Democratic People's Republic of Korea Walkthrough

lolmenow, SG, & a_person

Medium/Hard

February 11, 2025

Introduction

Project Conceptualization and Rational

This document aims to help our fellow competitors not only know the vulnerabilities in our virtual machine but also to help them get a deeper understanding of cybersecurity and the new vulnerabilities in Windows Server 2025, specifically SMB.

In this document, we will provide a walkthrough of this VM (categorized by the standard vulnerability categories in CyberPatriot) and a scoring report completed by lolmenow.

We will note any new vulnerabilities not in Windows Server 2022 by adding an asterisk after the vulnerability.

Note that some vulnerabilities may not be aligned as it is in the scoring report.

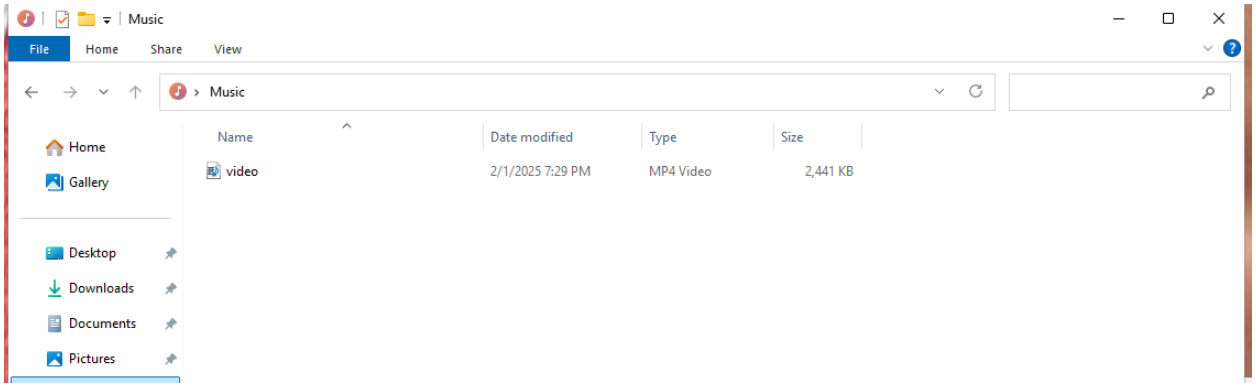
Walkthrough

Forensics Questions

[Forensic Question 1 Correct] - 1pt

“There is a file named “video.mp4”. What is the absolute path?”

This is pretty straightforward. You can use Everything or just simply find the video in the User’s music directory.



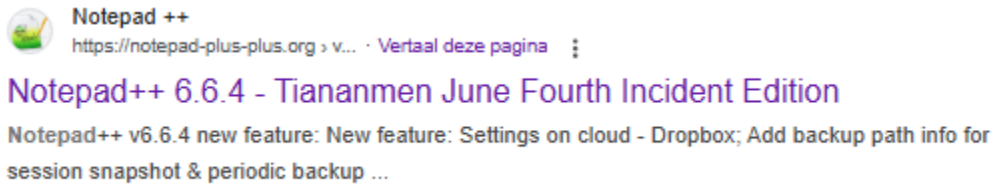
The absolute path is the entire path including the C drive. So, your answer should be:

ANSWER: **C:\Users\Kim Jong Un\Music\video.mp4**

Note, you can get the full path with Everything by Right Clicking > “Copy full name to clipboard”

[Forensic Question 2 Correct] -1pt
“What is the current version of notepad++ called?”

This question was also pretty straightforward, as we can see that the version of notepad++ is 6.6.4

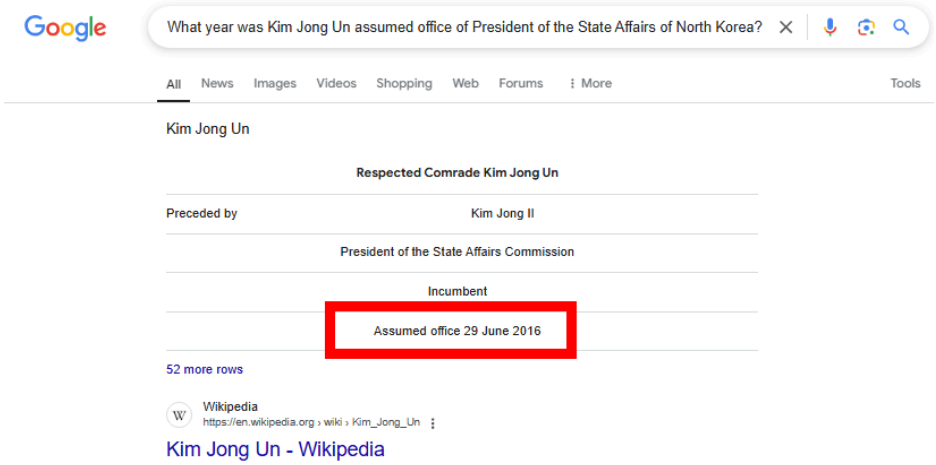


ANSWER: **Tiananmen June Fourth Incident Edition**

Note: This question was ambiguous, sorry if it caused any confusion. The question was referring to the currently installed version of notepad++ on the virtual machine.

[Forensic Question 3 Correct] -1pt
“What year was Kim Jong Un assumed office of President of the State Affairs of North Korea?”

