# Nessus Vulnerability Management

I have 2 VMS set in place (Kali VM has the Nessus)

For My person lab what we are going to do is a basic scan to the "**Windows 11 VM**" Machine which is a VM that I downloaded to do labs related to Windows or AD, I won't be showing how to install it because that is out of the intentions of this lab.

The point of scanning this machine, is that I want to get some kind of result back. As we can see I have 2 VM's the "*Kali*" and the "*Windows 11 VM*"
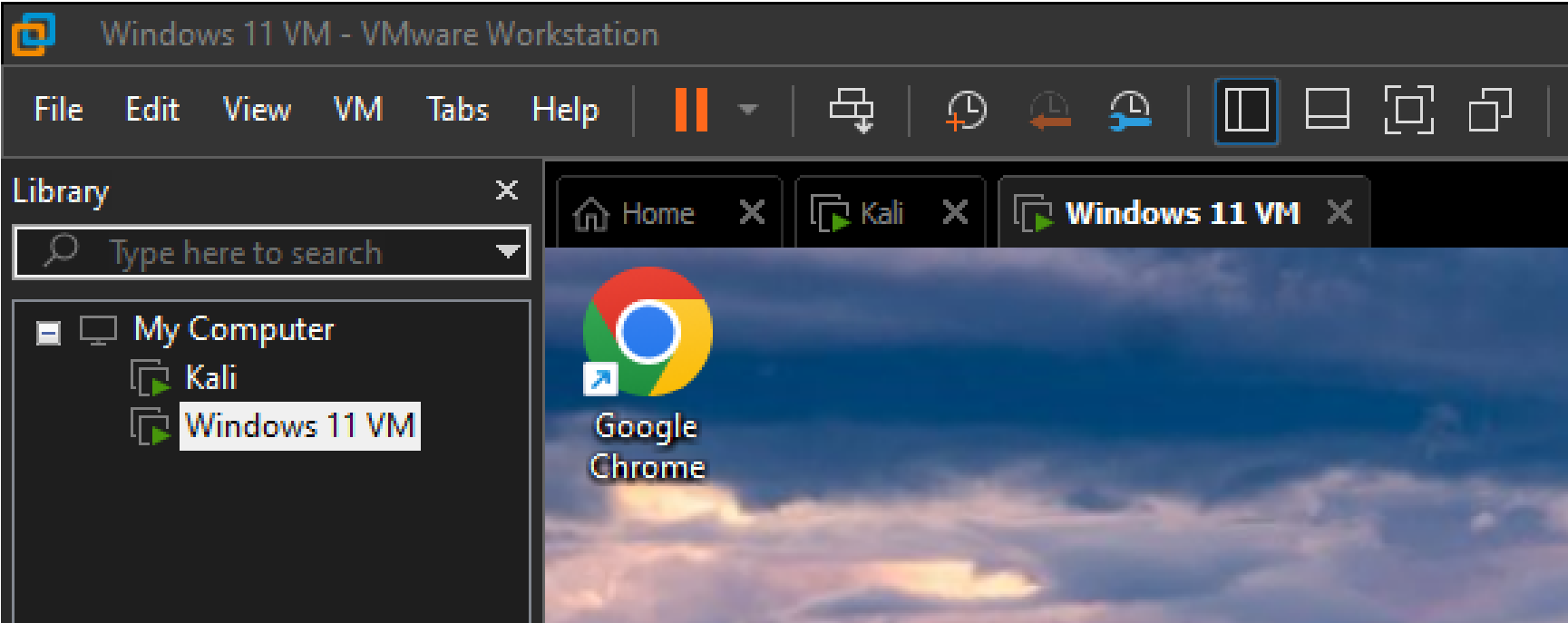
First of all what we are going to do is get the "*Windows 11 VM*" Ip (As well in order for the machine to communicate properly with the VM or just to be in the same network as my Physical Computer, the *"Network Adapter"* has to be configured to **Bridged**)

