RECONNAISSANCE

Group Members
Ajmal
Ambadi Kurup SG
Archana SR
Aromal Kurup SG

Contents

Summary

The phase 2 of the CSA project focuses on thorough reconnaissance of the assigned target environment, building upon the foundational understanding gained in Phase 1. The primary objective was to gather as much intelligence as possible about the target system using both passive and active information-gathering techniques. This process included identifying the target's open ports, services running, server version, potential technologies in use, and any exposed directories or subdomains.

We used industry-standard tools and methodologies to extract detailed insights that could aid in further penetration testing phases. Each team member contributed specific tasks as outlined in the work allocation table

This document serves as a formal submission of all reconnaissance findings, methodologies used, and work distribution. It will serve as a baseline for the subsequent phases of the Vulnerability Assessment and Penetration Testing (VAPT).

Scope

The scope for this assessment includes;

- Passive information gathering.
- Active information gathering.
- Identifying open ports and services.
- Network scanning and enumeration.
- Collecting server and technology details
- Work allocation table.

Out of scope

The following were **out of scope** for this phase;

- Exploitation or active attacks.
- Action that may alter, damage, or disrupt the target environment.
- Social Engineering or phishing attempts.
- Scanning systems outside the assigned target ip.
- Performing Denial of service (DoS) attack.
- Accessing or extracting sensitive user data or credentials

Target IP

The Target Ip for recon is **157.245.111.124**

Work Allocation Table

SL NO	NAME	DATE	IP ADDRESS	CONTRIBUTION
1	Ajmal			
2	Ambadi Kurup SG			
3	Archana SR			
4	Aromal Kurup SG			

1. Passive Reconnaissance

Passive reconnaissance is the process of gathering information about a target without directly interacting with it. It relies on publicly available sources like WHOIS records, DNS data, search engines, and social media. Since it doesn't touch the target system, it's stealthy and less likely to trigger security alerts.

1.1   WHOIS Analysis: IP Range 157.245.0.0/16

- WHOIS analysis is a passive method used in cybersecurity.

- It gathers information about IP addresses, domains, or networks.

- It helps identify the owner or organization behind the target.

- It provides contact details and registration history.

- It does not involve interacting with the target system.