This was probably the easiest question to answer. Link



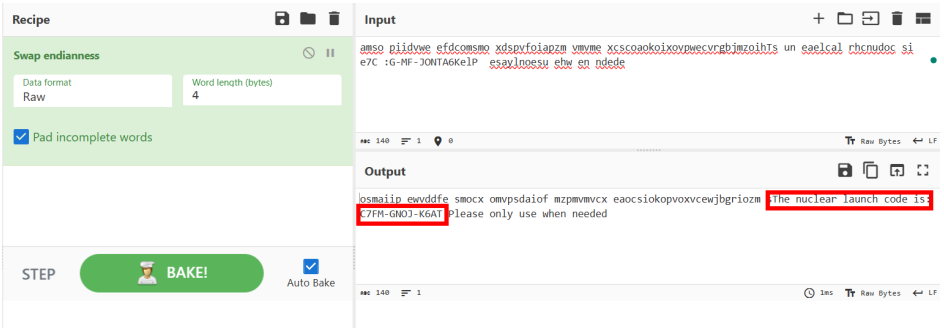
ANSWER: **2016**

[Forensic Question 4 Correct] -1pt
“The following text was discovered to be the encrypted nuclear launch code.
We have discovered that endianness was used to encode it. What is the nuclear launch code?
Encrypted text:

amvamso piidvwe efdcomsmo xdspvfoiapzm vmvme xcscoaokoixovpwecvrgbjmzoihTs un eaelcal rhcnudoc si e7C :G-MF-JONTA6KelP esaylnoesu ehw en ndede

NOTE: Once unencrypted, the nuclear launch code will be after the string ‘The nuclear launch code is:’”

This one is hard if you don’t know the trick. You have to delete some bytes for it to be unencrypted. Link



ANSWER: **C7FM-GNOJ-K6AT**

[Forensic Question 5 Correct] -2pt

“What is hidden in the nuclear weapons plans pdf? The text starts with string ‘THE FIRST’”

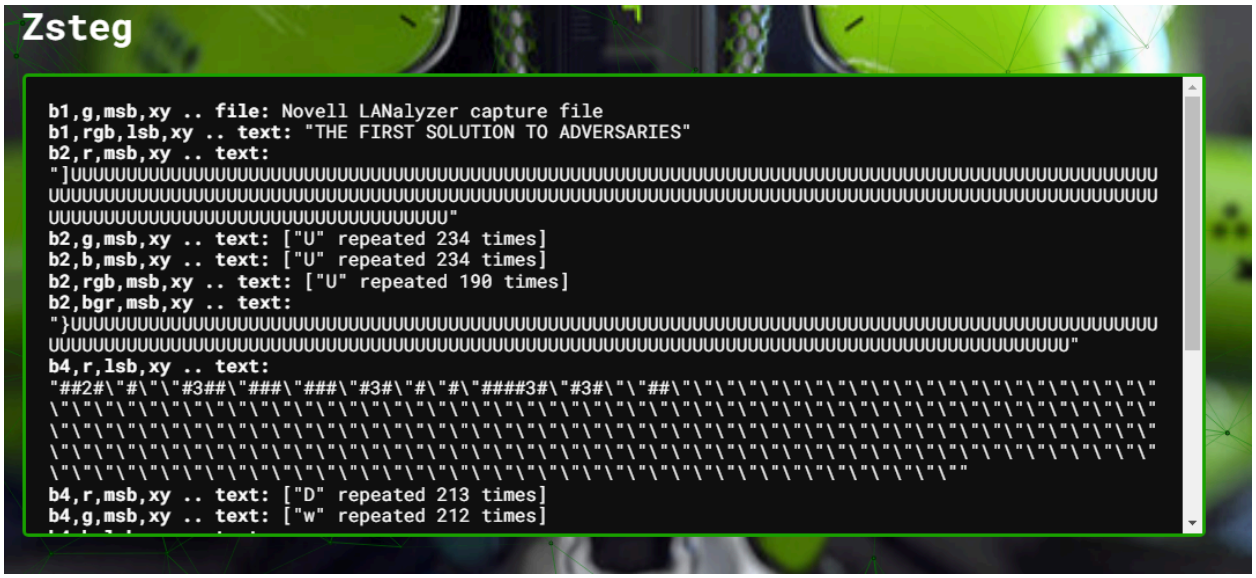
The text on the PDF is not relevant to this question. However, the image on the second page does and looks suspicious. Extract the image using any online tool.

This challenge utilizes basic steganography. More specifically, LSB steganography. You can use a tool such as zsteg to carve the message out.

We find the message at **b1,rgb,lsb,xy,** which says “THE FIRST SOLUTION TO ADVERSARIES”

ANSWER: **THE FIRST SOLUTION TO ADVERSARIES**

Aperisolve also catches it:



[Forensic Question 6 Correct] -2pt

“What is the password to the nuclear launch app?”

Opening the executable requires us to input a password. We do not know this, so we need to use a decompiler of some sort to look inside the executable.

I extracted the executable from the VM onto my host, and used IDA to start reversing.

```
__int64 sub_1400F2240()
{
  char *v0; // rdi
  __int64 i; // rcx
  _BYTE v3[32]; // [rsp+0h] [rbp-20h] BYREF
  char v4; // [rsp+20h] [rbp+0h] BYREF
  _BYTE v5[64]; // [rsp+28h] [rbp+8h] BYREF
  _BYTE v6[64]; // [rsp+68h] [rbp+48h] BYREF
  _BYTE v7[64]; // [rsp+A8h] [rbp+88h] BYREF
  _BYTE v8[288]; // [rsp+E8h] [rbp+C8h] BYREF
  _BYTE v9[48]; // [rsp+208h] [rbp+1E8h] BYREF
  __int64 v10; // [rsp+238h] [rbp+218h]
  __int64 v11; // [rsp+240h] [rbp+220h]
  __int64 v12; // [rsp+248h] [rbp+228h]

  v0 = &v4;
  for ( i = 98LL; i; --i )
  {
    *(_DWORD *)v0 = -858993460;
    v0 += 4;
  }
  sub_1400DC5C8(&unk_140309069);
  sub_1400D9698(v5, "%bq=3:`%+)}93(&l");
  sub_1400D9698(v6, "U29tZUNvZGVkU3RyaW5n");
  sub_1400DC555(v7);
  v10 = sub_1400DC01E(v9, v5);
  v11 = v10;
  v12 = sub_1400D81F8(v8, v10);
  sub_1400D7FE1(v9);
  sub_1400D7942(&unk_1402EDD10, "What is the password? ");
  sub_1400D9F12(&qword_1402EDC10, v7);
  if ( (unsigned __int8)sub_1400D85B8(v8, v7) )
    v10 = sub_1400D7942(&unk_1402EDD10, "Correct");
  else
    v10 = sub_1400D7942(&unk_1402EDD10, "Incorrect password!");
  sub_1400D9B6B(v10, sub_1400D7357);
  sub_1400D7FE1(v8);
  sub_1400D9788("pause");
  sub_1400D7FE1(v7);
  sub_1400D7FE1(v6);
  sub_1400D7FE1(v5);
  sub_1400DB6D7(v3, &unk_14029DC70);
  return 0LL;
}
```

This is the main portion of the entire binary. A lot of people, without reading the code, would see a base64 encoded string with the call from sub(1400D9698) and think that is the answer. However, that is not the case. This is because the final comparison is never checked against v6. Instead, it checks v8 after a transportation of two calls.

