Offensive Security

Certified Professional

Penetration Test Report

OSID: [OS-XXXXX]

Email: [your.email@example.com]

Exam Date: [Date]

Report Date: [Date]

Table of Contents

1. High-Level Summary

[Your Name / OS-XXXXX was tasked with performing an internal penetration test towards Offensive Security Labs and the OSCP exam network. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks similar to those of a threat actor and attempt to infiltrate Offensive Security's exam network.]

[Your overall objective was to evaluate the network, identify systems, and exploit vulnerabilities while reporting the findings back to Offensive Security. When performing the penetration test, there were several alarming vulnerabilities that were identified. When performing the attacks, you were able to gain access to multiple machines, primarily due to...]

The following systems were successfully exploited during the assessment:

Target	IP Address	Access Level	Method
Independent 1	[IP]	[user/root]	[Brief method]
Independent 2	[IP]	[user/root]	[Brief method]
Independent 3	[IP]	[user/root]	[Brief method]
AD Machine 1	[IP]	[user/root]	[Brief method]
AD Machine 2	[IP]	[user/root]	[Brief method]
AD Machine 3	[IP]	[user/root]	[Brief method]

1.1 Recommendations

[Provide your high-level recommendations here. Patch all identified vulnerabilities. Implement network segmentation. Enforce strong password policies across all systems. Regularly update and patch operating systems and third-party software. Implement proper access controls and the principle of least privilege.]

2. Methodologies

A widely adopted approach to performing penetration testing was used during this exam. The following sections detail the methodology and steps taken during the assessment.

2.1 Information Gathering

The information gathering phase focused on identifying open ports, running services, and potential attack vectors on each target system. Tools such as Nmap were used to perform comprehensive port scans and service enumeration.

2.2 Service Enumeration

Service enumeration was performed to identify specific versions of services and potential vulnerabilities. This included banner grabbing, directory enumeration, and script scanning.

2.3 Penetration

Exploitation was attempted using both publicly available exploits and manual techniques. Each vulnerability was verified and exploited to gain initial access or escalate privileges.

2.4 Post-Exploitation

Post-exploitation activities included privilege escalation, credential harvesting, lateral movement (for AD targets), and collection of proof files (proof.txt and local.txt).

2.5 House Cleaning

All artifacts, shells, accounts, and modifications made during testing were documented. In a real engagement, these would be removed. For the exam, all changes are documented in this section.

[List any files uploaded, accounts created, services modified, or persistence mechanisms established during testing. Include paths and filenames.]

3. Independent Targets

3.1 Target 1 - [IP Address]

Service Enumeration

[Insert your Nmap scan results here]

Port	State	Service	Version
[port]	open	[service]	[version]
[port]	open	[service]	[version]
[port]	open	[service]	[version]

Initial Access

[Describe how you gained initial access to this machine. Include the vulnerability exploited, the exact commands or steps used, and screenshots showing each step.]

Screenshot: [Insert screenshot showing initial access]

Privilege Escalation

[Describe how you escalated privileges on this machine. Include the method used, exact commands, and screenshots.]

Screenshot: [Insert screenshot showing privilege escalation]

Proof

Item	Value
local.txt	[hash value]
proof.txt	[hash value]
IP Address	[target IP]
Hostname	[hostname]

Screenshot: [Insert screenshot showing proof.txt contents and IP address (ifconfig/ipconfig)]

3.2 Target 2 - [IP Address]

Service Enumeration

[Insert your Nmap scan results here]

Port	State	Service	Version
[port]	open	[service]	[version]
[port]	open	[service]	[version]
[port]	open	[service]	[version]

Initial Access

[Describe how you gained initial access to this machine.]

Screenshot: [Insert screenshot showing initial access]

Privilege Escalation

[Describe how you escalated privileges on this machine.]

Screenshot: [Insert screenshot showing privilege escalation]

Proof

Item	Value
local.txt	[hash value]
proof.txt	[hash value]
IP Address	[target IP]
Hostname	[hostname]

Screenshot: [Insert screenshot showing proof.txt contents and IP address]

3.3 Target 3 - [IP Address]

Service Enumeration

[Insert your Nmap scan results here]

Port	State	Service	Version
[port]	open	[service]	[version]
[port]	open	[service]	[version]
[port]	open	[service]	[version]

Initial Access

[Describe how you gained initial access to this machine.]

Screenshot: [Insert screenshot showing initial access]

Privilege Escalation

[Describe how you escalated privileges on this machine.]

