such a large number of apps makes Cellebrite the top tool for by-passing lock codes. It is used by law enforcement, intelligence agencies and corporate security leaders when you need to go beyond security logs, such as Windows events or system logs that are often the only evidence of an attack.

### 3.11.1 Key Features of Oxygen Forensic® Detective

**► Graphical User Interface (GUI)**

**Description:**Modern, scalable and multi-tabbed Oxygen Forensic® Detective user interface consolidates the entire process in one place - from device extraction and cloud collections to data analysis and final report generation. The GUI is intuitive, the examiner is led in a logical process and has access to some strong data visualisation tools, such as connection diagrams and geomaps.

**Benefit:**Simplifies mobile and cloud forensics, minimizes risk for human errors, and helps quickly analyze evidence from multiple sources.

**► Extraction and Parsing Modules**

**Description:** Oxygen Forensics Features This software uses a modular design to recover and decrypt information from a wide range of sources. These are the modules that handle parsing raw data into something human readable.

**Some Typical Extraction and Parsing Module:**

- **Physical: Globe Throttler –** bypasses lock screens, full binary image extracted from mobile devices w/ deleted info included.
- **Cloud Service Extraction:** Data is collected directly from accounts on services such as Google, iCloud, Facebook and Telegram with the use of legal credentials.
- **Application Parsing:** Deciphers information from thousands of applications including chats, media and call logs (such as WhatsApp, Signal and Snapchat).
- **Password & Key Recovery:** Extracts passwords, tokens and other authentication details from the device to enable access to protected apps and data.
- **Geolocation Analysis:** Maps GPS, Wi-Fi and app artifacts data to interactive map views.
- **IoT & Drone Forensic:** Collects and analyzes data from smart devices, wearables and drones.

**Benefit:**

Automates data to be able to read, analyze & report on complex data from modern devices … a level of analysis which would otherwise be impossible with general-purpose forensic tools.

**► Unified Timeline Analysis**

**Description:**This functionality aggregates the time stamps of system events - application events, communication records (calls and text messages) location stainings history in chronological order. Events can be filtered by source, type and time range to replay the full story of any user's behaviour.

**Benefit:**Allows researchers to correlate events among various applications and system layers for fast analysis of potential sequences or patterns of important operations.

► **Data Visualisation Tools**

**Description:**Visual representation with Oxygen Forensics is great for representing relationship and movement. The Connection Diagram will show links between contacts, calls and messages while the Geomap will plot all location data recovered.

**Benefit:**Turns vast amounts of intricate data into simple visuals that better explain social links and travels between towns, for reports and courtroom demonstrations.

► **Advanced Reporting Tools**

**Description:**The product produces detailed reports in styles of PDF, HTML or XLSX ready for court. Reports are fully configurable and with tagged evidence, annotated screenshots, visualisations and comprehensive examiner notes.

**Benefit:**Demonstrates complex digital evidence to attorneys, clients and juries in a professional fashion.

►**Professional Support and Updates Official Plugin This plugin is officially developed by MailerLite.**

**Description:**A commercial tool, with its dedicated support staff, comprehensive documentation and the promise of swift development updates Oxygen Forensics If it doesn't live up to your expectations then drop a mail to me; I'm all ears! New device and application parsers regularly are included to keep up with developments in the digital world.

**Benefit:**Offers dependable, expert help for your most important investigations and makes sure that new device or application you have added to your lab is included in your data collection.

**3.11.2 Work Process of Oxygen Forensic® Detective**

**1. Create a New Case**

**Description:**Investigations start by creating a new case file in the Case Manager. It all brings out the extracted data, analysis and reports in one place.

**Purpose:**Preserve organization, integrity and continuous chain-of-custody of all evidence generated in association with a particular investigation.

**How It Works:**The examiner opens a new case by clicking New Case, enters the case (number, examiner and description) details.\nAt this point an organised data base for the case is created in Oxygen Forensics.

**2. Add a Data Source**

**Description:**The investigator includes the evidence source in the case. This can be a physical device connected with USB, a cloud account, a devices back-up (iTunes or Cellebrite/UFDR), or disk image.

**Purpose:**Scope: Determines what digital evidence to examine.

**How It Works:**Through a "Add Data Source" wizard, the investigator is presented with type of source ("Mobile Device," "Cloud Service," or their respective backup copies) and prompted to connect (device) or select file (backup).

**3. Extract Data**

**Description:**This crucial stage uses Oxygen Forensics' extraction modules to collect data from the chosen source. Mobile devices you might be prompted to choose the type of extraction (logical/physical/full file system) etc.

**Purpose:**To obtain a forensically sound copy of the data from the victim.

**How It Works:**The technique and software then acts according to the selected extraction method, such as bypassing lock screens or authenticating with cloud services. There is a progress indicator that lets you know the status.

**4. Analyse Results**

**Description:**After extraction and automatic parsing of data, the examiner examines the decoded artifacts.

**Key Analysis Areas:**

- Application Data (Chats, Calls, Media)
- Unified Timeline of Events
- Geolocation Data and Geomap
- Connection Diagrams
- File System Browser
- Tagged Evidence

**Purpose:**To recognise, understand and relate significant information from the already parsed data.

**How It Works:**Info is laid out in a left-hand navigation bar. Examiners look at a category, drill down into it, use search to find what they're looking for and then visualize results by marking relevant items.

**5. Generate Reports**

**Description:**Investigators provide a comprehensive report gathering of evidence for use in court or as part an internal examination.

**Purpose:**To officially record and report the evidence and the findings of an investigation.

**How It Works:**By "Reports" the examiner then choose format, pick granted tagged evidence

and visualisations they want to include and generate word document.

### 3.11.3 Limitations of Oxygen Forensic® Detective

**1. High Cost**

**Description:**Oxygen Forensic® Detective is a commercial tool that requires high investment, massive license fee and yearly maintenance fee for updates and support.

**Impact:**The exorbitant prices can be beyond the reach of small forensic departments, a single researcher or an organization with modest resources.

**2. Platform Focus**

**Description:**Although it can analyze computer disk images, its focus and development emphasis are mainly on mobile devices, cloud services, and IoT environment. It is not a replacement for full featured computer forensics tools such as FTK or X-Ways which perform full disk analysis.

**Impact:**Either that, or you're going to have to run Oxygen Forensics on other tools and make sure you can perform an investigation that spans the PC/mobile.

**3. Hardware and Cable Dependencies**

**Description:**The successful physical extraction of mobile devices relies on special reliable cables and USB hubs, as well as a stable hardware environment. It is the case that there can be subtle differences driven by hardware variability.

**Impact:**This introduces extra complexity, and means the examiners have to keep a stash of good cables/adapters on hand.… add delays for fixing connection problems

**4. Rapidly Evolving Target Environment**

**Description:**Apps, as well as mobile operating systems, are updated regularly. It takes time for Oxygen to support data extraction or decoding of information from a new app version or a major OS security update.

**Impact:**May slow down investigations of the most recent software, until a software update becomes available from Oxygen Forensics.

**5. Extraction Complexity on Secured Devices**

**Description:**Sophisticated physical extractions such as those performed on recent Android and iOS devices (with very strong hardware-backed security) often would be technically challenging, and chances of success are not assured.

**Impact:**Requires specialised training and level of expertise, and when unable to physically extract. Investigators should have alternatives available.

### 6. Dependence on Legal Credentials for Cloud Data

**Description:** Cloud extraction depended entirely on investigators lawfully having access to the account credentials (or access tokens) of the owner of the device or through a legal order.

**Effect:** In the absence of lawful access, a valuable potential source of evidence is lost which narrows the investigative possibility.