- It is useful for mapping infrastructure and planning further steps.

```
┌──(archana㉿archana)-[~]
└─$ whois 157.245.111.124
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       157.245.0.0 - 157.245.255.255
CIDR:           157.245.0.0/16
NetName:        DIGITALOCEAN-157-245-0-0
NetHandle:      NET-157-245-0-0-1
Parent:         NET157 (NET-157-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   DigitalOcean, LLC (DO-13)
RegDate:        2019-05-09
Updated:        2020-04-03
Comment:        Routing and Peering Policy can be found at https://www.as14061.net
Comment:
Comment:        Please submit abuse reports at https://www.digitalocean.com/company/contact/#abuse
Ref:            https://rdap.arin.net/registry/ip/157.245.0.0


OrgName:        DigitalOcean, LLC
OrgId:          DO-13
Address:        105 Edgeview Drive, Suite 425
City:           Broomfield
StateProv:      CO
PostalCode:     80021
Country:        US
RegDate:        2012-05-14
Updated:        2025-04-11
Ref:            https://rdap.arin.net/registry/entity/DO-13


OrgTechHandle: NOC32014-ARIN
OrgTechName:    Network Operations Center
OrgTechPhone:  +1-646-827-4366
OrgTechEmail:  noc@digitalocean.com
OrgTechRef:     https://rdap.arin.net/registry/entity/NOC32014-ARIN

OrgAbuseHandle: DIGIT19-ARIN
OrgAbuseName:   DigitalOcean Abuse
OrgAbusePhone:  +1-646-827-4366
```

```
OrgAbuseEmail:   abuse@digitalocean.com
OrgAbuseRef:     https://rdap.arin.net/registry/entity/DIGIT19-ARIN

OrgNOCHandle: NOC32014-ARIN
OrgNOCName:    Network Operations Center
OrgNOCPhone:   +1-646-827-4366
OrgNOCEmail:   noc@digitalocean.com
OrgNOCRef:     https://rdap.arin.net/registry/entity/NOC32014-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
```
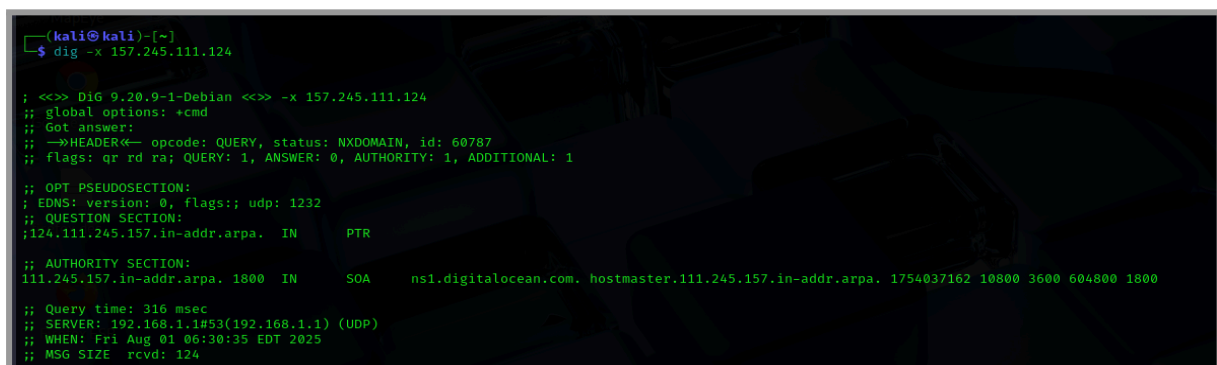
Key Information Extracted:

- **IP Range:**

    - **Range:** 157.245.0.0 – 157.245.255.255

    - **CIDR Notation:** 157.245.0.0/16 (Contains 65,536 IP addresses)

- **Owning Organization:**

    - **Name:** DigitalOcean, LLC

    - **Org ID:** DO-13

    - **Location:** 105 Edgeview Drive, Suite 425, Broomfield, Colorado (CO), 80021, US

    - **Registered Since:** 14-May-2012

    - **Last Updated:** 11-Apr-2025

- **Network Allocation Information:**

    - **NetName:** DIGITALOCEAN-157-245-0-0

    - **NetType:** Direct Allocation

    - **NetHandle:** NET-157-245-0-0-1

    - **Registered On:** 09-May-2019

    - **Last Updated:** 03-Apr-2020

- **Contact Information:**

    - **Routing/Peering Policy:** https://www.as14061.net

    - **Abuse Reporting:** abuse@digitalocean.com, +1-646-827-4366

    - **Technical Support (NOC):** noc@digitalocean.com, +1-646-827-4366

Summary of findings

The IP address 157.245.111.124 is part of a larger block owned by DigitalOcean, a major cloud hosting provider. This suggests the target is likely hosted on a VPS or cloud server.

1.2 Reverse DNS (Dig) Lookup

- **Reverse DNS lookup** is a method used to find the domain name associated with an IP address. Unlike a regular DNS lookup (which maps domain names to IPs), reverse DNS maps an IP back to its hostname. It's commonly used for logging, spam filtering, and network troubleshooting. If no domain is linked to the IP, the lookup may return "NXDOMAIN" or no result.
- A reverse DNS (PTR) lookup for the IP 157.245.111.124 resulted in NXDOMAIN. This indicates that no domain name is currently mapped to this IP address. The authoritative DNS servers are managed by DigitalOcean, which corroborates the WHOIS findings.

```
┌──(kali㉿kali)-[~]
└─$ dig -x 157.245.111.124


; <<>> DiG 9.20.9-1-Debian <<>> -x 157.245.111.124
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 60787
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;124.111.245.157.in-addr.arpa.   IN      PTR

;; AUTHORITY SECTION:
111.245.157.in-addr.arpa. 1800  IN      SOA     ns1.digitalocean.com. hostmaster.111.245.157.in-addr.arpa. 1754037162 10800 3600 604800 1800

;; Query time: 316 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Fri Aug 01 06:30:35 EDT 2025
;; MSG SIZE  rcvd: 124
```

