Princeton-Plainsboro Teaching Hospital

Windows 11 Education - 40 vulns - “Hard”

# Forensics - 5v, 37pts

## FQ1

This computer was recently re-imaged with Windows 11 Education as a part of a push to modernize the hospital’s infrastructure. For some reason on this PC, it wouldn’t install without some modifications to WinPE’s registry. Please provide the full path to the keys that were modified. You may shorten the root key.

EXAMPLE: HKLM\SOFTWARE\CVSM\CVSM

ANSWER: HKLM\SYSTEM\Setup\LabConfig\BypassTPMCheck

ANSWER: HKLM\SYSTEM\Setup\LabConfig\BypassSecureBootCheck

5pts

## FQ2

When you first set up this machine, you created security questions to help you in the event that you need to reset your password. Unfortunately, you just performed brain surgery on yourself and totally fucked up the part of your brain that remembered the answers to said questions. What was your childhood nickname?

EXAMPLE: goose

ANSWER: matt

10pts

## FQ3

Oh great. The only authorized administrator on this computer, Dr. Cuddy, forgot her password. She has no security questions nor does she have a password reset disk. Fortunately, there’s a way to reset it using some Windows trickery that allows you access to the SYSTEM account. What is the flag in the Documents folder of the SYSTEM account?

EXAMPLE: 1984

ANSWER: Teardrop by Massive Attack is a banger

10pts

## FQ4

What famous quote from Dr. House is embedded in the script that keeps resetting some important security options?

EXAMPLE: I don't ask why patients lie, I just assume they all do.

ANSWER: It's nothing personal. I don't like anybody.

7pts

## FQ5

What is the name of the task that blue screens the PC at 20 minutes past every hour?

ANSWER: MicrosoftEdgeUpdateTaskUserUA

5pts

# User Auditing - 6v, 10pts

Lcuddy’s password was reset - 4pts

Remote Work group created and populated - 1pts

eforeman is no longer a Remote Management User - 2pts

Cpark’s password expires - 1pts

Dibala deleted - 1pts

Guest account disabled - 1pts

# Prohibited Files & Malware - 6v, 12pts

Powershell script persistence removed - 4pts

Unencrypted medical records removed - 2pts

McAfee Antivirus removed - 1pts

AnyDesk Portable removed - 1pts

Mimikatz Driver removed - 3pts

FTP Server Disabled - 1pts

# Local Policies - 3v, 3pts

Password requirements are not ignored - 1pts

Audit object access [Success/Failure] - 1pts

Prompt for authentication on the secure desktop - 1pts

# Application Security - 13v, 24pts

SMB Security Signature enabled - 2pts

SMB Unencrypted Password Transmission disabled - 2pts

SMBv1 uninstalled - 1pts

RDP Requires secure RPC communication: Enabled - 1pts

RDP Group logon permissions check passed - 3pts

RDP SSL security [Enabled] - 2pts

SRCDS Little anti-cheat installed - 4pts

SRCDS unauthorized SourceMod administrators removed - 2pts

SRCDS allowed through firewall - 1pts

SRCDS connection password exists - 2pts

Firefox no longer crashes on startup - 1pts

Firefox Accounts disabled - 2pts

Firefox Block dangerous and deceptive content [Enabled] - 1pts

# Defensive Countermeasures - 5v, 8pts

Block Win32 imports from macro code in Office - 2pts

Windows Defender Firewall service enabled and started - 1pts

Script Scanning [On] - 1pts

Default threat action for severe threats no longer ignore - 3pts

Incoming connections not matching a rule are blocked in Public profile - 1pts

# Uncategorized OS Settings - 2v, 5pts

Windows Updates installed - 4pts

Bitlocker drive encryption enabled - 1pts