### 3.11.4 Work Process Screenshot:

### Open Oxygen Forensic

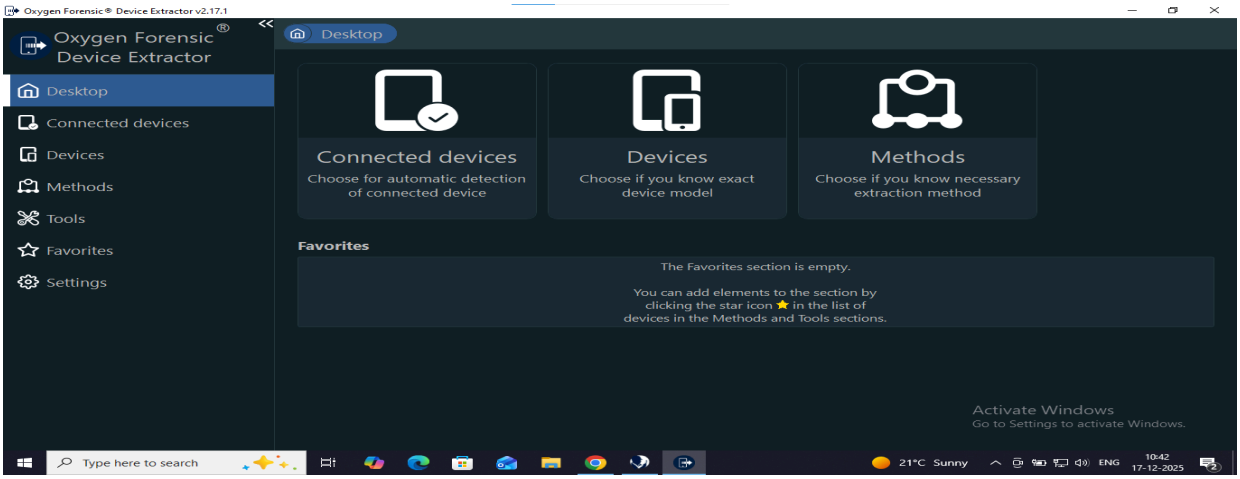



*Figure 45: Oxygen Forensic opening Page*

### Oxygen Forensic Home page:

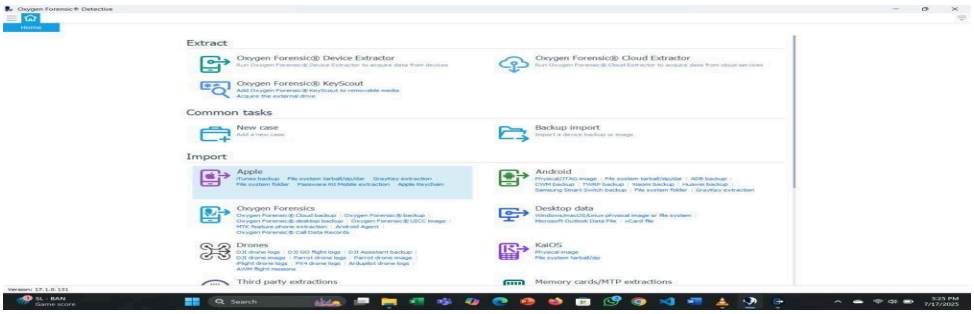



*Figure 46: Oxygen Forensic Home Page*

**Device Connect option:**

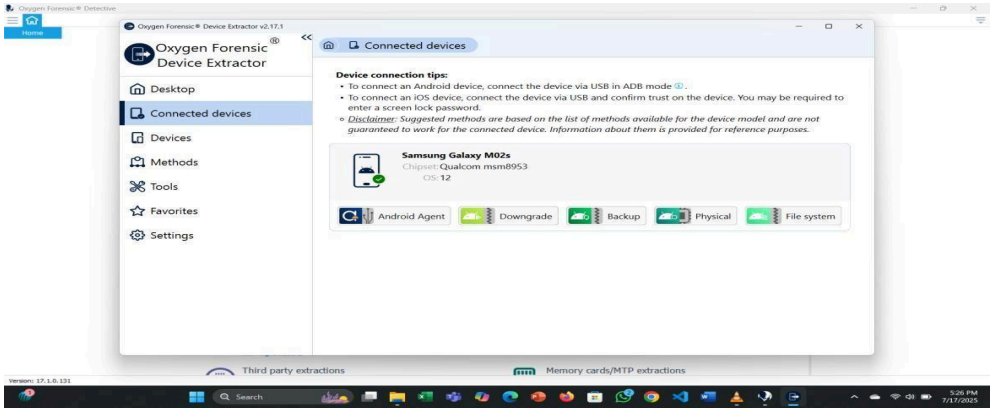



*Figure 47: Device connection option*

**Connection Device:**

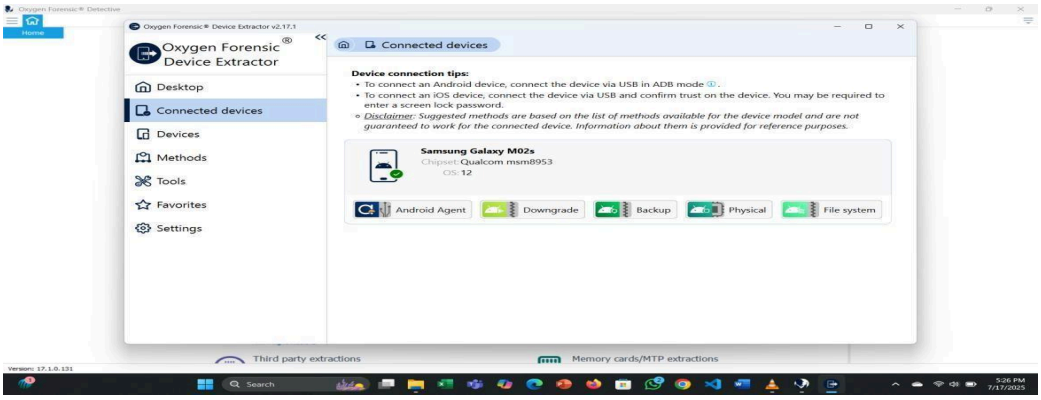



*Figure 48: Connection Device*

**Select file system**

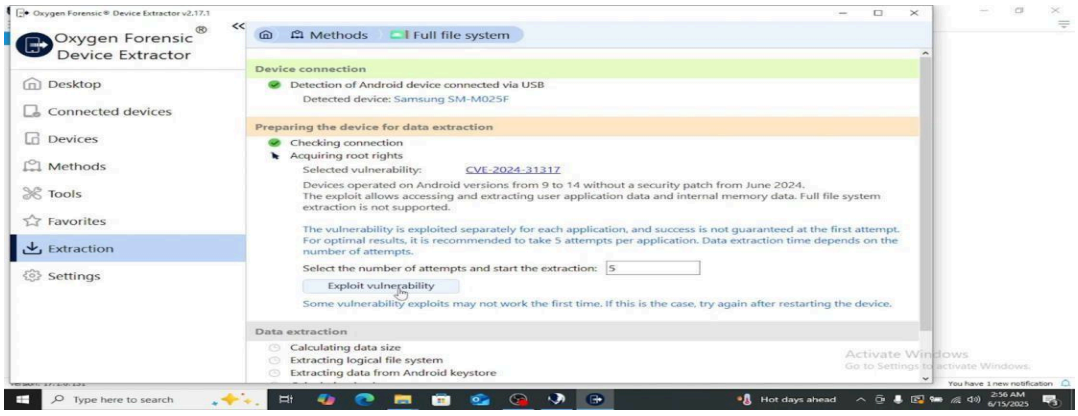



*Figure 49: Select file System*

**Find the Vulnerability: Exploit the vulnerabilities and gain root access to this device.**

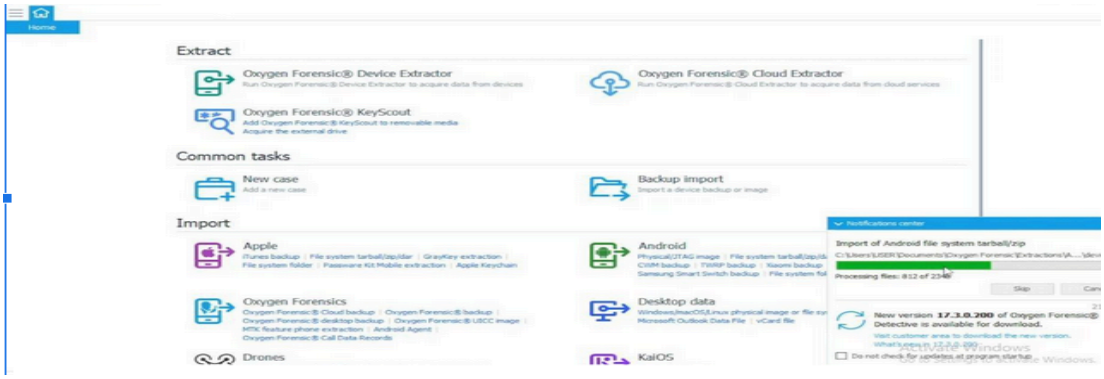



*Figure 50: Find the Vulnerability*

**Import Android system :**

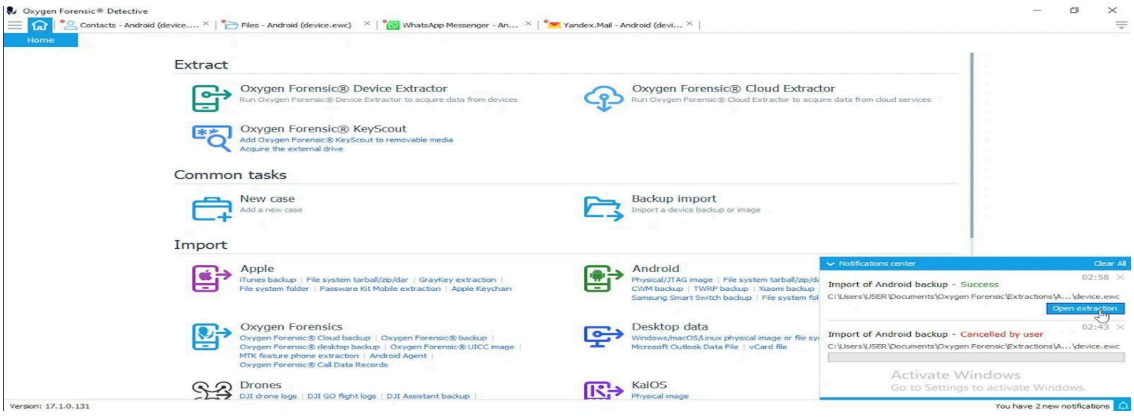



*Figure 51:Import Android system*

**Import Backup file:**

*Figure 52:***Import Backup file**

**Recover the file from this Android system:**

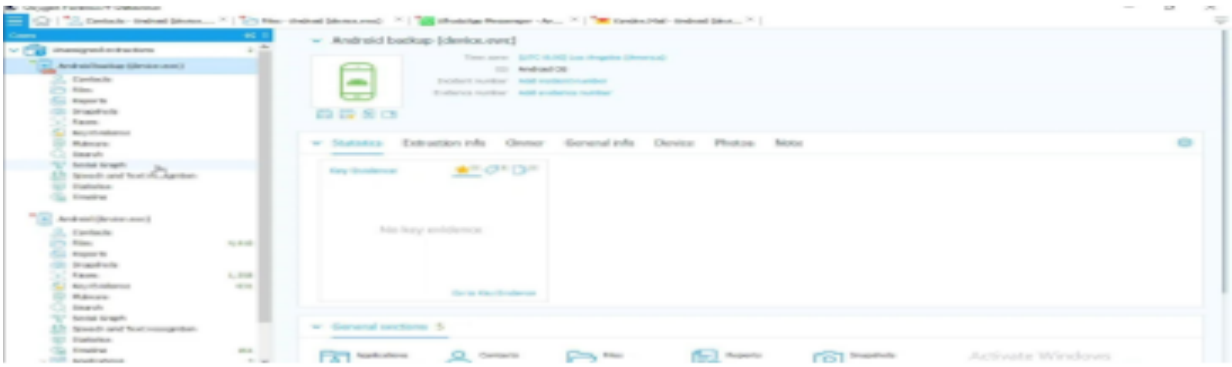


*Figure 53: Recover the file from this Android system.*

**Malware Scanning this Android system:**

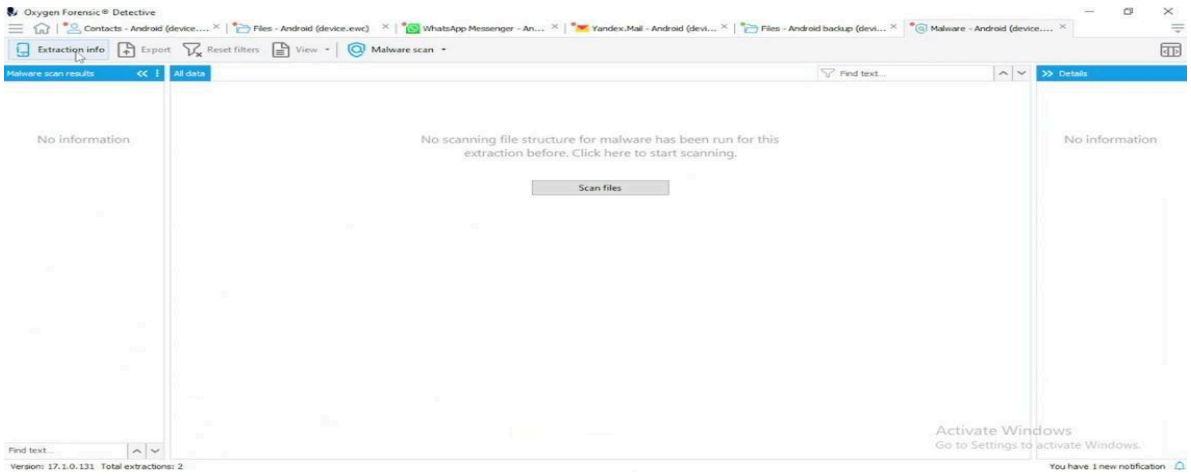



*Figure 53: Malware Scanning this Android system*

## 3.12 Autopsy

**Description:** Autopsy An easy to use, all in one digital forensic suite for investigators. It offers compatibility with several file systems and dissimilar data sources, as well as important features like lost-file recovery, keyword searching, timeline analysis and automatic report writing. Due to the wide range of powerful features and its dependable functioning, Autopsy is a first choice for forensics professionals in law enforcement, cyber crime investigations, and incident response among others.

### 3.12.1 Key Features of Autopsy

**Graphical User Interface (GUI)**

**Description:** Autopsy has a graphical browsing interface that makes the analysis of large volumes of object data easier than other tools. It's very usable even to people who aren't great on the command line. the user interface presents the information in structured views (file trees, timelines, categorised artifacts). Internally, Autopsy leverages The Sleuth Kit (TSK) for low-level analysis of the file system.

**Benefit:** Improves ease of use, shortens the learning curve and streamlines investigative workflow.

**Ingest Modules**

**Description:**
The development project that the Berlin Police are a part of provides ingest conponents which can process and extract artifacts using Autopsy's modular ingest. These modules are executed during the first processing steps and assist investigators to obtain important pieces of information fastly.

**Common Ingest Modules Include:**

- **Hash Lookup:** Looks up file hashes against known databases to find malicious or contraband files.
- **File Type Identification:** Sort files in accordance with file types for easy access.
- **Keyword Search:** Searches for user-defined keywords or regex patterns across allocated and unallocated space.
- **Email Analysis:** Parses email content, attachments and metadata from formats like PST & MBOX.
- **Web Artifacts:** Retrieves data associated with the browser such as history, downloads and cookies.
- **Exif Data Extraction:** Get info, such as GPS coordinates and time stamps from image or video files.
- **Recent Activity:**Notifies you about such things as USB use or opened files.