1.3 Shodan Analysis

Shodan is a search engine that allows users to discover internet-connected devices and systems around the world. It indexes information about devices such as servers, webcams, routers, industrial control systems, and IoT devices by scanning their exposed ports and services. Shodan provides details like open ports, software versions, banners, and vulnerabilities, making it a valuable tool for cybersecurity professionals to assess attack surfaces, detect misconfigurations, and conduct reconnaissance. While powerful for ethical hacking and research, Shodan can also highlight how many insecure systems are publicly accessible on the internet.

Shodan analysis involves using the Shodan search engine to gather information about internet-connected devices and services. It helps identify open ports, running services, software versions, and potential vulnerabilities. This passive method is useful in reconnaissance to understand a target's exposure without direct interaction.

General Information

- **Cloud Provider:** DigitalOcean
- **Cloud Region:** in-ka (India - Karnataka)
- **Country:** India
- **City:** Doddaballapura
- **Organization:** DigitalOcean, LLC
- **ISP:** DigitalOcean, LLC
- **ASN:** AS14061

Open Ports

- Port 80 (HTTP)
- Port 111 (RPC)
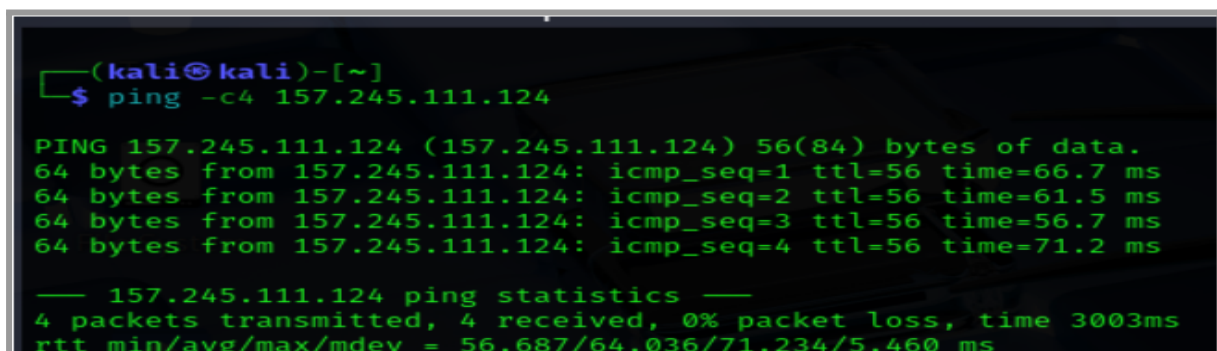
Service on Port 80

- **Service:** Apache httpd 2.4.41
- **Message:** Apache2 Ubuntu Default Page: It works
- **Last Seen:** August 1, 2025
- **Headers (Observed):**
    - **Content-Length:** 10918
    - **Content-Type:** text/html
    - **Server:** Apache/2.4.41 (Ubuntu)
    - **Vary:** Accept-Encoding

2. Active Reconnaissance

Active reconnaissance involves directly interacting with a target system to gather information such as open ports, running services, and operating system details. Unlike passive recon, it sends probes or requests to the target, which can be detected by security systems. Tools like Nmap, traceroute, and telnet are commonly used, making it effective but potentially noisy during penetration testing.

2.1 Ping

The ping command is a basic network tool used to test the reachability of a host (IP address or domain) and measure the round-trip time for messages sent. It works by sending ICMP Echo Request packets and waiting for Echo Reply. It helps identify network connectivity issues, delays, or packet loss.

