Sunset Noontide Proving Ground

Penetration Test Report

Table of Contents

1.0-High-Level Summary………………………………………………………………………………………………………………………….3

1.1-Recommendations………………………………………………………………………………………………………………..3

2.0-Methodologies………………………………………………………………………………………………………………………………….4

2.1-Information Gathering………………………………………………………………………………………………………….4

2.2-Service Enumeration…………………………………………………………………………………………………………….4

2.3-Penetration Testing………………………………………………………………………………………………………………4

**Service Vulnerable**…………………………………………………………………………………………………………5

2.4-Report…………………………………………………………………………………………………………………………………..6

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 testing, it was found that a version of IRC being run on the network was vulnerable to an exploit that allowed for remote shell connection to the device. With this shell, access to all local level files and folders for the server user were able to be viewed. This resulted in the contents of the local.txt being retrieved from the device.

The root user had default credentials existing for the su command, which was used to achieve root shell into the network system. All assets stored on the system were then available for exploitation.

1.1-Recommendations

The UnrealIRC program being run on the server will need to be updated to a more current stable version to prevent the backdoor exploit from being used to gain access to the system.

The credentials of all users should be changed from any default values, and a password policy should be put in place that requires a passphrase of 15+ characters to keep up with current standards.

The unreal program is in the home directory which is able to be edited by the local user. This should be moved to a new location, to prevent local level users from being able to change the values of the configuration as an exploit path.

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 192.168.191.35 was provided ahead of the pentest commencing.

2.2-Service Enumeration

All available TCP ports were scanned to check for any available attack vector for testing to break into the network. The UDP scan of the top 1000 ports returned no positive results for exploitation. This left it with the following ports as possible exploit vectors:

6667 UnrealIRCd

6697 UnrealIRCd

8067 UnrealIRCd

2.3-Penetration Testing

During the enumeration phase of the engagement, there was found to be only 3 TCP ports open for exploitation, all involving the IRC program being hosted. Based on the version running an exploit script was found that would allow for backdoor access into the system.

Text

Description automatically generated

Running the script allowed for a shell to be created with the server user giving local level access to the files and folders for that user. This allowed for the retrieval of the contents of the local.txt file.

Text

Description automatically generated

The only exploit that presented itself was unable to be performed due to the pkexec binary being removed from the system. Default credentials were then checked within the system to find that the root user password had not been changed from its initial value.

Graphical user interface, text, application

Description automatically generated

This represented a complete compromise of the network, with access provided for all files and folders on the system.

**System Vulnerable 192.168.191.120:**

**Vulnerabilities Exploited:**

Outdated IRC program allowed for backdoor exploit to gain system access

Default credentials for root user allowing for privilege escalation to root.

**Severity: Critical**

**Proof of Privilege Escalation:**

Local.txt: 28a9e475f8c3c16300f59333e0016083

Proof.txt: 4acc925266b07a9fb5472def5dc9587a

2.4-Report: Clean-up

Enumeration scripts were uploaded to identify all possible attack vectors on the system, then removed after the output was received. Exploits were uploaded to the /tmp directory to check for exploitation of outdated binaries, that were unsuccessful due to removed binaries called. These exploits and their generated folders were then removed from the directory.

All information retrieved from the device and found through testing are isolated in their own directory on the attack system and will be removed pending hand-over of all information requested per the terms of engagement for this test.