**Benefit:** Automated extraction of evidence, labor saving, and unequivocal scope.

**File System Analysis**

**Description:**
Autopsy is file system and data carving tool that enables the analysis of directory structures, such as file metadata, unallocated space or deleted contents. The software assists in the recreation of file fragments and the decoding of filesystem timestamps.

**Benefit:**Deep insight to local storage media and facilitate the recovery of hidden, lost or stolen data.

**Timeline Analysis**

**Description:** This item is a chronological visualization of system activity, documenting creation and modification times for files as well as directory access times. Investigators may also trim events based on time, file type or any artifact source.

**Benefit:** Investigators can put these pieces back together while looking at how user behavior fits throughout this scenario, see any anomalies in the process and then align evidence with the incident's time frame.

**Hash-Based File Verification**

**Description:** Autopsy can calculate MD5,SHA1 and SHA256 hashing algorithms on files. It guarantees that offences is not tampered with in the course of the examination.

**Benefit:** Tightens the chain of custody and assists with forensic admissibility in court.

**Deleted File Recovery**

**Description:** Similar to software recovery, AUTOPSY may revive lost items by examining the file system metadata or by data carving the unallocated space. Even if the file's data is partially rewritten, there is still a good chance of recovery.

**Benefit:** Restores valuable evidence deliberately deleted or purged to conceal criminal activity.

**Reporting Tools**

**Description:** Autopsy produces HTML, PDF and Excel reports. Reports can feature tagged evidence, keyword hits, file metadata, timelines, screenshots and investigators' notes.

**Benefit:** Results can be communicated to legal teams, clients or business decision-makers.

**Open-Source and Community Support**

**Description:** Autopsy is a free, open-source digital forensics tool that offers excellent extensibility, can be run from a USB stick or DVD, and includes multi-core processor support. Software and plugin updates are also rolled into the mix to enhance capability, stabilisation, and alignment with ever-changing forensic directions.

**Benefit:**The solution is cheap and extremely versatile in terms of forensics.

### 3.12.2 Work Process of Autopsy

**1. Create a New Case**

**Description:** The Investigation starts with the case creation, where all of the evidence-artifact-logsANALYSIS[1] output is saved in a structured way.

**Purpose:** Ensures structured organisation, and maintain complete traceability of forensic process.

**How It Works:** The investigator selects **"New Case"**, enters case information (name,

investigator name and storage location) and Autopsy will automatically creates the database for the new case

**2. Add a Data Source**

**Description:** User choose the evidence source and it can be disk (RAW, E01), logical drive, mobile backup or even a memory that needs bit-to-bit image.

**Purpose:** To determine the essence of data and maintain original evidence.

**How It Works:** The investigator chooses the type of evidence, finds the file/device, verifies hash (optional) using **"Add Data Source"** wizard.

**3. Configure Ingest Modules**

**Description:** Investigators select from among ingest modules that can be turned on for automated artifact extraction, including keyword search, hash lookup, email analysis and web artifact processing.