It first transforms v5 through sub_1400DC01E. This returns sub_1400F1870, which is:

```
__int64 __fastcall sub_1400F1870(__int64 a1, __int64 a2)
{
  char *v2; // rdi
  __int64 i; // rcx
  _BYTE v5[32]; // [rsp+0h] [rbp-20h] BYREF
  char v6; // [rsp+20h] [rbp+0h] BYREF
  __int64 v7; // [rsp+68h] [rbp+48h]
  unsigned __int8 *v8; // [rsp+88h] [rbp+68h]
  __int64 v9; // [rsp+A8h] [rbp+88h]
  unsigned __int8 v10; // [rsp+C4h] [rbp+A4h]
  int v11; // [rsp+1C4h] [rbp+1A4h]
  __int64 v12; // [rsp+1D8h] [rbp+1B8h]

  v2 = &v6;
  for ( i = 66LL; i; --i )
  {
    *(_DWORD *)v2 = -858993460;
    v2 += 4;
  }
  v11 = 0;
  sub_1400DC5C8(&unk_140309069);
  v12 = sub_1400DC555(a1);
  v11 |= 1u;
  v7 = a2;
  v8 = (unsigned __int8 *)sub_1400DBE84(a2);
  v9 = sub_1400D7343(v7);
  while ( v8 != (unsigned __int8 *)v9 )
  {
    v10 = *v8;
    if ( (char)v10 < 33 || v10 == 127 )
      sub_1400D9C97(a1, v10);
    else
      sub_1400D9C97(a1, (unsigned __int8)(((char)v10 + 14) % 94 + 33));
    ++v8;
  }
  sub_1400DB6D7(v5, &unk_14029D9E0);
  return a1;
}
```

TLDR: The transformation here is rot47, specifically in this line:
sub_1400D9C97(a1, (unsigned __int8)(((char)v10 + 14) % 94 + 33));

The other transformation, as shown in sub_1400D81F8, which returns sub_1400EFB10, is:

```
__int64 __fastcall sub_1400EFB10(__int64 a1, __int64 a2)
{
  char *v2; // rdi
  __int64 i; // rcx
  _BYTE v5[32]; // [rsp+0h] [rbp-20h] BYREF
  char v6; // [rsp+20h] [rbp+0h] BYREF
  _BYTE v7[124]; // [rsp+28h] [rbp+8h] BYREF
  int v8; // [rsp+A4h] [rbp+84h]
  int v9; // [rsp+C4h] [rbp+A4h]
  __int64 v10; // [rsp+E8h] [rbp+C8h]
  unsigned __int8 *v11; // [rsp+108h] [rbp+E8h]
  __int64 v12; // [rsp+128h] [rbp+108h]
  unsigned __int8 v13; // [rsp+144h] [rbp+124h]
  int v14; // [rsp+164h] [rbp+144h]
  _BYTE v15[44]; // [rsp+248h] [rbp+228h] BYREF
  int v16; // [rsp+274h] [rbp+254h]
  __int64 v17; // [rsp+288h] [rbp+268h]

  v2 = &v6;
  for ( i = 114LL; i; --i )
  {
    *(_DWORD *)v2 = -858993460;
    v2 += 4;
  }
  v16 = 0;
  sub_1400DC5C8(&unk_140309069);
  sub_1400D9698(v7, "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/");
  v17 = sub_1400DC555(a1);
  v16 |= 1u;
  v8 = 0;
  v9 = -8;
  v10 = a2;
  v11 = (unsigned __int8 *)sub_1400DBE84(a2);
  v12 = sub_1400D7343(v10);
  while ( v11 != (unsigned __int8 *)v12 )
  {
    v13 = *v11;
    if ( v13 == 61 )
      break;
    v14 = sub_1400D9D82(v7, v13, 0LL);
    if ( v14 == -1LL )
    {
      sub_1400D8027(v15, "Invalid character in Base64 string");
      sub_1400DCD9D(v15, &unk_1402EA9F8);
    }
    v8 = v14 + (v8 << 6);
    v9 += 6;
    if ( v9 >= 0 )
    {
      sub_1400D8D79(a1, (unsigned __int8)(v8 >> v9));
      v9 -= 8;
    }
    ++v11;
  }
  sub_1400D7FE1(v7);
  sub_1400DB6D7(v5, &unk_14029DAC0);
  return a1;
}
```

The function is a basic base64 transformation.

To reverse the string and pass the password check, you would need to rot47 and base64 the string **%bq=3:`%+)}93(&l**

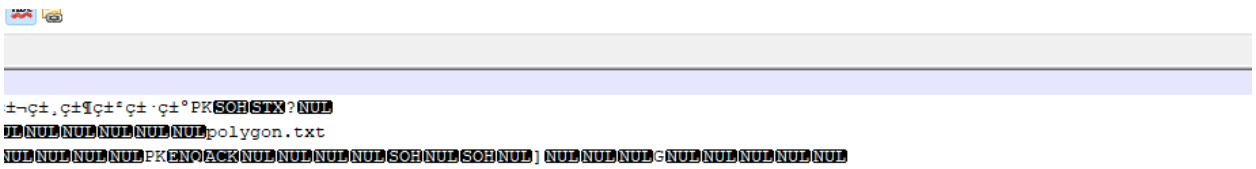
Cyberchef

ANSWER: **Open-Sesame**

[Forensic Question 7 Correct] -2pt

“There is a file on the desktop named “polygon.png” What is the hidden message? It starts with the letter H.”