- **Command Used:** ping -c 4 157.245.111.124
- **Target IP:** 157.245.111.124
- **Packets Sent/Received:** 4 transmitted, 4 received
- **Packet Loss:** 0% (no loss)
- **Response Times:**
    - Min: 56.687 ms
    - Avg: 64.036 ms
    - Max: 71.234 ms
- **Result:** Host is reachable and network connection is stable.

2.2 Traceroute

The **traceroute** command is used to trace the path that packets take from your computer to a destination host. It shows each hop (router or gateway) along the way and how long each takes to respond. This helps identify network delays, routing loops, or unreachable points, making it a valuable tool for diagnosing connectivity issues.

```
  ┌──(kali㉿kali)-[~]
  └─$ traceroute 157.245.111.124
traceroute to 157.245.111.124 (157.245.111.124), 30 hops max, 60 byte packets
 1  Unit (192.168.1.1)  2.757 ms  2.663 ms  2.602 ms
 2  10.240.15.124 (10.240.15.124)  47.228 ms  47.171 ms  42.775 ms
 3  172.30.1.130 (172.30.1.130)  54.255 ms 172.30.1.138 (172.30.1.138)  54.134 ms 172.30.1.155 (172.30.1.155)  106.791 ms
 4  125.18.214.137 (125.18.214.137)  46.134 ms nsg-corporate-89.104.187.122.airtel.in (122.187.104.89)  46.075 ms 125.18.214.137 (125.18.214.137)  45.700 ms
 5  116.119.44.252 (116.119.44.252)  81.548 ms  93.114 ms 182.79.153.39 (182.79.153.39)  88.531 ms
 6  dsl-tn-190.97.246.61.airtelbroadband.in (61.246.97.190)  81.026 ms  73.886 ms  64.054 ms
 7  143.244.224.250 (143.244.224.250)  74.330 ms  72.331 ms  63.813 ms
 8  * * *
 9  * * *
10  157.245.111.124 (157.245.111.124)  80.432 ms  72.078 ms  71.548 ms
```

- **Command Used:** traceroute 157.245.111.124
- **Target IP:** 157.245.111.124
- **Total Hops:** 10 (network devices/routers between source and destination)
- **First Hop:** Local gateway (192.168.0.1)
- **Hops 2 to 9:** Include internal ISP routers and transit network (e.g., Airtel, Tata Communications)
- **Final Hop (Hop 10):** Successfully reached target IP
- **Average Latency to Target:** Around 71.5 ms
- **Observation:**
    o All hops responded with valid times (no asterisks, meaning no timeouts)
    o Network path shows progression through private, ISP, and cloud-hosted routers
    o No major latency spikes or routing issues

- **Key Inferences:**
    o **Routing Path:** The path originated from a private network, traversed through an ISP (Airtel), and terminated at the DigitalOcean cloud infrastructure.
    o **Firewalled Nodes:** Hops 8 and 9 were unresponsive, which is common for transit routers configured not to respond to ICMP probes for security or performance reasons.
- **Path Breakdown:**

    o **Hops 1-3:** Internal ISP network

    o **Hops 4-7:** Public ISP backbone and regional routers

    o **Hops 8-9:** Unresponsive transit hops

    o **Hop 10:** Final destination server (157.245.111.124)

2.3 Nmap Scan

The **nmap** (Network Mapper) command is a powerful tool used in cybersecurity to scan networks and discover hosts, open ports, services, and operating systems. It helps identify potential vulnerabilities by revealing what services are running and whether they are properly secured. Nmap is widely used in both network auditing and penetration testing.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn -T4 157.245.111.124