**Purpose:** Prevents human efforts and ensures effective data processing.

**How It Works:** A few modules will run for free as data is ingested. Users could tunings keyword lists, hashs databases and much more according to need.

**4. Process the Data Source (Ingest)**

**Description:** Autopsy examines the source data, retrieves deleted files, calculates hash values, and populates the case database.

**Purpose:** Analyzes raw evidence in order to present data uniformly and allow for further analysis.

**How It Works:**Setup, then finish (ingesting) investigators [redacted] fill the ampoules with chemical agents and click I'm finished to ingest them. The status of each module is indicated with progress indicators.

**5. Analyse Results**

**Description:** After ingestion, investigators can analyze the data gathered.

**Key Analysis Areas:**

- **File Browser**
- **Timeline Visualization**
- **Keyword Hits**
- **Email and Web Artifacts**
- **Metadata Details**
- **Tagged Evidence**

**Objective:** Aids valid identification, correlation, and interpretation of evidence.

**How It Works:** Data types are displayed in the left navigation bar, where you can filter evidence, preview files with ease of access and quickly export or tag them as you see fit.

**6. Recover Deleted Files**

**Description:** Autopsy recovers files, file fragments and various sorts of meta information by analyzing file system and through carving the data.

**Purpose:** To recover evidence in which suspects may have tried to hide or destroy.

**How it Works:** Restored items are listed under the "Deleted Files" section, making it possible to review and export them.

**7. Generate Reports**

**Description:**Investigators can generate comprehensive reports that summarize findings, artifacts, timelines and the tagged evidences.

**Purpose:**Used to create an organized record in case of legal action and for stakeholder reporting.

**How It Works:** From **"Reports"** menu, report format and content are chosen by the user before downloading the final document.

### 3.12.3 Limitations of Autopsy

**1. Processing Time for Large Datasets**

Time to process large disk images is considerable, particularly if multiple ingest modules are activated.

**2. Resource Intensive**

Autopsy uses up a lot of resources (CPU, RAM), so its slower on lower end machines.

**3. Learning Curve for Advanced Operations**

Very technical specifications using regex searches or configuring custom modules may need previous experience in forensics.

**4. Limited Mobile Device Support**

Mobile forensics is not as full-featured as dedicated tools such as Oxygen or Cellebrite.

**5. Dependence on File System Compatibility**

Uncommon or closed-form file systems are often not yet well supported.

**6. Incomplete Deleted File Recovery**

The quality of the recovery is a function of file system behavior and degree of subsequent write activity.

**7. No Real-Time or Live System Analysis**

Autopsy was designed to be an end-to-end platform with no support for live or real-time forensics.

**8. Limited Reporting Customisation**

More complex formatting or visual report may need extra tools.

**9. Community-Driven Support**

Support is also community-driven, so you might not find a quick answer to your problems.

### 3.12.4 Limitation:

**Processing Time for Large Datasets**

**Description**: It can take a lengthy amount of time to analyse sources of Big data, e.g. multi-terabyte disk images, particularly if more than one ingest module (keyword search, hash lookup) is turned on. The rate of processing is a function of the resource allocation and the complexity of analysis.

**Impact**: Slows down investigations when time is of the essence, investigators have to prioritise modules or work with high-performance hardware (Mitigation).

**Resource Intensive**

**Description:** Autopsy requires high system resources (CPU, RAM and disk space) when processing large cases or multiple ingest modules simultaneously. Sarcastic This sort of thing can make low end systems slow and unstable under load.

**Impact:** Users will require very powerful hardware (multi-core processor, 16+ GBs of RAM) to work efficiently for analysis and this could become expensive for smaller departments or individual researchers.

**Learning Curve for Advanced Features**

**Description:** While it is possible to use Autopsy`s graphical interface quite simply, advanced features such as building custom modules, searching with regular expressions or doing timeline analysis require significant forensic knowledge and training. Beginning users could find it a bit challenging to configure or understand the results.

**Impact:** Could be trained or knowledge for digital forensic basics, that not such easy to access

by beginners nor non-specialists.

**Limited Mobile Device Support**

**Description:** Autopsy does mobile device dumps (backups for Android or iOS), but they are not as powerful as full-featured mobile-analyzer tools such Oxygen or Mobile Forensic. It may not work with encrypted and proprietary mobile formats.

**Impact:** Additional resources required for full mobile forensics, which elevates cost or increases workload.

**Dependence on File System Support**

**Description:** Autopsy has general or no support at all for the common file systems and limited or virtually no support for unusual, proprietary, or newer file systems. Unsupported formats may interrupt analysis.

**Affect:** The user would require other utilities to be used or it is necessary to convert the files in suitable format for them; thus making it complex job.

**Incomplete Deleted File Recovery**

**Description:** Though Autopsy can recover files removed by file system metadata or data carving, the recovery may not be complete, especially if the tested data is overwritten or fragmented. This is a hack that will only works under certain file systems and on some delete operations.

**Impact:** Evidence of a critical nature could be retrievable, which would not necessarily prove the case.

**Limited Real-Time Analysis**

**Description:** This tool is intended to be used for post-mortem action on a data source (disk or directory) used during an incident and not live response. It cannot analyze a running system or volatile memory in real-time.

**Impact:** When under investigation, some work and equipment is needed from another side of the toolbox (volatile memory forensics) for live specimens to extend incident response.

**Reporting Customisation Restrictions**

**Description:** Autopsy 8 Reporting Overview and Vision Abstract Body: Methodology Although Autopsy supports report customization (HTML, PDF, Excel) the reporting interface is very flexible, without the need to code with limited formatting options or include complicated visualizations**Impact:** For legal or business use, manual post processing of reports is necessary when work load increases.

**Community-Driven Support**

**Description:** As an open-source tool, Autopsy does not have dedicated commercial support but community support. New features could be so badly documented that they didn't exist, and bug fixes or improvements were only made according to the input of the community.

**Impact:** Users receive delayed solutions or are forced to seek answers on community forums that are less reliable than commercial tool support.