The image file does not open. Using a text editor/hex editor, we see something suspicious:



Polygon.txt is embedded inside the image.

Use a tool, such as binwalk, to extract it, or just rename the file to the extension *.zip.

We get this:

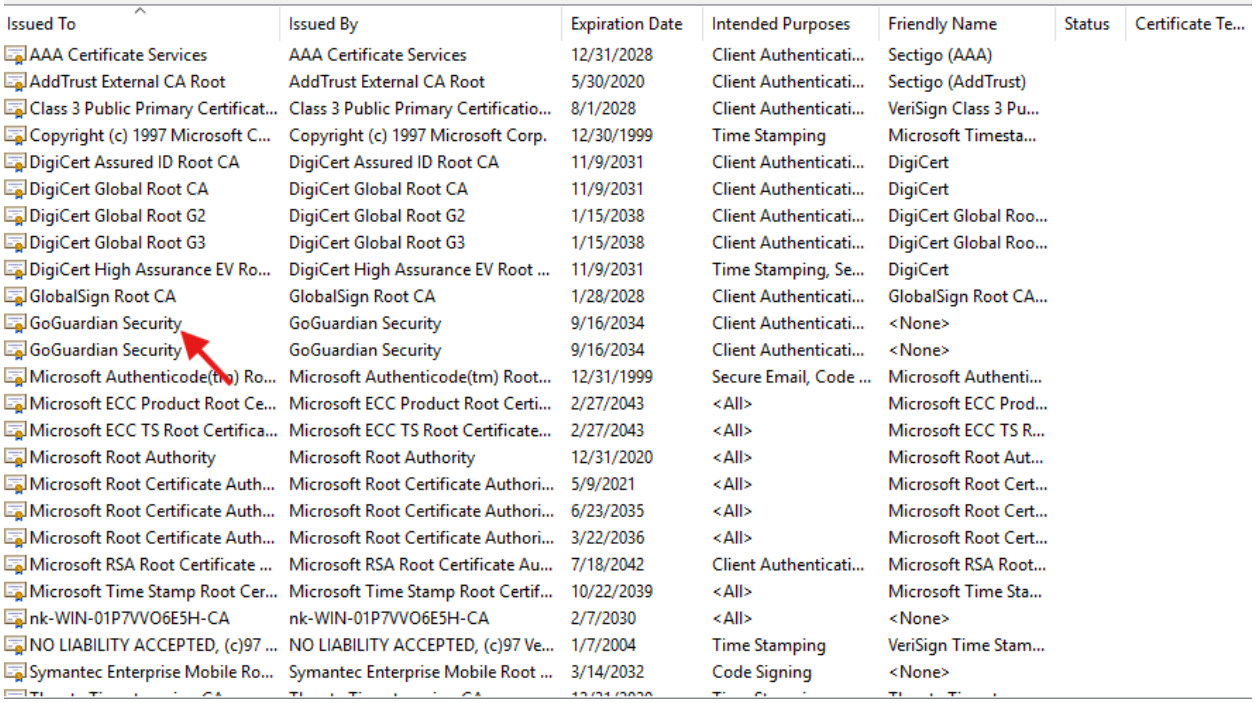
The text is ciphered with rot8000. Reverse it by using rot8000, and you get your answer! [Cyberchef Rot8000]

ANSWER: **Homecoming**

[Forensic Question 8 Correct] -2pt

“What was the CN of the last cert issued that does not start with WIN and is not preconfigured?”

This is pretty simple to solve, you may compare the default certificates to a clean machine, or look for ones out of the ordinary. Using certmgr.msc, under Trusted Root Certification Authorities > Personal, we see an unusual certificate.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati...	Sectigo (AAA)		
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Client Authenticati...	Sectigo (AddTrust)		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Client Authenticati...	VeriSign Class 3 Pu...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticati...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Global Roo...		
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticati...	DigiCert Global Roo...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Time Stamping, Se...	DigiCert		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati...	GlobalSign Root CA...		
GoGuardian Security	GoGuardian Security	9/16/2034	Client Authenticati...	<None>		
GoGuardian Security	GoGuardian Security	9/16/2034	Client Authenticati...	<None>		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate...	2/27/2043	<All>	Microsoft ECC TS R...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
Microsoft RSA Root Certificate ...	Microsoft RSA Root Certificate Au...	7/18/2042	Client Authenticati...	Microsoft RSA Root...		
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	10/22/2039	<All>	Microsoft Time Sta...		
nk-WIN-01P7VVO6E5H-CA	nk-WIN-01P7VVO6E5H-CA	2/7/2030	<All>	<None>		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/14/2032	Code Signing	<None>		

