Geisha Proving Grounds

Penetration Test Report

Table of Contents

1. High-Level Summary………………………………………………………………………………………………………………………….3
   1. Recommendations………………………………………………………………………………………………………………..3
2. Methodologies………………………………………………………………………………………………………………………………….4
   1. Information Gathering………………………………………………………………………………………………………….4
   2. Service Enumeration…………………………………………………………………………………………………………….4
   3. Penetration…………………………………………………………………………………………………………………………..4

**System Vulnerable**……………………………………………………………………………………………………………….8

2.4-Report…………………………………………………………………………………………………………………………………..8

1.0-High-Level Summary

An internal penetration test was performed on the potato network in the Offensive Security Proving Ground Labs. An internal test simulates an attacker that is directly connected into the network, in this case through a VPN tunnel.

The purpose of this test was to simulate an attack where the attacker had access to the network, with attempts made to break into a system and then elevate privileges on the machine.

Over-all, the intent was to enumerate the services on the exposed network, determine an attack vector to get access, and then exploit any flaw found within the system.

During the test, it was discovered that the user geisha had a weak password, that was able to be brute-forced. This user was able to be confirmed existing, as the /etc/passwd file was located on the web server hosted on port 7125 under the /passwd directory. Going there started an immediate download of the file, which had the listing of all users on the system.

With the credentials from hydra, access was gained to the system as a local user. This allowed the contents of the local.txt to be available to retrieve. Following this, it was found that there was a base32 file that allowed for root level reading of any file on the system. With this, it was possible to gain the root file contents of proof.txt, /etc/shadow file hashes, as well as a private RSA key for root user.

With this key, it was then possible to login to the device as root, and have complete control of the system.

1.1-Recommendations

It is recommended that a more strict policy for stronger passwords be implemented, to prevent brute force attacks against user credentials. A passphrase of 15+ characters would be a good requirement based on current standards. It is also necessary to remove the /etc/passwd file off of the port 7125 website, as that is visible and accessible to anyone who does a full port nmap scan.

After that, removing the SUID set for base32 would prevent the escalation of privilege that allowed for access to all root files. Removing this would have prevented escalation to root from local user, and protected the system from unauthorized access.

2.0-Methodologies

Below are the methods that were undertaken to break into the device, and ultimately achieve root access on the device.

2.1-Information Gathering

The information gathering portion was mostly null, as the network address of 192.168.191.82 was provided ahead of the pentest commencing.

2.2-Service Enumeration

This was mainly accomplished with nmap scan of the base 1000, followed by a scan of all tcp ports on the device. Through this scanning, the following services were found on the open ports:

21 FTP server

22 Secure Shell Remote access

80 HTTP web service

7080 Empowerid

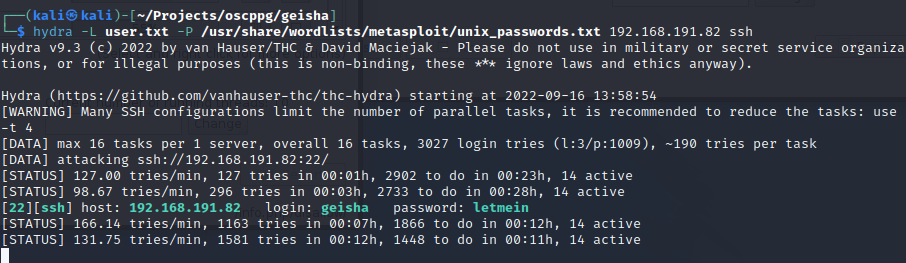
7125 HTTP web service

8088 HTTP web service

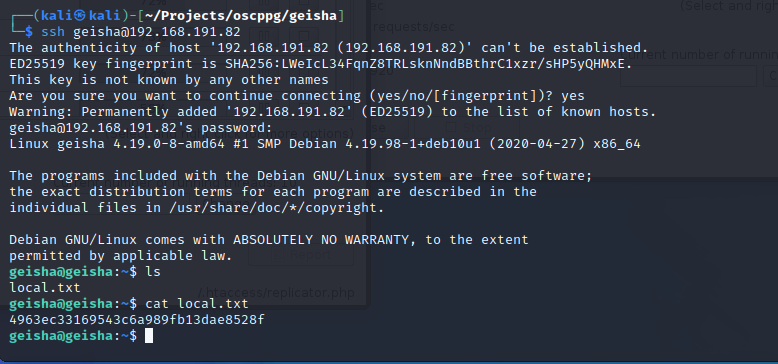
9198 HTTP web service

2.3-Penetration Testing

Performed initial testing with nmap, nikto, dirbuster, zap, and gobuster. During this testing, the various directories for the ports were discovered. The ssh service was brute forced with hydra, which discovered the password was of weak complexity.