### 3.12.5 Work Process Screenshot Step by Step:

Open Autopsy Tool in Windows and create a new case for a new case

**Create a new case Details**


***Figure 55:*** **Create a new case Details**

**Select host**

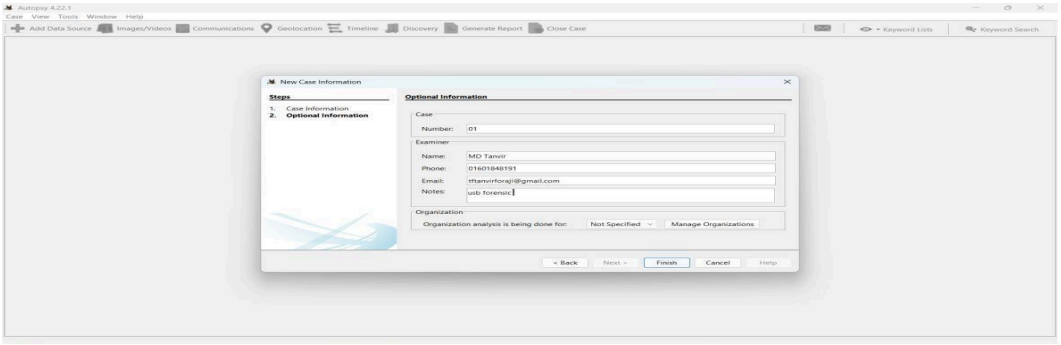



***Figure 56:*** **Select host**

**Select Data source:**

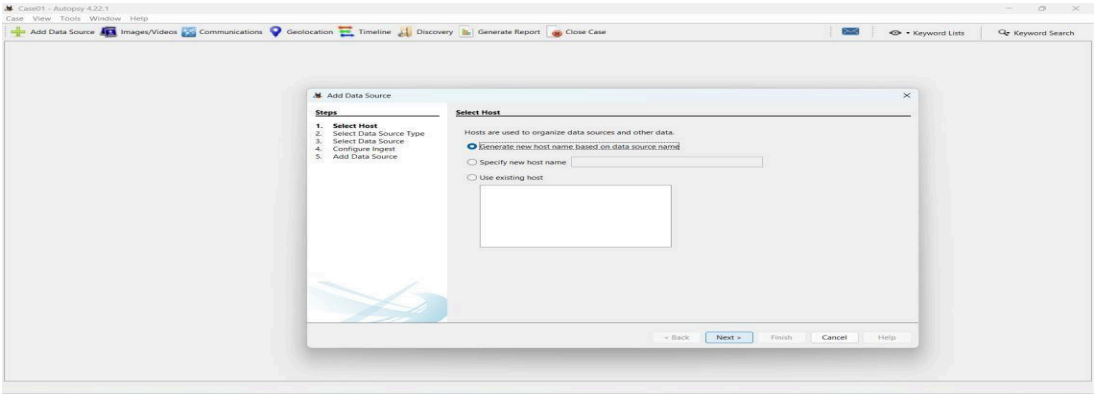



***Figure 57:*** **Select Data source**

**Select Data source:**

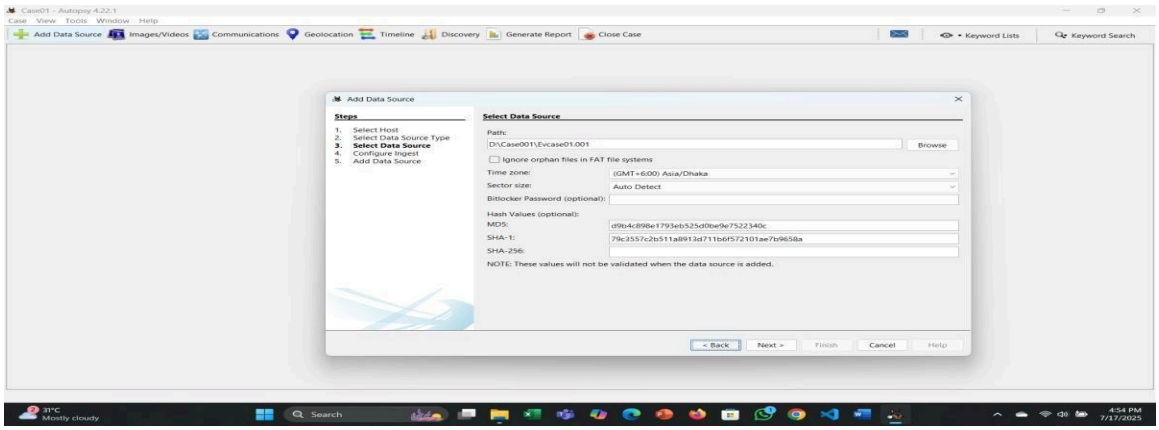



***Figure 58:*** **Select Data source**

**Configuration Inges**

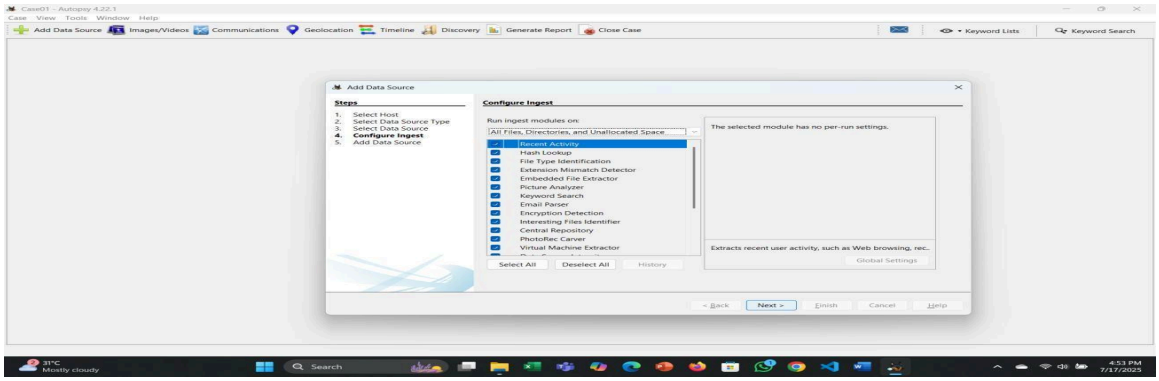



***Figure 59:*** **Configuration Inges**

**Creating this case for forensic analysis to identify the evidence**

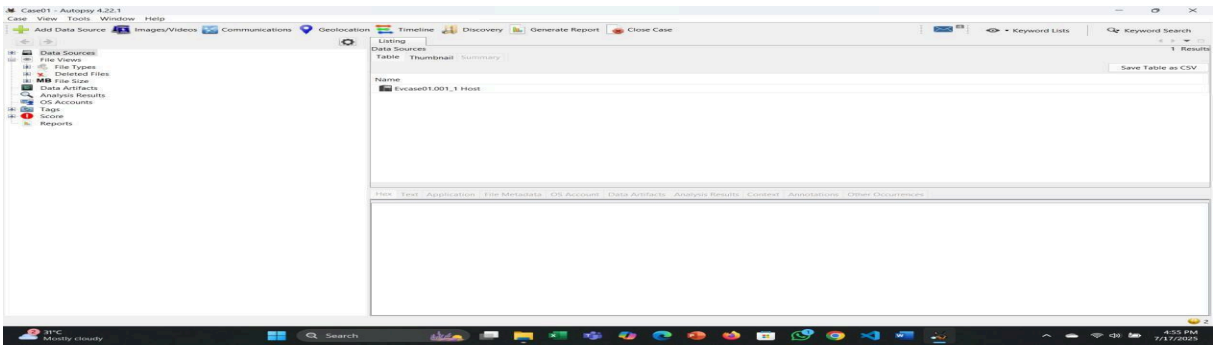



***Figure 60:*** **Creating this case for forensic analysis to identify the evidenc**

### 3.13 FTK Imager:

**Description:** FTK Imager is a well known digital forensics tool by Access Data. It is useful for data preview, imaging and analysis of forensic investigations. The ability to create forensic images of computer hard drives, storage devices and digital media without altering the original data. It retains such evidence in its original form, while preventing the write-blocked content from being tampered with. The software supports multiple image types such as DD, E01, and AFF. 'protocol') : in a way that is forensically sound Allows examiners to view and / or extract data as : deleted files, file systems, and partition structures. User-Friendly Design Items like memory capture, hash verification (MD5 or SHA-1), and the ability to export files and folders for further analysis are included right in FTK Imager. It's an essential stage of digital forensics, because law enforcement, cybersecurity employees and forensic analysts use it in their work to assist them collect and organize digital evidence toward a court case.

#### 3.13.1 Work Process:

**Case Creation and Setup:**

Forensic examiners create a case in FTK, and specify things like case number, evidence number and the examining person's details.

Forensic images are most commonly collected using FTK Imager prior to analysis in FTK. It is executable from a forensic workstation or can be installed on and executed from a USB drive on a live system.

**Data Acquisition:**

**Disk Imaging:** FTK Imager allows users to create bit-by-bit copies of disks and disk partitions, ensuring all data is preserved while reducing time spent acquiring evidence. It is capable of examining RAW and DD images as well as E01 (EnCase image file format) images and AFF (Advance Forensics Format - used by The Sleuth Kit).

**Source Selection:** Users will need to choose what the source (ie physical drive, logical drive or image file) and where it is going.

**Hash Verification:** FTK Imager generates an MD5, SHA1 or SHA256 hash value to validate and verify the integrity of the image with the original source.

**Live RAM Acquirement:** FTK Imager collects the contents of system memory (RAM), such as running processes, network connections and encryption keys that are essential for analysing live systems.

**Previewing Data:** FTK Imager offers file, folder and deleted data previewing in advance of imaging, to assist the forensic technician in choosing which content to image.

► **Data Processing and Indexing:**

FTK also relies on a centrialised database to presort and index data, which makes searching or analysing it much faster.

Information is classified and artifacts are parsed, including emails, documents and media.

► **Data Processing and Indexing:**

FTK also relies on a centrialised database to presort and index data, which makes searching or analysing it much faster.

Information is classified and artifacts are parsed, including emails, documents and media.

FTK's use of a database model guarantees its stability – the program does not suffer from crashing commonly experienced with memory-based tool.

► **Analysis:**

➢ **File analysis:** FTK Imager enables users to analyze forensic images, view file structure, generate zeroed data and recover deleted files using data mining.

➢ **Advanced Analysis:** on the FTK side there are advanced e-mail analysis, parsing (keywords, headers or IP addresses), decryption support and password cracking as well as graphic depictions of data relationships in timelines and cluster graphs.

➢ **FULL TEXT SEARCH & FILTERING:** With FTK keyword searches and filters quickly return relevant hits across all types of investigation data.

➢ **Mobile and Database Forensics:** FTK is capable of ingesting mobile extractions and analyzing databases, to include extracting information from apps such as WhatsApp or Telegram.

► **Reporting and Collaboration:**

FTK generates customisable reports of the findings which may be exported for export to court or as part of stakeholder communication.

FTK Web Viewer provides networked, real time access to case files on multiple cases for colleagues.

FTK Enterprise and FTK Central supports remote endpoint collection, along with shared analysis for massive investigations.

► **Documentation and Chain of Custody:**

FTK Imager records everything, including hash reports, to preserve a defensible chain of custody.

FTK guarantees that all actions conducted are up to court-approved legal standards of evidence introduction

### 3.13.2 Key Features of FTK Imager:

**FTK Imager:**

- **Forensic Imaging:** Ensures that the forensic data is an exact bit-for-bit copy of the original Evidence, created in E01 or DD ρaw Format All existing %data including deleted files and un-allocated space.