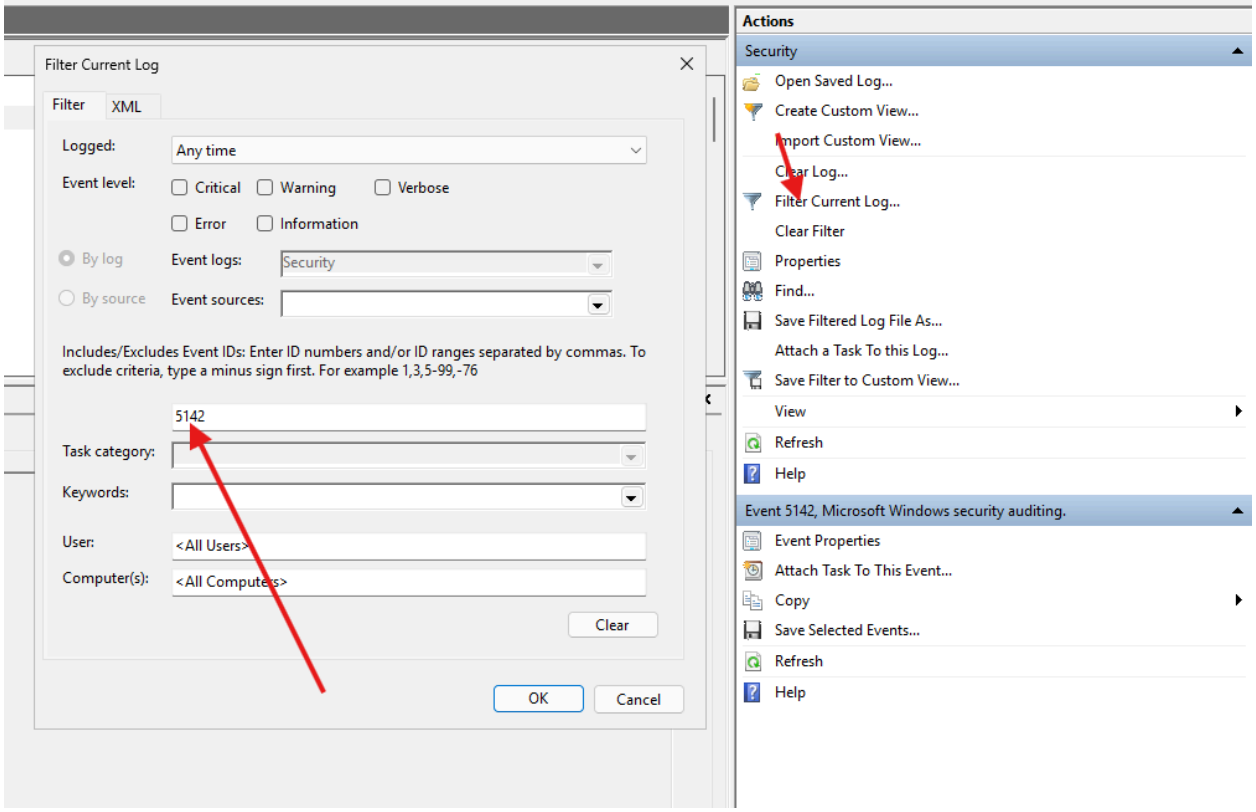
ANSWER: **GoGuardian Security**

[Forensic Question 9 Correct] -2pt

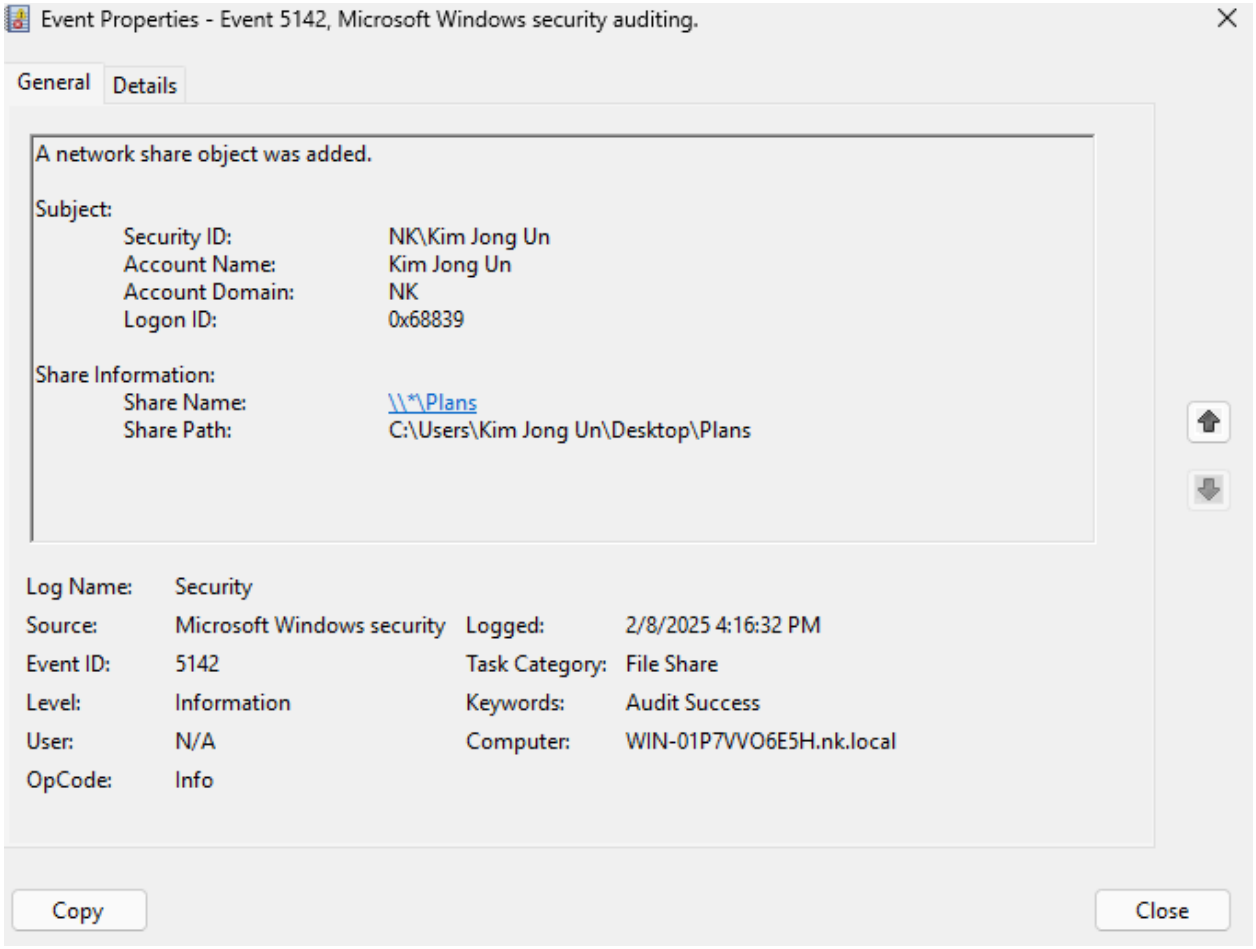
“When was file share "Plans" created?”

Using the event viewer, you can check when certain shares were created. With a google search, we know the ID to check this is **5142**

Filter the current log to check only IDs of 5142 under the security section.