With these credentials, it was possible to get local access to the contents of the user. This compromised the local.txt file contents.



Checking for sudo permissions for the user showed that none were available. On checking for SUID enabled files, base32 was found on the list. This file can be used to view any file on the system with root access privileges. This compromised the hashes for root and users on the system, the proof.txt contents in the root directory, and ultimately the private ssh key of id\_rsa of the root user.



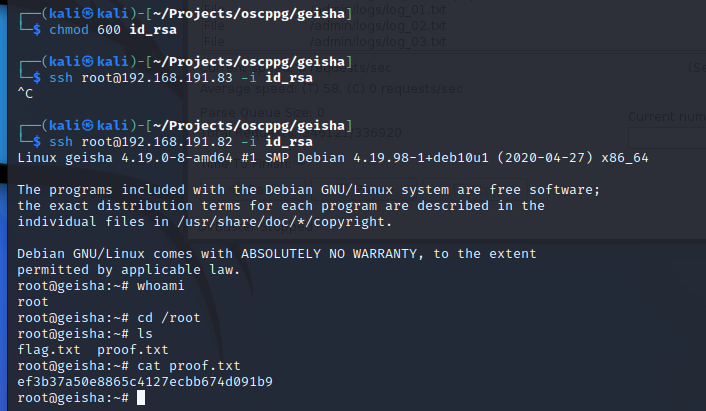
Graphical user interface, text

Description automatically generated

Text

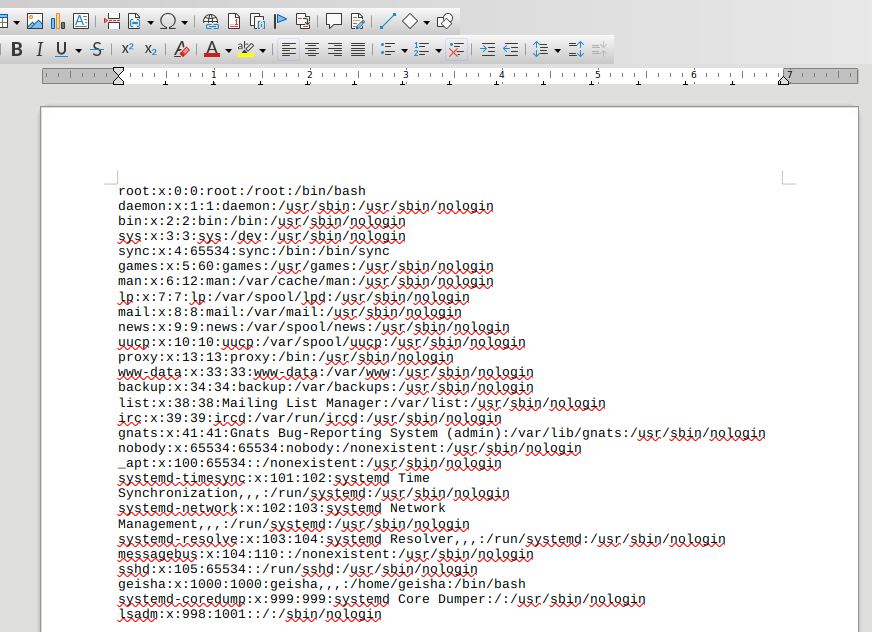
Description automatically generated

With the contents of the id\_rsa ssh private key, it was possible to use it to log in to the system with root access. This allowed for full compromise of the system.



Linpeas.sh was uploaded to check for additional vulnerabilities, but none were found and the file was removed. Checking all the individual port clones of the website found the /etc/passwd file on port 7125.

This would allow for user enumeration and allow for brute forcing any of the users to determine passwords. This is on an outward facing server, which needs to be removed to protect the network.



**System Vulnerable 192.168.191.82**

**Vulnerabilities Exploited:**

Weak password policy allowing for brute-forcing attack

Sensitive file is publicly accessible from the web server

SUID enabled file allowed for root access viewing of any file on the system

**Severity: Critical**

**Proof of Privilege Escalation:**

local.txt: 4963ec33169543c6a989fb13dae8528f

proof.txt: ef3b37a50e8865c4127ecbb674d091b9

2.4-Report: Clean-up

The exploit was performed without needing to upload or modify any files on the system. Linpeas was uploaded to the /tmp folder to validate for any further vulnerabilities, and removed from the directory after the program completed. At this point, the system is in the state it was before the pentest began.