- **Hash calculation and verification:** MD5, SHA-1, and SHA-256 are available to check data integrity.
- **Live RAM Analysis:** Acquires volatile memory, providing details of running processes, network connections and encryption keys.
- **Data Carving:** Retrieves files with no metadata in forensic images
- **File Analysis:** You can Preview and Extract the files, metadata & hidden as well as deleted content without altering the source evidence
- **Portability:** Runs from a USB drive so you can perform flash memory diagnostics.
- **Friendly interface:** Easy to use for both beginners and experts
- **Free:** FTK Imager is free to download and use**.**

**FTK Forensic Toolkit:**

- **Enhanced Data Recovery:** Retrieves data from open, password-protected or missing files using exact algorithms
- **Analytics:** Everything but the kitchen sink for processing large data sets, different types of files, and mobile extractions with other tools that help in email analysis, registry parsing, or even database forensics.
- **Decryption and Password Recovery:** Decrypts files and retrieves keys for more than one hundred applications.
- **Parallel processing:** Utilizes multi-core CPU and four processing workers for fast results.
- **Visualisation Tools:** Timelines, and cluster graphs, and pie charts used to interpret the data are offered**.**
- **Malware:** Includes Cerberus for automated malware analysis (triage) and scoring of threats.,,.setVerticalGroup Malware Detection(KeyEvent push-button name: Malware
- **Explicit Image Recognition:** It automatically determines pornographic images and trains on a database of 30,000 adult images to help cases involving child sexual abuse materials.
- **OCR Engine:** Easily convert images into text supporting all major languages and improve the OCR processing time by up to 30%
- **Interoperability:** Operates smoothly with third-party mobile extraction tools and other forensic programs.
- **Scale:** The Remote Collect feature in FTK Enterprise and FTK Central enable investigations of virtually unlimited size to be collaborated.
- **Wide range of file system support:** Investigates DMG (Mac OS and Linux disk image format), Ext4, exFAT, VxFS, VHD, YAFFS as well as other types acros Windows, macOS. Linux & Unix.

**Limitations of FTK and FTK Imager**

**FTK Imager Limitations:**

- **Limited forensics capabilities –** Although great for imaging, FTK Imager does not have as much analysis powers compared to the rest of the FTK suite (e.g. detailed email parsing or visualizations). B) Analysis (for more advanced testers who have access to

FTK or other free tools)

- **Windows Only:** If you are a user who is only using Windows, then FTK Imager should be the right tool for you!You cannot install FTK Imager on Linux machines or macOS X. You can still image devices from these platforms. This restricts its use to non-Windows systems.
- **Compatibility:** May have problems with new FS or encrypting method, user must follow version that fit his OS and minimize problem potential causes by TightVNC.
- **Live Imaging:** Live imaging, especially RAM acquisition, could hit the performance of the live system and requires a good amount of resource to avoid interruption.
- **No Mobile Data Acquisition:** FTK Imager cannot be used to acquire data from mobile devices — thus, users should connect FTK with other third party tools for mobile forensics solutions.
- **FTK Forensic Toolkit Limitations:**
- **High hardware needs:** FTK requires powerful hardware (especially for distributed processing) which might be a bottleneck for small organizations.
- **Price:** FTK's pricing is not public but, unlike FTK Imager, FTK does have a cost associated with it after you have tried the tool which will make some of people out there feel that using this tool is expensive to do so.
- **Learning curve:** Its deceptively simple interface belies FTK's complexity, and anyone using its more advanced features must first undergo extensive training--especially those without technical expertise.
- **Lack of a Timeline View:** As FTK lacks a proper timeline view, you are limited in your ability to put events together on the time line compared to tools such as Magnet AXIOM.
- **Disjointed Registry Viewer:** Doing the Registry examination requires a separate application (Registry Viewer), which isn't always as practical as being built in.
- **Hashes Vulnerabilities :** Old hashes of FTK like MD5 or SHA-1 are theoretically risked for collisions even legal proceedings may have suspects with these hashes, but this happens rare due to the new storage size.
- **Startup Time is Slow:** It's not uncommon to hear users bitching about FTK taking forever to open, which could negatively effect a time sensitive investigation.