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 11:39 EDT
Nmap scan report for 157.245.111.124
Host is up (0.089s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE    SERVICE       VERSION
21/tcp   open     ftp           OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp   open     ssh           OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
25/tcp   open     smtp          Postfix smtpd
80/tcp   open     http          Apache httpd 2.4.41 ((Ubuntu))
111/tcp  open     rpcbind       2-4 (RPC #100000)
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1022/tcp filtered exp2
1023/tcp filtered netvenuechat
1026/tcp filtered LSA-or-nterm
9898/tcp filtered monkeycom
Service Info: Hosts: ubuntu-s-1vcpu-1gb-blr1-CYBER-03-10-2024-1-01,  ubuntu-s-1vcpu-1gb-blr1-01; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn 157.245.111.124
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 11:44 EDT
Nmap scan report for 157.245.111.124
Host is up (0.011s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Host Status:

- **Status:** Host is up

- **Latency:** Approximately 0.089 seconds

Operating System Information:

- **Hostname(s):**

  o ubuntu-s-1vcpu-1gb-blr1-CYBER-03-10-2024-1-01

  o ubuntu-s-1vcpu-1gb-blr1-01

- **Operating System:** Linux (cpe:/o:linux:linux_kernel)

Port and Service Analysis:

Port	State	Service	Version Information
21	open	FTP	OpenBSD ftpd 6.4 (Linux port 0.17)
22	open	SSH	OpenSSH 8.2p1 (Ubuntu)
25	open	SMTP	Postfix smtpd
80	open	HTTP	Apache httpd 2.4.41 ((Ubuntu))
111	open	RPC	rpcbind 2-4 (RPC #100000)

Filtered Ports:
Common Windows ports including 135, 139, 445, 1022, 1023, 1026, and 9898 were found to be **filtered**, indicating they are likely blocked by a firewall.

2.4 Potential Vulnerabilities Identified via Nmap

1. **Port 21 - FTP (OpenBSD ftpd 6.4):**

   o **Risk:** FTP transmits credentials in cleartext.

   o **Potential Vulnerability:** May be vulnerable to issues like CVE-2019-19521 related to file permissions. Anonymous login might be enabled.

   o **Recommendation:** Disable FTP and use a secure alternative like SFTP.

2. **Port 22 - SSH (OpenSSH 8.2p1):**

   o **Risk:** Older versions can be prone to enumeration or side-channel attacks.

   o **Potential Vulnerability:** CVE-2020-14145 (user enumeration timing attack).

   o **Recommendation:** Enforce key-based authentication and disable password-based logins.

3. **Port 25 - SMTP (Postfix):**

   o **Risk:** Misconfiguration could lead to an open relay for spam.

   o **Potential Vulnerability:** Older versions may be affected by command execution flaws like CVE-2021-33515.

   o **Recommendation:** Restrict relay access and validate email headers.
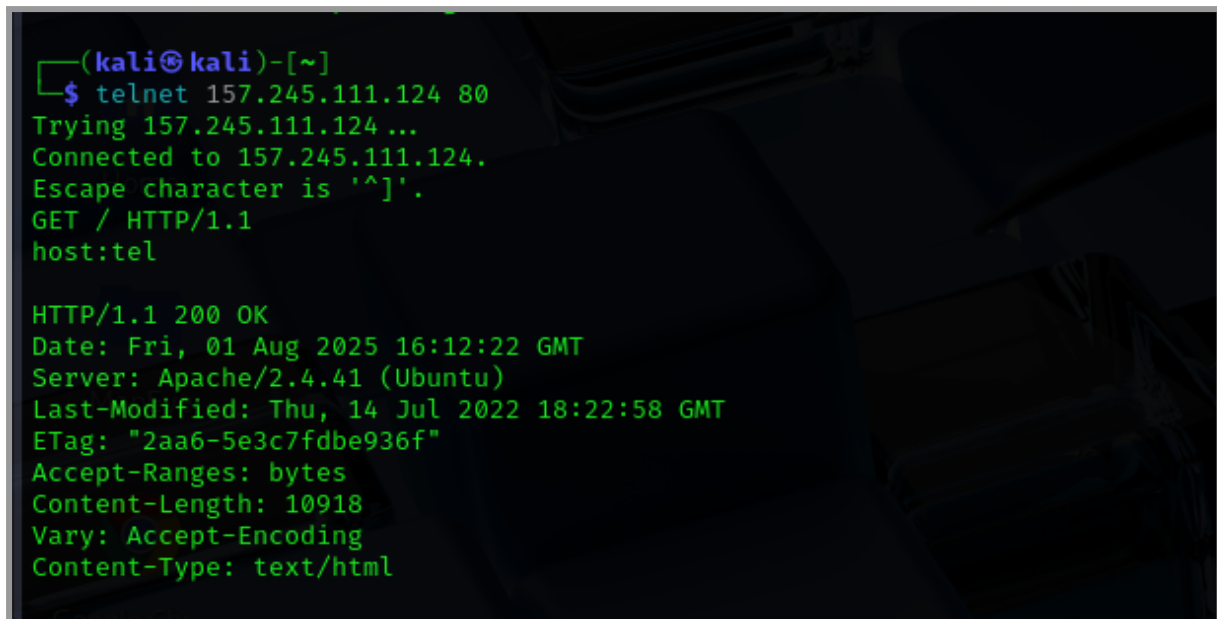
4. **Port 80 - HTTP (Apache 2.4.41):**