We see the share being created here, the last event in the filtered log.



ANSWER: **2/8/2025 4:16:32 PM**

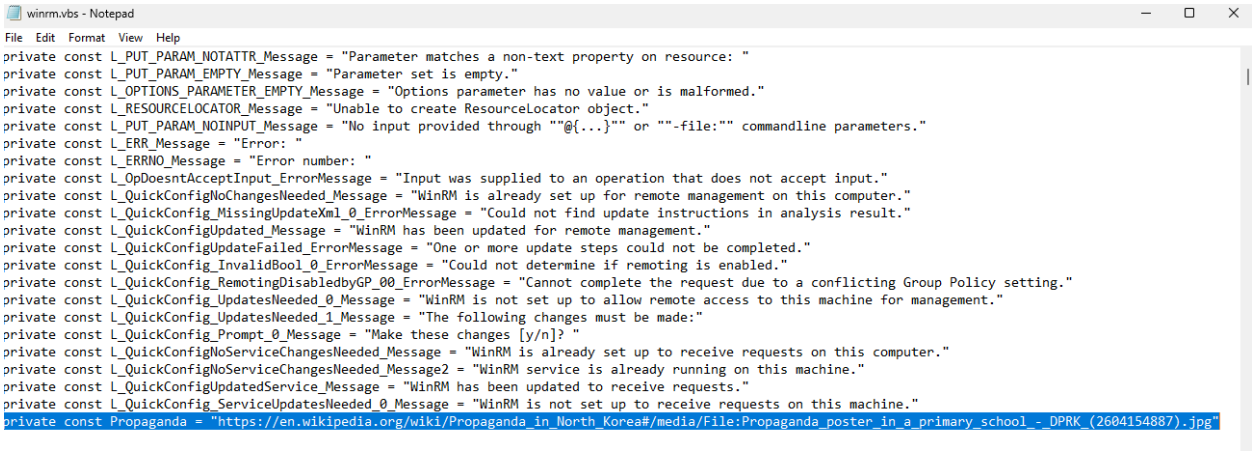
[Forensic Question 10 Correct] -2pt

“There is a vbs script that has been tampered with. What is the absolute path of the vbs script?”

Because the script has been tampered with, not a new vbs scripted being added, we need to baseline vbs scripts from a clean machine to the VM, and check for hash differences.

There are various programs/scripts out on the internet to accomplish this task. At the end, we see that C:\Windows\SysWOW64\winrm.vbs was tampered with, making that our answer.

If you’re curious, here is what was added:



ANSWER: **C:\Windows\SysWOW64\winrm.vbs**

User Auditing

[Removed Unauthorized User 에이든**]** - 2 pts

This user was not on the Allowed Users list.
Active Directory Users and Computers > Users > Right click 에이든 > Delete

[Kim Chang-bong is not an Administrator] - 2 pts

This user was not on the Allowed Administrators list.
Active Directory Users and Computers > Users > Right click Kim Chang-bong > Properties > Member of > Then remove the user from the “Administrators” group.

[Guest Account is disabled] - 1 pts

The guest account should always be disabled because it reduces the attack surface.
Active Directory Users and Computers > Users > Right click Guest > Disable Account

[Created AD group Generals] - 2 pts

This was stated in the README.
Active Directory Users and Computers > Users > Right Click > New Group > Name: Generals > Ok

[Added Users to group Generals] - 2 pts

This was stated in the README.
Active Directory Users and Computers > Users > Right Click Generals > Properties > Members > Add > Add the users mentioned in the README

[Kim Kwang-hyop is no longer an Enterprise Admin] - 2 pts

Users should not be in the group unless specified by the README.
Active Directory Users and Computers > Users > Right Click Enterprise Admins > Properties > Members > Kim Kwang-hyop > Remove > Ok

[Domain Controllers group is no longer managed by Domain Guests] - 2 pts

Go to Active Directory Users and Computers > Users > Right Click Domain Controllers > Properties > Managed By > Clear > Ok

Having a critical group being managed by a low privileged group can allow for privilege escalation.

[Enterprise Admins no longer managed by Users] - 2 pts

Go to Active Directory Users and Computers > Users > Right Click Enterprise Admins> Properties > Managed By > Clear > Ok

Having a critical group being managed by a low privileged group can allow for privilege escalation.

[Everyone does not have FullControl rights on the domain] - 2 pts

Go to Active Directory Users and Computers > Right click on nk.local > Properties > Security > Remove “Full control” from Everyone.

This can allow for privilege escalation if everyone has full control on the domain.

Local Policy

[A minimum password length is set] - 2 pts
The acceptable range was 10-30.
Windows+R > secpol.msc > Account Policy > Password Policy > Minimum Password Length

[Password must meet complexity requirements[enabled]] - 2 pts
Windows+R > secpol.msc > Account Policy > Password Policy > Password must meet complexity requirements

[Audit Computer Account Management [Success/Failure]] - 2 pts
Windows+R > secpol.msc >Advanced Audit Policy Configuration > Account Management > Audit Computer Account Management

[Audit SAM [Success/Failure]] - 2 pts
Windows+R > secpol.msc >Advanced Audit Policy Configuration > Object Management > Audit SAM

[Advanced Audit for Certification Services is enabled] - 2 pts
Windows+R > secpol.msc >Advanced Audit Policy Configuration > Object Management > Audit Certification Services

[Do not allow anonymous enumeration of sam accounts[enabled]] - 2 pts
Windows+R > gpedit.msc > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

[Restrict cd-rom access to locally logged on user only] - 2 pts
Windows+R > gpedit.msc > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

Defensive Countermeasures

[Firewall is Enabled] - 1 pts
Windows + R > control > System and Security > Windows Firewall >
Select Turn Windows Firewall on.