### 3.13.4 Work process screenshot:

**Open FTK imager:**

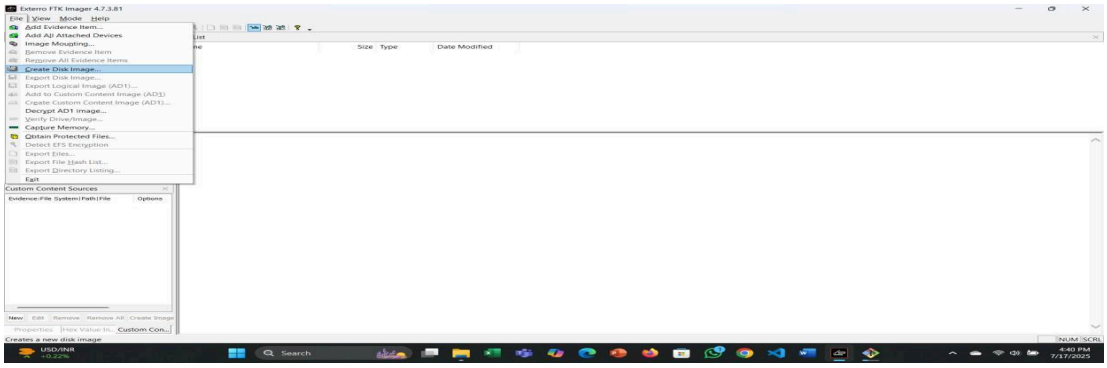


*Figure 61: Open FTK imager*

**Create a Disk image:**

*Figure 62: Create a Disk image*

**Select Source Evidence type**

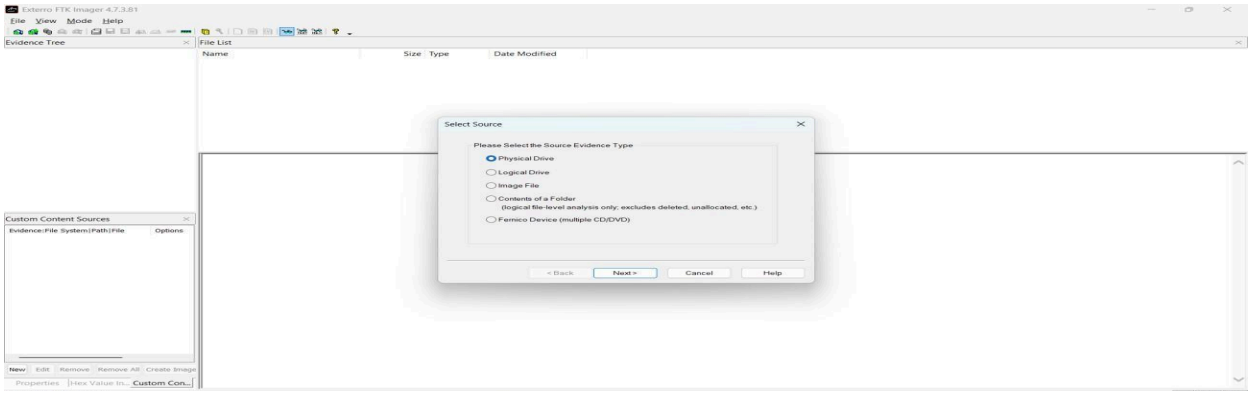


*Figure 63: Select Source Evidence type*

**Select the source of Drive:**

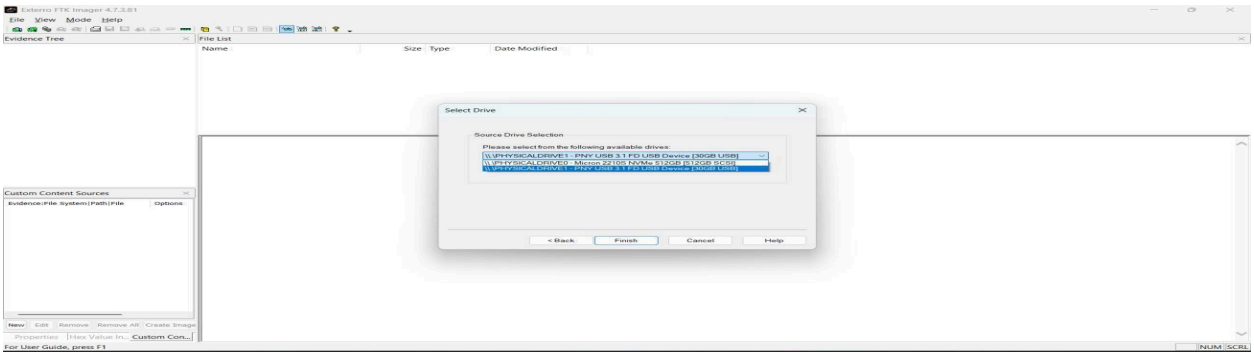


*Figure 64: Select the source of Drive*

**Select the source of the image file:**

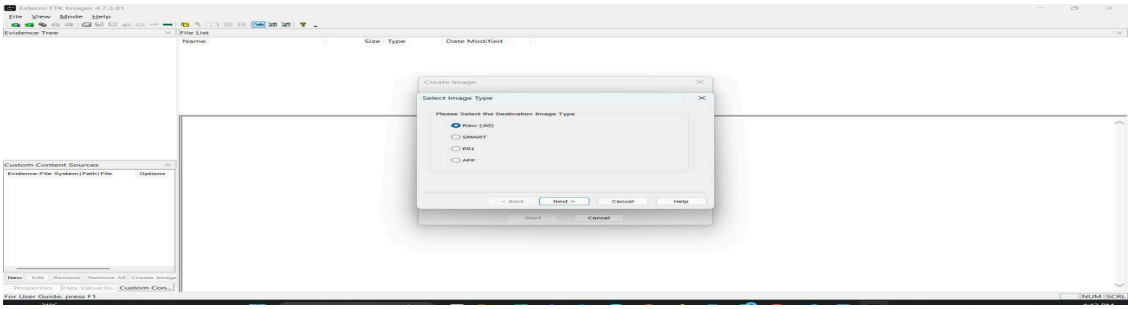


*Figure 65: Select the source of the image file*

**Select the Destination Image type:**

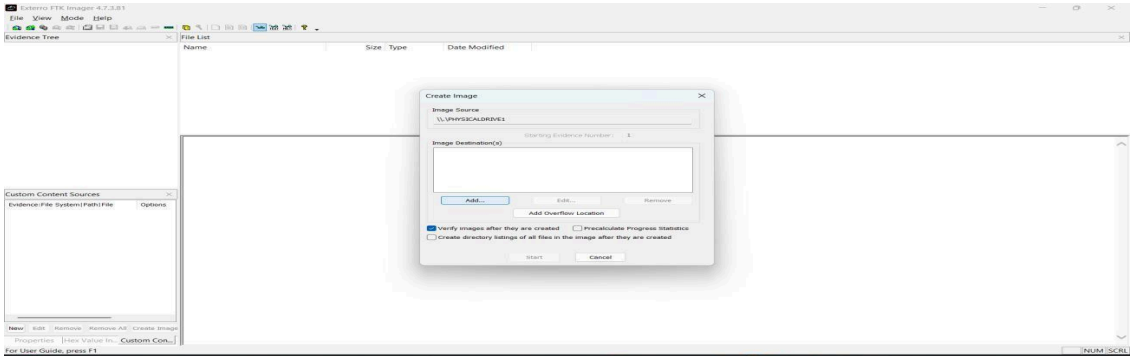


*Figure 66: Select the Destination Image type*

**Select the evidence Item information and the examiner's name.**

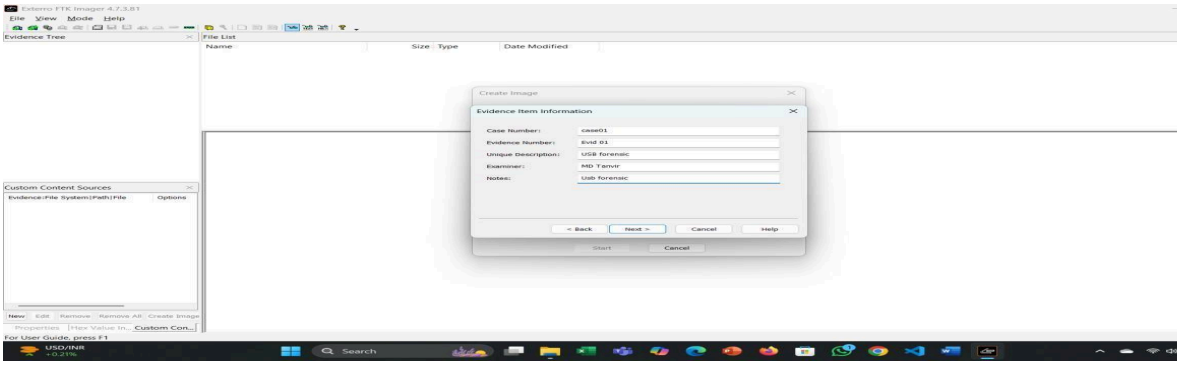


*Figure 67: Select the evidence Item information and the examiner's name*

**Select the image Destination and select the folder. Image Fragmentation size selecs:**

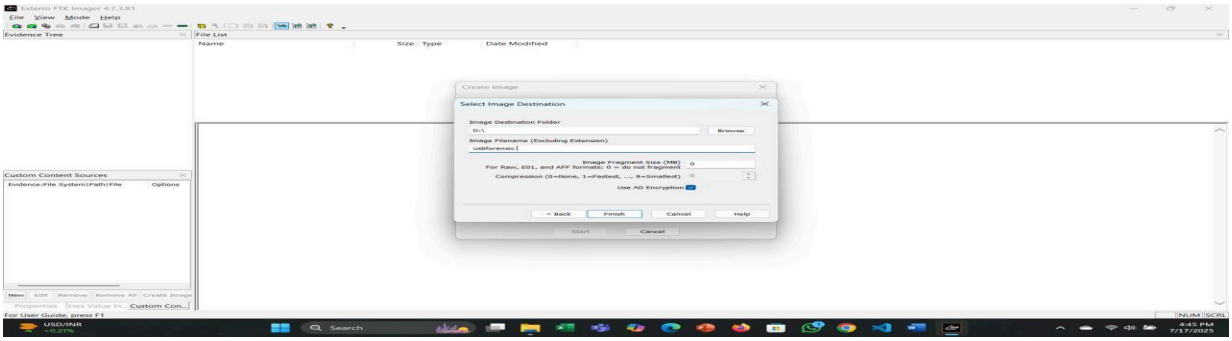


*Figure 68:* **Select the image Destination and select the folder. Image Fragmentation size selects**

**Start creating the Image for the evidence disk:**

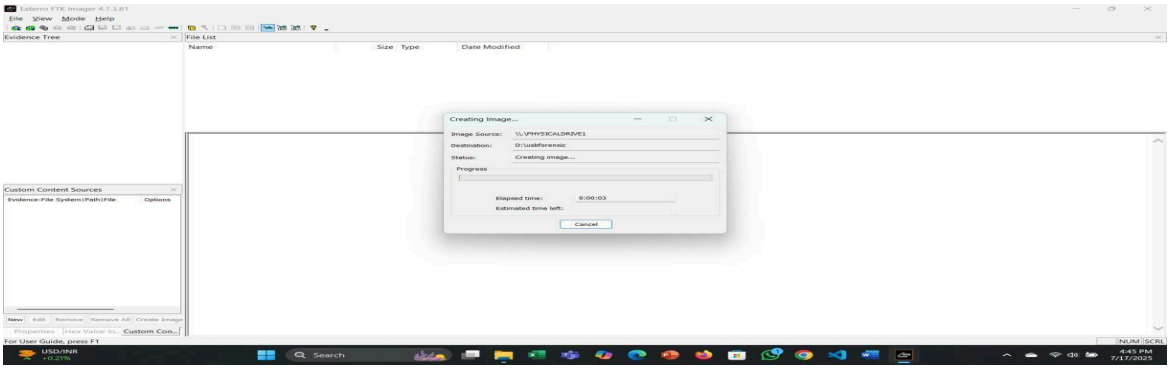


***Figure 69: Start creating the Image for the evidence disk***

# CHAPTER 4
# INTERNSHIP SUMMARY

## 4.1 Overview:

As a Technical Executive in **Backdoor Private Limited,** one of the largest cybersecurity and IT solutions company in Bangladesh offered the massive space to integrate my **theoretical knowledge on Information Technology** with practical works at its best. During this time, I worked with two mentors: **Tahsina Sadia Meem**, as Forensic Analyst, and **Shuvo Sarkar** as SOC Analyst We accomplished practical projects which strengthened my skills in **cyber security and digital forensics.**

Goals of the internship were to utilize IT concepts in everyday tasks, including system updates, defect tracking, and network security operations, as well as necessary soft skills how to be a team player or one who interacts professionally with others while technically solving issues.

During the course I have used a variety of tools such as Nmap, Whois, SpiderFoot, Oxygen Forensic Suite Detective Edition (2011) Lite v4.6.5.15 Autopsy Digital Forensics Tools FTK Imager Nessus OpenVAS Zenmap Scan Fierce Dnsenum DNSMap to conduct Network foot printing, scanning and Digital forensics work. Here, I gained knowledge in host discovery, port scanning, data recovery and threat detection which allowed me to approach cybersecurity challenges with an arsenal of skills as well as the confidence of applied skills.

At Backdoor Private Limited, my advanced preparedness in a cybersecurity career was enabled by the company's proactive threat monitoring and client-centric approach to resolving IT security matters in tandem with their interactive culture -> MDA Copy gave me firm roots.

