Oliver Jones

ojon6348@gmail.com

Report Date: [dd.mm.yy]

[Client / Project Name]
Penetration Test Report

[Web App / Network / Internal / External Pentest]

v.3.0

COMPANY LOGO

SLOGAN HERE

Testing Dates: [from dd.mm.yy to dd.mm.yy]

CONFIDENTIAL AND PROPRIETARY

This report contains sensitive findings and vulnerabilities intended solely for authorized personnel of [Client Name]. Unauthorized distribution, reproduction, or disclosure is strictly prohibited. Violators may be subject to legal action.

Table of Contents

1 Executive Summary

The tester, Oliver Jones, is tasked with performing an internal penetration test towards OffSec Labs. 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 hacker and attempt to infiltrate OffSec's internal lab systems – the example.com domain. The overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to OffSec.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on OffSec's network. When performing the attacks, Mr. Jones was able to gain access to multiple machines, primarily due to information disclosure, unpatched or outdated applications, and security misconfigurations that allowed information disclosure. During the testing, Mr. Jones had administrative level access to multiple systems. Most systems were successfully exploited and elevated access granted.

1.1 Risk Overview

Severity	**Count**	**Targets**
Critical	x	x
Medium	x	x
Low		

[Critical vulnerabilities could enable full system compromise …]

1.2 Recommendations

Mr. Jones recommends patching the vulnerabilities identified during testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching. Once patched, these systems should remain on a regular patch program to protect additional vulnerabilities discovered at a later date.

2 Methodologies

Mr. Jones utilized a widely adopted approach to performing penetration testing that is effective in testing how well the example.com environments are secure. Below is a breakdown of how Mr. Jones was able to identify and exploit the variety of systems, including how all individual vulnerabilities were found.

2.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, Mr. Jones was tasked with exploiting [an example] network. The specific IP addresses were:

2.2 Network Scope

Standalone Computers:
192.168.124.110,
192.168.124.111,
192.168.124.112.

Active Directory Joined Computers:
192.168.124.206/172.16.124.206 (Single machine with a dual ethernet adapter),
172.16.124.200,
172.16.124.202

Mr. Jones's IP address in the network for the full duration of the engagement was: [***insert Oliver's machine IP here***]. It's important to note that during portions of the engagement where pivoting was required, traffic was being routed through and appears to come from the pivot host's IP. Specifically in the active directory, any communication between Mr. Jones's machine and the internal network is being routed through a pivot on [***insert IP here***].

2.3 Exclusions / Out of scope

During the duration of this test, the following will not be performed:

- DDoS Attacks
- Phishing
- Exploits that are known to cause downtime
- etc.

2.4 Service Enumeration

This portion of the penetration test focuses on gathering information about what services are alive/running on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system provides insight into the network and machines before performing the actual penetration test. In some cases, some ports may not be listed.

2.5 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, Mr. Jones was able to successfully gain access to 5 out of the 6 systems.

2.6 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has been executed (i.e. a buffer overflow), the attacker is able to persist in their access over the target system. Many exploits may only be exploitable once and attackers may not be able to get back into a system after they have already performed the exploit.

Mr. Jones escalated to administrator and root level accounts on 4 machines. In addition to administrative/root access, sometimes persistence methods were sought out in order to return to the systems later on without needing to re-run exploits, allowing for quieter persistence.

2.7 Findings Overview

Vulnerability	**Severity**	**CVSS**	**Target**	**Details**	**Remediation**
SQLi	Critical	9.3	[IP] - Web Portal	SQLi in the login panel allows an attacker to dump the full database, including hashed user passwords etc.	Sanitise user input
RCE	Critical	8.8	[IP] - Port [x]	An outdated version of [x] software allows unauthenticated RCE.	Update / Patch [x] software
XSS	Medium	6.5	[IP] - Admin Login Panel		
Self-XSS	Low	2.1	[IP] - Admin Login Panel		

Several high severity vulnerabilities were found, allowing for an attacker to fully compromise relevant systems.

2.8 Conclusion

Remediation of existing vulnerabilities and patching [x] outdated software would reduce risk by [x %]...

2.9 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left-over is important.

Mr. Jones removed all user accounts and passwords created on the system during the engagement. OffSec should not have to remove any user accounts or services from the system.

2.6 Tester Environment

Below is the information regarding the tools used in Mr. Jones's toolkit during the engagement. Individual executables, scripts and payloads will be listed separately in the report in the relevant sections and uses.

Tool Name	**Version**
nmap	Nmap 7.95
feroxbuster	feroxbuster 2.11.0
evil-winrm	Evil-WinRM shell v3.7
NetExec	Version : 1.4.0; Codename : SmoothOperator
impacket-psexec	Impacket v0.13.0.dev0
Metasploit framework (msfconsole + msfvenom)	metasploit v6.4.64-dev
NetCat	v1.10-50
John the Ripper	John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c
ligolo-proxy	dev

3.1 Target #1 - [IP]

IP Address	Ports Open
[IP address of the machine]	[List open ports]

3.1.1 Initial access

[Describe how Initial Access was obtained]

3.1.2 Service Enumeration

[Initial automated scans for ports and service discovery: nmap, rustscan etc.]

3.1.3 Exploitation

[Detail the exploitation phase. Detail exploitation path all the way from port scan until pre-privilege escalation]

3.1.4 Privilege Escalation

[Detail the steps to obtaining `root` user or `nt authority/system` account on a machine, starting from a low level user account and ending in an interactive shell as the elevated user.]