Uncategorized OS Settings

[Windows Smart Screen Enabled] - 2 pts

Windows+R > gpedit.msc > Computer Configuration > Administrative Templates > Windows Components > Windows Defender SmartScreen > Explorer > Configure Windows Defender SmartScreen

[Microsoft Defender Antivirus - Block Webshell creation for Servers ASR rule configured] - 3 pts*

Windows +R > Powershell (run as administrator) > Type in the following Command:

reg add 'HKLM\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules' /v 'a8f5898e-1dc8-49a9-9878-85004b8a61e6' /t 'REG_SZ' /d '1' /f

OR

Add-MpPreference -AttackSurfaceReductionRules_Ids a8f5898e-1dc8-49a9-9878-85004b8a61e6 -AttackSurfaceReductionRules_Actions Enabled

Service Auditing

[Remote Registry Service Disabled] - 2 pts

Windows +R > Services.msc > Double Click Remote Registry > Startup Type > Disabled

Operating System Updates

[Windows Automatically Checks for Updates] - 1 pts

Registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate set to 0

OR

gpedit.msc

Computer Configuration > Windows Components > Windows Update > Manage End User Experience > Configure Automatic Updates

Application Updates

[Notepad++ is updated] - 1 pts

We know Notepad++ is outdated because of the forensic question.
Notepad++ > ? icon > Update Notepad++

Or just download the installer from their site.

Prohibited Files

[Removed Prohibited MP4 files] - 1 pts

We know there is a prohibited MP4 file because of the forensic question
Delete the mp4 file C:\Users\Kim Jong Un\Music\video.mp4.

[Plaintext file with passwords removed] - 1 pts

In the main user's document folder, there is a txt file named “passwords.txt”. Delete it

Unwanted Software

[Prohibited Software Wireshark is removed] - 1 pts
Control Panel > Uninstall a Program > Right Click Wireshark > Uninstall

[Prohibited Software Pong is removed] - 2 pts
This file was located in C:\Pong. Delete the folder.

[PowerShell 2.0 is disabled] - 1 pts
Run the Powershell Command
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowershellV2 -Remove

This feature should be removed as Powershell 2.0 did not have many security features.

Malware

[Prohibited Spyware GoGuardian removed] - 3 pts

In C:\Program Files\, there seems to be no folder named GoGuardian, and if we use command prompt, it also does not appear. This is because it is a system-protected file. To view system-protected files, go to Explorer> view > options > View > Uncheck “Hide protected Operating System files(recommended).” You should now be able to view it and delete it.

[Malicious Chrome Extension removed] - 3 pts

Go to Google Chrome> Puzzle piece icon > Manage extension > Remove the GoGuardian extension.

[Malicious PS1 Startup Script removed] - 2 pts

Sadly, this didn’t work for some reason. Anyways, there is a ps1 script in C:\Users\Kim Jong Un\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\uwu.ps1. Delete it.

[Netcat Backdoor Removed] - 2 pts

C:\Windows\System32\printui.exe was tampered with, so delete it. Windows Defender might have caught this automatically.

Application Security

[RDP Requires Network level Authentication] - 1 pts

Set the Registry Key
HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication to 1

OR

Settings > Remote Desktop > Drop down > Require Devices to Use Network Level Authentication to Connect. Tick this box.

As Microsoft states, “Allowing connections only from computers running Remote Desktop with NLA is a more secure authentication method that can help protect your computer from malicious users and software.”

[Require use of specific security layer for RDP set to TLS] - 2 pts

Set the Registry Key
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\SecurityLayer to 2

OR

gpedit.msc

Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Require Use of specific security layer for Remote (RDP) connections > Enabled > Choose SSL

By enforcing TLS encryption, it significantly enhances the protection of data transmitted between the client and the remote server during RDP sessions, mitigating potential eavesdropping risks.

[File Share Western Influence Stopped sharing] - 2 pts

Go to Computer Management > Shared Folders > Shares > Right Click Western Influence > Stop Sharing

[SMB over QUIC is enabled on Server and Client] - 2 pts

Set the Registry Keys
HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanServer\EnableSMBQUIC and

HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation\EnableSMBQUIC to 1

OR

gpedit.msc

Computer Configuration > Administrative Templates > Network > Lanman Server > Enable SMB over QUIC
Do the same inside of Lanman Workstation

SMB over QUIC makes SMB more secure as its data is now transported over Quick UDP Internet Connections, which, by design, encrypts data with TLS 1.3 over port 443 instead of the legacy port 445.

[SMB Blocks NTLM is enabled]* - 2 pts

Set the Registry Key
HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation\BlockNTLM to 1

OR

gpedit.msc

Computer Configuration > Administrative Templates > Network > Lanman Workstation > Block NTLM

As Microsoft says, this is secure as it “prevents bad actors from tricking clients into sending NTLM requests to malicious servers, counteracting brute force, cracking, and pass-the-hash attacks” Learn more here

[A Minimum SMB Version(3.0.0+) is configured]* - 2 pts

Set the Registry Key
HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanServer\MinSmb2Dialect to 300

OR

gpedit.msc

Computer Configuration > Administrative Templates > Network > Lanman Workstation > > Mandate the Minimum Version of SMB > Set to SMB 3.0.0 or higher.

Having the latest version of critical services is necessary to prevent exploits/threat actors over the network.

[Authenticator Rate Limiter is enabled]* - 1 pts

Set the Registry Key HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanServer\EnableAuthRateLimiter to 1

OR

gpedit.msc

Computer Configuration > Administrative Templates > Network > Lanman Server > Enable authentication rate limiter.

Delaying invalid authentication attempts delays threat actors to brute force logins.

[An Invalid Authentication Delay exists on the system]* - 2 pts

Set the Registry Key HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanServer\InvalidAuthenticationDelayTimeInMs to whatever you want, the recommended value is 2000

OR

gpedit.msc

Computer Configuration > Administrative Templates > Network > Lanman Server > Set authentication rate limiter delay (milliseconds)

Having a higher rate limiter will delay threat actors' attempts to bruteforce even more. As Microsoft says, “The SMB server service uses the authentication rate limiter to implement a 2-second delay between each failed NTLM or PKU2U-based authentication attempt. Meaning if an attacker previously sent 300 brute force attempts per second from a client for 5 minutes (90,000 passwords), the same number of attempts would now take 50 hours or more.” Learn more here

[CAPolicy.inf insecure permissions fixed] - 2 pts

Go to C:\Windows\System32 > Right Click the file > Properties > Security > Change the permissions of Everyone so that they do not have full control.