## 4.2 Achievement:

As an intern with Backdoor Private Limited, I achieved multiple personal goals throughout my stint as a Technical Executive which bettered my experience and understanding of cyber security and IT. I practically applied my theoretical knowledge by learning tools such as Nmap, Whois, SpiderFoot, Oxygen Forensic, Autopsy, FTK Imager and Nessus for tasks ranging from finding hosts and scanning ports to performing vulnerability assessment and digital forensics.

Aided with development work on live projects such as system updates, local computer maintenance and defect tracking; which resulted in improved system efficiency and better organisation security. My hands on experience with network reconnaissance and forensic analysis such as data recovery and evidence preservation also significantly added to my technical knowledge.

Aside from the technical knowledge, I gained invaluable soft skills like efficient Team Work,

professional communication and dealing/ resolving real problems on such a high constraint world. Under Tahsina Sadia Meem and Shuvo Sarkar's supervision, I was mentored and shaped professionally which later helped me stepping in today's challenging IT/Cybersecurity job market with confidence.

### 4.3 Limitations of Internship:

While my hands-on knowledge on cybersecurity and forensics was shaped by my internship Backdoor Pvt Ltd, there were certain challenges that reduced the practicality of learning. One of the main constraining factors was the legal and regulatory barriers to executing penetration tests. Those restrictions kept me from conducting any meaningful offensive security work, and trying to emulate the real internet using Nmap, Nessus or OpenVAS was out of the question.

And I was blocked from running some of SpiderFoot's and my own custom Nmap modules on thegrounds that it might have resulted in network issues; probably company policy. This constraint restricted the configuration to support automated vulnerability discovery and more advanced remediation.

Certain tools also introduced logistical difficulties. For instance:

- The autopsy when ran on big datasets it was very slow.
- FTK Imager offered little data access on mobile devices.
- OpenVAS was difficult to configure and hardware-limited.

The internship was mainly centered around routine like system updates and bug tracking that coupled with high learning curves of tools such as Nessus and Oxygen Forensics limited exposure to larger IT aspects such as solo project completion and cloud security scans.

Despite my challenges with this product, I was able to learn basic network scanning and some digital forensics skills during the internship In addition, it laid the groundwork for me to further develop my vulnerability assessment skills, which is an invaluable component of developing proficiency in a cybersecurity specialization.

### 4.4 Future The Internship:

My position as a Technical Executive at Backdoor Private Limited (BDP) internship has greatly enhanced my career path in areas such as cybersecurity and IT. "I gained practical experience using the tools people use in the industry every day, leading me to launch a career as an entry-level cybersecurity analyst or penetration tester or forensic investigator."

Using what I learned, from both sides, bridged theory with real-world application—like updating systems, monitoring issues and saving data—made me think about Fitbit IT in a more complex way that made me appreciate professional workflows. This practical experience has given me a solid foundation to solve unique problems in the ever-changing IT landscape.

In addition, the internship developed important "soft" skills such as cooperation, professional

speaking and following company policy that are essential for successful interactions within a high-level working environment. The technical proficiencies and soft skills obtained during this internship serve as the basis for a strong career in cybersecurity.

### 4.5 Coverage And Conclusion Of This Internship:

Backdoor Private Limited My role was as a Technical Executive, where it became an eye-opener for me that they made the bridge to which was often just academics information in Cyber Security and Digital Forensics. Throughout the internship, I improved my technical skills and developed practical exposure to core industry tools including Nmap, Whois, SpiderFoot, Oxygen Forensic, Autopsy FTK Imager dnswalk Nessus OpenVAS Zenmap Fierce Dnsenum DNSMap I used these tools to perform network reconnaissance, vulnerability scans and data rescue with some reasonable level of knowledge.

In addition to technical knowledge, the internship had me work on my soft skills like team management, answering adults in a corporate world and solving issues given real-world constraints. While some restrictions - like the prohibition of penetration testing and the running of critical shell scripts – inhibited access to comprehensive security testing, advanced automation etc., I was working on real projects in a collaborative professional environment under mentorship of Tahsina Sadia Meem & Shuvo Sarkar.

This situation not only grew my confidence but also placed me on a very firm footing in the professional sense moving forward (not too long after this I was prepared to pursue much higher level cybersecurity certs) and contributing properly back to digital security as well. The experience and training provided as part of this internship has equipped with the knowledge, expertise and insights necessary for my journey into the challenges of cybersecurity industry.

**Key Word:**

Cybersecurity, vulnerability assessment, penetration testing, VAPT, digital forensics, Security Operations Center, SOC, network reconnaissance, threat detection, incident response, Nmap, Whois, SpiderFoot, Oxygen Forensic, Autopsy, FTK Imager, Nessus, OpenVAS, Zenmap, Fierce, Dnsenum, DnsMap, host discovery, port scanning, data recovery, forensic analysis, SIEM platforms, network security, system updates, defect tracking, malware detection, evidence management, data acquisition, keyword search, timeline analysis, hash verification, subdomain enumeration, DNS queries, proactive security, teamwork, professional communication, problem-solving, industry-standard tools, compliance, threat landscape, data visualization, reporting, file system analysis, live RAM capture, client-focused solutions, scan techniques, TCP SYN scan, TCP connect scan, UDP scan, script scan, port exclusion, fast scan, sequential scanning, top ports, port ratio, DNS resolution, traceroute, ICMP probes, Lua scripts, firewall evasion, domain lookup, IP lookup, ASN lookup, OSINT automation, vulnerability scanning, Greenbone Security Assistant, Network Vulnerability Tests, NVTs, forensic imaging, data carving, hash algorithms, MD5, SHA-1, SHA-256, mobile forensics, cloud extraction, email analysis, web artifacts, Exif data, file type identification, deleted file recovery, chain of custody, report customization, Kali Linux, network mapping, penetration testing frameworks, cyber threats, soft skills, system resources, data integrity, forensic workstation, client organizations, real-world projects, and career preparation.

# REFERENCE


- **Nmap Tools:** https://www.kali.org/tools/nmap/
- **Whois:** https://www.kali.org/tools/whois/
- **Fierce:** https://www.kali.org/tools/fierce/
- **Dnsenum:** https://www.kali.org/tools/dnsenum/
- **DnsMap:** https://www.kali.org/tools/dnsmap/
- **Spiderfoot:** https://www.kali.org/tools/spiderfoot/

- **Nessus :** https://www.tenable.com/ , https://localhost:11127
- **Openvas:** https://www.openvas.org/index.html , https://localhost:9392
- **Zenmap:** https://nmap.org/zenmap/

- **FTK imager:** https://www.exterro.com/digital-forensics-software/ftk-imager

- **Autopsy:** https://www.autopsy.com/

- **Oxygen forensic**: https://digitalintelligence.com/store/products/oxygen-forensic- detective

# Appendix: A

## APPOINTMENT LATER

BACKDOOR
IN SEARCH OF ROOTS

Flat- 9(B), House-30, Road-42,
Gulshan-02, Dhaka 1212, Bangladesh.
www.backdoor.com.bd
info@backdoor.com.bd
+880 2 4881216-9

Ref: BPL/AL/007125

Date: 14/09/2025

Md. Badiujjaman Badhon
Khagan Bazar, Daffodil Road, Dhaka
Phone: +8801724218266
E-mail: badhon.cyber@gmail.com

Subject: **Internship (Cyber Security) in Backdoor Private Ltd.**

Dear Md. Badiujjaman Badhon,
Backdoor Private Ltd. is pleased to appoint you as an intern (Technology Department). Your internship shall be for a period of three (03) months effective from 16th September, 2025 under the following terms and conditions:

1. You will report to respective Tahsina Sadia Meem, Forensic Analyst of Backdoor Private Ltd. and will work under her guidance and supervision.

2. Your working hours will be 10:00 AM to 6:00 PM from Saturday to Thursday. You may need to work extensive office hours if required.

3. You will conduct yourself in a manner that is not prejudicial to the company's interest. You have to follow all the standard practices of the company according to its policies.

4. During the period, you might be allowed a maximum of 3 (three) days leave for emergency purposes, subject to the approval of your team leader.

5. You will be assigned on the departments as per the internship plan, and upon completion of the internship period, you are required to submit a report on your completed assignment to the technical department or Forensic Analyst Tahsina Sadia Meem.

6. You will be given a remuneration of BDT-5000/- only per month.

We look forward to working with you in the coming days.

Thank you,

General Manager (GM)
Backdoor Private Ltd.

I, Md. Badiujjaman Badhon, confirm acceptance of your offer of employment based on the terms and conditions contained here in above which have read and understood.

Signed: Badiujjaman Date: 16.09.25

Head Office: 17/B/3, Monipuripara (2nd Floor), Shangshad Avenue, Dhaka-1215, Bangladesh

# Appendix: B

# Clearance