Screenshot: [Insert screenshot showing privilege escalation]

Proof

Item	Value
local.txt	[hash value]
proof.txt	[hash value]
IP Address	[target IP]
Hostname	[hostname]

Screenshot: [Insert screenshot showing proof.txt contents and IP address]

4. Active Directory Set

This section covers the Active Directory (AD) environment that was part of the OSCP+ exam. The AD set consists of three machines that form a domain environment. The objective is to compromise the entire AD domain by chaining vulnerabilities across the machines.

4.1 AD Overview

[Provide a high-level overview of the AD environment. Describe the domain name, the role of each machine (Domain Controller, workstation, etc.), and the overall attack path you took to compromise the domain.]

Machine	IP Address	Role	OS
AD Machine 1	[IP]	[Role - e.g., Web Server]	[OS]
AD Machine 2	[IP]	[Role - e.g., Client]	[OS]
AD Machine 3	[IP]	[Role - e.g., Domain Controller]	[OS]

4.2 AD Machine 1 - [IP Address]

Service Enumeration

[Insert your Nmap scan results here]

Port	State	Service	Version
[port]	open	[service]	[version]
[port]	open	[service]	[version]

Initial Access

[Describe how you gained initial access to this AD machine. This is typically the entry point into the AD environment.]

Screenshot: [Insert screenshot]

Proof

Item	Value
local.txt	[hash value]
proof.txt	[hash value]
IP Address	[target IP]
Hostname	[hostname]

4.3 AD Machine 2 - [IP Address]

Service Enumeration

[Insert your Nmap scan results here]

Port	State	Service	Version
[port]	open	[service]	[version]
[port]	open	[service]	[version]

Lateral Movement

[Describe how you moved laterally from AD Machine 1 to this machine. Include credentials obtained, techniques used (pass-the-hash, Kerberoasting, etc.), and evidence.]

Screenshot: [Insert screenshot]

Proof

Item	Value
local.txt	[hash value]
proof.txt	[hash value]
IP Address	[target IP]

Hostname	[hostname]

4.4 AD Machine 3 - [IP Address / Domain Controller]

Service Enumeration

[Insert your Nmap scan results here]

Port	State	Service	Version
[port]	open	[service]	[version]
[port]	open	[service]	[version]

Domain Compromise

[Describe how you compromised the Domain Controller. Include the final privilege escalation or lateral movement step that gave you Domain Admin access. Show the full attack chain.]

Screenshot: [Insert screenshot showing Domain Admin access]

Proof

Item	Value
proof.txt	[hash value]
IP Address	[target IP]
Hostname	[hostname]
Domain Admin	[Yes/No]

4.5 AD Attack Chain Summary

The following summarizes the full attack chain used to compromise the Active Directory domain:

[Step 1: Gained initial access to Machine 1 via [vulnerability/method]]

[Step 2: Obtained credentials for [user] via [method - e.g., credential dumping, Kerberoasting]]

[Step 3: Moved laterally to Machine 2 using [method - e.g., pass-the-hash, WinRM]]

[Step 4: Escalated privileges on Machine 2 via [method]]

[Step 5: Compromised Domain Controller via [method - e.g., DCSync, Golden Ticket]]

[Step 6: Obtained Domain Admin access and retrieved proof.txt]

5. Appendix

5.1 Proof and Local Contents

Target	IP Address	local.txt	proof.txt
Independent 1	[IP]	[hash]	[hash]
Independent 2	[IP]	[hash]	[hash]
Independent 3	[IP]	[hash]	[hash]
AD Machine 1	[IP]	[hash]	[hash]
AD Machine 2	[IP]	[hash]	[hash]
AD Machine 3 (DC)	[IP]	N/A	[hash]

5.2 Tool and Payload Listing

The following tools and payloads were used during the assessment:

Tool	Purpose	URL
Nmap	Port scanning and service enumeration	https://nmap.org

Gobuster	Directory and DNS enumeration	https://github.com/OJ/gobuster
Burp Suite	Web application testing	https://portswigger.net
Metasploit	Exploitation framework (if used)	https://metasploit.com
Linpeas/Winpeas	Privilege escalation enumeration	https://github.com/carlospolop/PEASS-ng
Chisel	Port forwarding and tunneling	https://github.com/jpillora/chisel
Impacket	AD attack tools	https://github.com/fortra/impacket
BloodHound	AD enumeration and attack path mapping	https://github.com/BloodHoundAD/BloodHound
[Other tool]	[Purpose]	[URL]

5.3 Metasploit/Meterpreter Usage

Metasploit was used on the following target(s) during the exam:

[List the target IP(s) where Metasploit was used and the specific module(s) used. Remember: You are only allowed to use Metasploit on ONE target machine during the OSCP exam.]

Target	Module Used	Purpose
[IP or N/A]	[module path or N/A]	[Purpose or N/A]

End of Report