CAPolicy.inf is a critical file that has configuration settings to a root CA certificate.

[AD CS disallowed certs auto update is enabled] - 3 pts

Set the Registry Key HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\EnableDisallowedCertAutoUpdate to 1 or use the admx templates that Microsoft provides.

TLDR: this setup prevents automatic updates of trusted certificate trust lists while allowing updates for untrusted CTLs. This stops malicious or unverified certificates from being automatically trusted. More on this can be found here.

[VBS is in Mandatory Mode] - 1 pts

Set the Registry Key
HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Mandatory to 1

OR

reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "Mandatory" /t REG_DWORD /d 1 /f

More can be found here. This also prevents the downdate vulnerability, which is CVE-2024-21302.

[Machine Identity Isolation is set to audit mode or enforcement mode]- 2 pts

Set the Registry Key
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\MachineIdentityIsolation to 1 or 2

OR

gpedit.msc

Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security > Machine Identity Isolation Configuration

Machine Identity Isolation should be enabled because it provides a critical layer of security by separating and protecting machine identities, preventing unauthorized access to sensitive systems and data. More can be found here.

[msDS-KeyCredential object '05jf' is deleted from LostAndFound] - 2 pts

Go to Active Directory Users and Computers > LostAndFound> right click 05jf > delete.

Having extraneous key credentials that is not authorized by the README is a security risk.

[Chrome sends a Do Not Track request] - 2 pts

Google Chrome > Settings > Privacy and Security > Third-party cookies > Enable: Send a “Do Not Track” request with your browsing traffic

This setting asks websites you visit to not track your activity on the webpage.

Full Scoring Report

Completed by lolmenow

55 out of 55 scored security issues fixed, for a gain of 100 points:

Forensics Question 1 correct - 1 pts
Forensics Question 2 correct - 1 pts
Forensics Question 3 correct - 1 pts
Forensics Question 4 correct - 2 pts
Forensics Question 5 correct - 2 pts
Forensics Question 6 correct - 2 pts
Forensics Question 7 correct - 2 pts
Forensics Question 8 correct - 2 pts
Forensics Question 9 correct - 2 pts
Forensics Question 10 correct - 2 pts
Removed Unauthorized User 에이든 - 2 pts
Kim Chang-bong is not an Administrator - 2 pts
Guest Account is disabled - 1 pts
Created AD group Generals - 2 pts
Added Users to group Generals - 2 pts
Kim Kwang-hyop is no longer an Enterprise Admin - 2 pts
A minimum password length is set - 2 pts
Password must meet complexity requirements[enabled] - 2 pts
Firewall is Enabled - 1 pts
Microsoft Defender Antivirus - "Block Webshell creation for Servers" ASR rule configured - 3 pts
Audit Computer Account Management [Success/Failure] - 2 pts
Audit SAM [Success/Failure] - 2 pts
Advanced Audit for Certification Services is enabled - 2 pts
Windows Smart Screen Enabled - 2 pts
Do not allow anonymous enumeration of sam accounts[enabled] - 2 pts
Restrict cd-rom access to locally logged on user only - 2 pts
Remote Registry Service Disabled - 2 pts
File Share Western Influence Stopped sharing - 2 pts
Windows Automatically Checks for Updates - 1 pts
Notepad++ is updated - 1 pts
Removed Prohibited MP4 files - 1 pts
Plaintext file with passwords removed - 1 pts
Prohibited Spyware GoGuardian removed - 3 pts
Prohibited Software Wireshark is removed - 1 pts
Prohibited Software Pong is removed - 2 pts
Malicious Chrome Extension removed - 3 pts
Malicious PS1 Startup Script removed - 2 pts
Netcat Backdoor Removed - 2 pts
RDP Requires Network level Authentication - 1 pts
PowerShell 2.0 is disabled - 1 pts
SMB over QUIC is enabled on Server and Client - 2 pts
SMB Blocks NTLM is enabled - 2 pts
Authenticator Rate Limiter is enabled - 1 pts
A Minimum SMB Version(3.0.0+) is configured - 2 pts
Require use of specific security layer for RDP set to TLS - 2 pts
An Invalid Authentication Delay exists on the system - 2 pts
CAPolicy.inf insecure permissions fixed - 2 pts
AD CS disallowed certs auto update is enabled - 3 pts
VBS is in Mandatory Mode - 1 pts
Machine Identity Isolation is set to audit mode or enforcement mode - 2 pts
Domain Controllers group is no longer managed by Domain Guests - 2 pts
Everyone does not have FullControl rights on the domain - 2 pts
msDS-KeyCredential object '05jf' is deleted from LostAndFound - 2 pts
Enterprise Admins no longer managed by Users - 2 pts
Chrome sends a Do Not Track request - 2 pts

Conclusion, Notes, and Future Considerations

Most of the SMB Vulnerabilities come from the new Windows Server 2025 features. Microsoft officially released their own baseline, which you should look into as it is helpful in securing Windows Server 2025 as there are currently(as of February 2025) no DoD stigs, nor CIS Benchmarks for Windows Server 2025. You can find an article about the OSConfig PowerShell module here. Most of the vulnerabilities inside the VM are some of the few in the same area/cluster that need to be configured. For example, the vulnerability “Machine Identity Isolation is set to audit mode or enforcement mode” is one of the many settings that need to be configured inside of the “Turn On Virtualization Based Security.” We have not included all of the vulnerabilities in these areas as it would be extraneous, so it is up to you to study the new features.

To the people who have not completed the virtual machine to the best of your ability, or looked at this walkthrough without a valid attempt on the VM: As lolmenow stated, it is up to you to decide whether or not you truly want to gain experience; it only hurts you if you cheat.

We hope that everyone has enjoyed trying this VM and that you have learned something from it. If you have any questions regarding the vulnerabilities or this walkthrough, dm lolmenow or a_person.