**puT-TY For The Proofs**

**Dillon Wu**

Executive Summary:

The goal of the penetration testing was to identify all security flaws in the designated scope, to exploit these flaws in such a way that would grant access to the machines, and to find the hash values of proof.txt files. The engagement was carried out with approval from the PWN Challenge #1 client.

The main attack vector was the weak password protection deployed by the company. Publicly available exploits were used to break into the machines and achieve admin privilege in the machines. With admin privilege, I was able to bypass the firewall and obtain the proof.txt files in both hosts. I recommend that your organization work closely with the organization’s security team to upgrade the company’s password protection protocols.

Detailed Findings

\*\*Severity levels are determined according to two primary factors: (1) Ease of security upgrade (2) Cost of not upgrading

**Vulnerability Name:** Anonymous FTP Login

Description: Anonymous FTP Login allows public users to login into the machine’s FTP server using the username “anonymous” and any password. Anonymous login is generally enabled when you have a large number of users that all need to access similar files. Using this vulnerability, I was able to get into the machine with a meterpreter session.

Severity: 3/10; Anonymous login should be disabled unless there is a good reason to keep it.

Affected Hostname: 10.20.160.41

Recommended Mitigations: I recommend that the organization disable anonymous login. If the organization needs to enable anonymous login for commercial purposes, I recommend that any valuable information like the proof.txt file be secured by allowing access only at the admin level.

Evidence:

**Vulnerability Name:** Overflow in Konica Minolta Server 1.00

Description: The exploit used takes advantage of Structured Exception Handler (SEH) overflow vulnerability in the Konica Minolta Server 1.00. SEH was designed by Windows to handle segmentation faults, but the one utilized in Konica Minolta 1.00 does not check the input size of “cwd” (change working directory) commands, resulting in an overflow.

Severity: 10/10; Un-updated software is always a red flag, and is an easy problem to fix. However, within the system, I still only had reduced privileges.

Affected Hostname: 10.20.160.41

Recommended Mitigations: Update the software for Konica Minolta.

**Vulnerability Name:** User Account Control (UAC) Bypass

Description: User Account Control is a security mechanism in Windows that prohibits unauthorized alterations to the operating system. UAC Bypass is a module in Metasploit that utilizes the trusted publisher certificate to create a second shell that turns the UAC flag off.

By turning the flag off, the anonymous user can be given admin privileges. As a result, the user can perform operations like changing the password on the machine, and using malicious executables.

Severity: 10/10; UAC Bypass allows for any user to escalate their privileges to get sensitive information the company may have.

Affected Hostname: 10.20.160.41

Recommended Mitigations: The UAC is broken down into three main options: (1) Always Notify (2) Notify Me When Programs Try to Make Changes to My Computer (3) Never Notify. The UAC Bypass exploit can only work on the (2) and (3). If there are valuable documents on the machine, enabling the Always Notify option will stop the exploit from occurring.

**Vulnerability Name:** Password on Desktop

Description: A user named Jill left her password credentials on the desktop of Fred’s machines. Using these credentials, I was able to connect to machine 10.20.170.87 by way of PuTTY. PuTTY is a terminal emulator and provides remote access to other desktops. It is generally paired in usage with Secure Socket Shell (ssh); the combination allows for a convenient and secure access portal to the remote desktop, and allows for a way to interchange the use of Windows and UNIX operating systems.

Severity: 10/10; Users should never leave their passwords on the desktop they are operating from.

Affected Hostname: 10.20.170.87

Recommended Mitigations: I recommend that employees at the company receive a background training module on basic security protocols. I am generally free on the weekends, and my rates are very reasonable.

Attack Path

First, an nmap scan was run to determine which ports on the machine were open.

A screenshot of a cell phone screen with text

Description automatically generated

After seeing that anonymous login was enabled on port 21, I used the exploit module kmftp\_utility\_cwd. This module exploits the overflow error in Konica Minolta Server 1.00.

A black and silver text on a screen

Description automatically generated

A black sign with white text

Description automatically generated

After entering the meterpreter sessions, I was able to locate the first proof file on Fred’s desktop.

A screenshot of text

Description automatically generated

Using UACPass, I was able to elevate my admin privileges and create a second meterpreter session.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

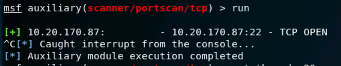
Description automatically generated

I then used netenum to find the host machine behind the firewall. Running nmap proved fruitless since the firewall filtered any packets coming from 10.20.150.101.

A close up of a sign

Description automatically generated

Using portscan, I also found that port 22 was open.



With admin privileges, I used the exploitation package Kiwi to do a hashdump on the password and renamed the password for Fred’s desktop “hi.”

A screenshot of a cell phone

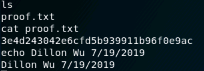
Description automatically generated

With these tools, I utilized rdesktop to remotely log onto Fred’s account, and opened the SSH.bat file to find Jill’s username and password.

A screenshot of a social media post

Description automatically generated

Finally, I executed the file to retrieve the proof.txt file on Jill’s account.



Technical Details

Hostname: 10.20.160.41

Open Ports: 21

Vulnerability Description: Anonymous login via port 21

Proof file: df5962c70b1abac2c6d8e1c194d781eb

Hostname: 10.20.170.87

Open Ports: 22

Vulnerability Description: Login via port 22 using Jill’s credentials

Proof file: 3e4d243042e6cfd5b939911b96f0e9ac