   o **Risk:** This version has several known vulnerabilities.

   o **Potential Vulnerabilities:** Includes Server-Side Request Forgery (CVE-2021-40438), buffer overflow (CVE-2020-11984), and a Denial of Service (CVE-2020-9490).

   o **Recommendation:** Update Apache to the latest version and harden server configurations.

5. **Port 111 - RPCBind:**

   o **Risk:** Exposes RPC services, which can be a target for enumeration and exploitation.

   o **Potential Vulnerability:** Can be used to discover other services like NFS and is susceptible to remote crashes (CVE-2017-8779).

   o **Recommendation:** Block external access to this port via a firewall.

2.5 Telnet

The telnet command is a network protocol used to connect to remote computers over TCP/IP, typically on port 23. It allows users to test connectivity to specific ports and interact with services like web servers, mail servers, or routers. Although useful for troubleshooting, Telnet is insecure as it transmits data in plaintext, and is mostly replaced by SSH for secure communication.

- **Command Used:** telnet 157.245.111.124 80

- **Target IP:** 157.245.111.124

- **Port Tested:** 80 (HTTP)

- **Connection Status:** Successfully connected to the server

- **Manual Request Sent:** GET / HTTP/1.1

- **Response Code:** HTTP/1.1 200 OK (successful HTTP response)

- **Web Server:** Apache/2.4.41 (Ubuntu)

- **Response Date:** Fri, 01 Aug 2025

- **Last Modified:** Thu, 14 Jul 2022

- **Content-Length:** 10918 bytes

- **Content-Type:** text/html

- **Other Headers:** Accept-Ranges, Vary: Accept-Encoding, ETag present

- **Conclusion:** Port 80 is open, the server is live, and responding with HTTP 200, confirming successful HTTP service.

3. Conclusion

From the passive and active Reconnaissance done in this phase, following conclusions were derived;

- The IP address 157.245.111.124 is owned by DigitalOcean and hosted in India.

- Passive reconnaissance revealed the hosting provider, server location, and open ports using WHOIS, Reverse DNS lookup and Shodan.

- Apache web server version 2.4.41 running on Ubuntu was identified.

- No direct interaction was made during passive information gathering.

- Active reconnaissance confirmed the host is live and reachable.

- Traceroute showed a successful path with 10 network hops.

- Nmap detected open ports including 80 (HTTP) and 111 (RPC) with service details.

- Telnet verified that the Apache server is actively responding on port 80.

- The combined reconnaissance provided a clear picture of the target's online infrastructure.

This phase sets the groundwork for identifying vulnerabilities in future stages and is strictly limited to non-intrusive activities to ensure the integrity and stability of the target environment.