3.1.5 Post Exploitation

[Talk about the steps taken to revert the machine to its previous state: Restoring backup, placing original files back in their place, removing payloads or persistence methods, removing additional user accounts created during the engagement.

Also mention remediation steps to fix the vulnerabilities or privilege escalation paths discovered, and give general advice to keep the system secure in the future.]

4.1 Target #1 - [IP]

IP Address	Ports Open
[IP address of the machine]	[List open ports]

4.1.1 Initial access

[Describe how Initial Access was obtained]

4.1.2 Service Enumeration

[Initial automated scans for ports and service discovery: nmap, rustscan etc.]

4.1.3 Exploitation

[Detail the exploitation phase. Detail exploitation path all the way from port scan until pre-privilege escalation]

4.1.4 Privilege Escalation

[Detail the steps to obtaining `root` user or `nt authority/system` account on a machine, starting from a low level user account and ending in an interactive shell as the elevated user.]

4.1.5 Post Exploitation

[Talk about the steps taken to revert the machine to its previous state: Restoring backup, placing original files back in their place, removing payloads or persistence methods, removing additional user accounts created during the engagement.

Also mention remediation steps to fix the vulnerabilities or privilege escalation paths discovered, and give general advice to keep the system secure in the future.]

5.1 Target #1 - [IP]

IP Address	**Ports Open**
[IP address of the machine]	[List open ports]

5.1.1 Initial access

[Describe how Initial Access was obtained]

5.1.2 Service Enumeration

[Initial automated scans for ports and service discovery: nmap, rustscan etc.]

5.1.3 Exploitation

[Detail the exploitation phase. Detail exploitation path all the way from port scan until pre-privilege escalation]

5.1.4 Privilege Escalation

[Detail the steps to obtaining `root` user or `nt authority/system` account on a machine, starting from a low level user account and ending in an interactive shell as the elevated user.]

5.1.5 Post Exploitation

[Talk about the steps taken to revert the machine to its previous state: Restoring backup, placing original files back in their place, removing payloads or persistence methods, removing additional user accounts created during the engagement.

Also mention remediation steps to fix the vulnerabilities or privilege escalation paths discovered, and give general advice to keep the system secure in the future.]

6. Active Directory Set

IP Address - [Machine Name]	**Ports Open**
172.16.124.200	[List Ports]
172.16.124.202	[List Ports]
192.168.124.206 / [internal IP, if connected]	[List Ports]

7.1 AD Target #1 - [IP]

IP Address	Ports Open
[IP address of the machine]	[List open ports]

7.1.1 Initial access

[Describe how Initial Access was obtained]

7.1.2 Service Enumeration

[Initial automated scans for ports and service discovery: nmap, rustscan etc.]

7.1.3 Exploitation

[Detail the exploitation phase. Detail exploitation path all the way from port scan until pre-privilege escalation]

7.1.4 Privilege Escalation

[Detail the steps to obtaining `root` user or `nt authority/system` account on a machine, starting from a low level user account and ending in an interactive shell as the elevated user.]

7.1.5 Post Exploitation

[Talk about the steps taken to revert the machine to its previous state: Restoring backup, placing original files back in their place, removing payloads or persistence methods, removing additional user accounts created during the engagement.

Also mention remediation steps to fix the vulnerabilities or privilege escalation paths discovered, and give general advice to keep the system secure in the future.]

8.1 AD Target #1 - [IP]

IP Address	Ports Open
[IP address of the machine]	[List open ports]

8.1.1 Initial access

[Describe how Initial Access was obtained]

8.1.2 Service Enumeration

[Initial automated scans for ports and service discovery: nmap, rustscan etc.]

8.1.3 Exploitation

[Detail the exploitation phase. Detail exploitation path all the way from port scan until pre-privilege escalation]

8.1.4 Privilege Escalation

[Detail the steps to obtaining `root` user or `nt authority/system` account on a machine, starting from a low level user account and ending in an interactive shell as the elevated user.]

8.1.5 Post Exploitation

[Talk about the steps taken to revert the machine to its previous state: Restoring backup, placing original files back in their place, removing payloads or persistence methods, removing additional user accounts created during the engagement.

Also mention remediation steps to fix the vulnerabilities or privilege escalation paths discovered, and give general advice to keep the system secure in the future.]

9.1 AD Target #1 - [IP]

IP Address	Ports Open
[IP address of the machine]	[List open ports]

9.1.1 Initial access

[Describe how Initial Access was obtained]

9.1.2 Service Enumeration

[Initial automated scans for ports and service discovery: nmap, rustscan etc.]

9.1.3 Exploitation

[Detail the exploitation phase. Detail exploitation path all the way from port scan until pre-privilege escalation]

9.1.4 Privilege Escalation

[Detail the steps to obtaining `root` user or `nt authority/system` account on a machine, starting from a low level user account and ending in an interactive shell as the elevated user.]

9.1.5 Post Exploitation

[Talk about the steps taken to revert the machine to its previous state: Restoring backup, placing original files back in their place, removing payloads or persistence methods, removing additional user accounts created during the engagement.

Also mention remediation steps to fix the vulnerabilities or privilege escalation paths discovered, and give general advice to keep the system secure in the future.]

10. Appendix

[Include here Full Nmap scans, console outputs, payloads used, custom scripts etc. (anything too big to include in the main report sections).]