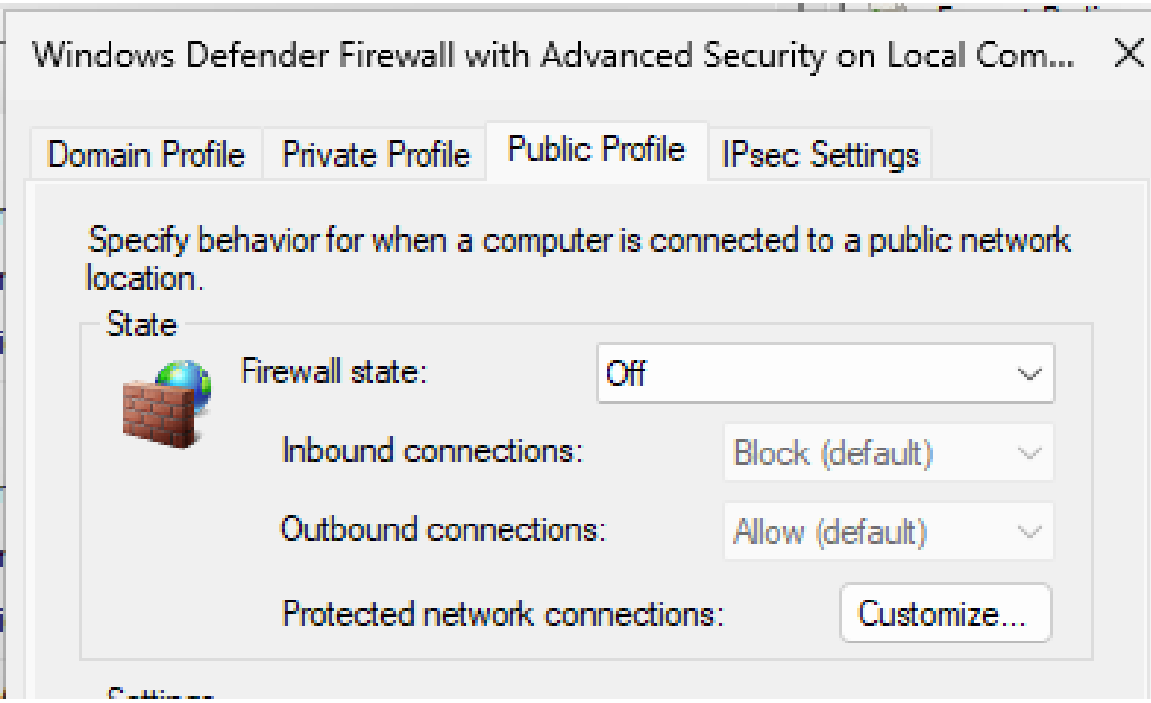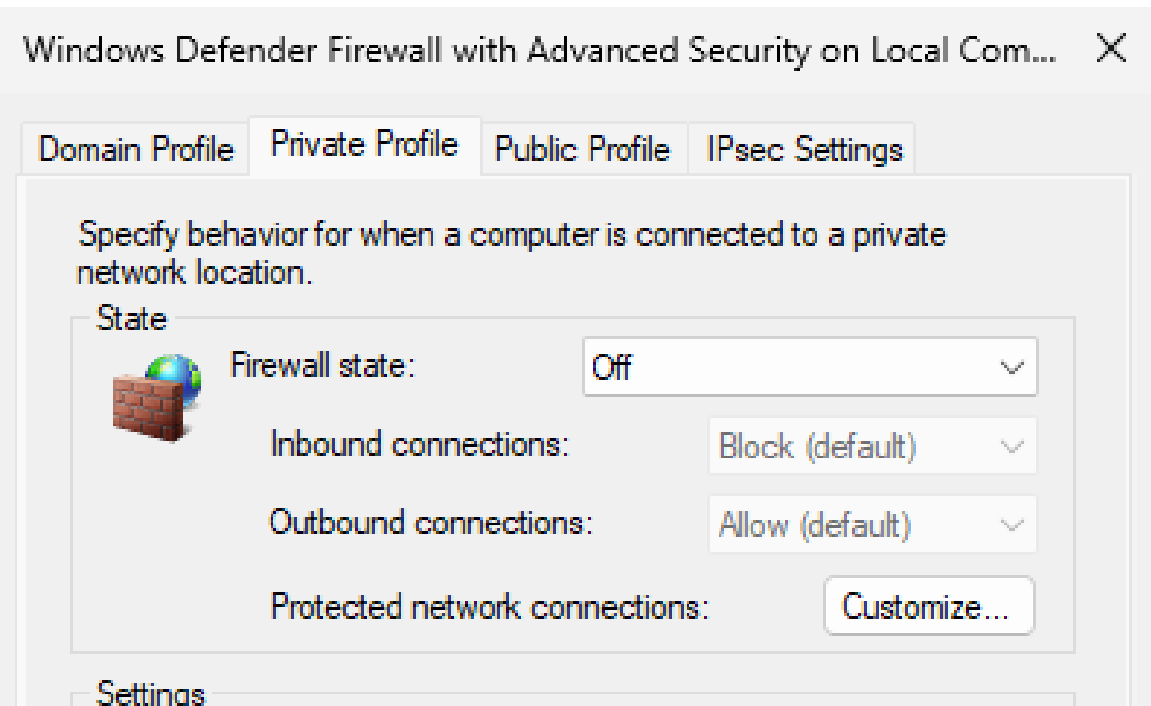Now what we do, we have to go to the "*Windows 11 VM*" and get the IP address

Now to make sure that we are able to ping the Windows VM, we have to disable the firewall in it

First of all, we go to "*wf.msc*" which is the Windows Firewall Console
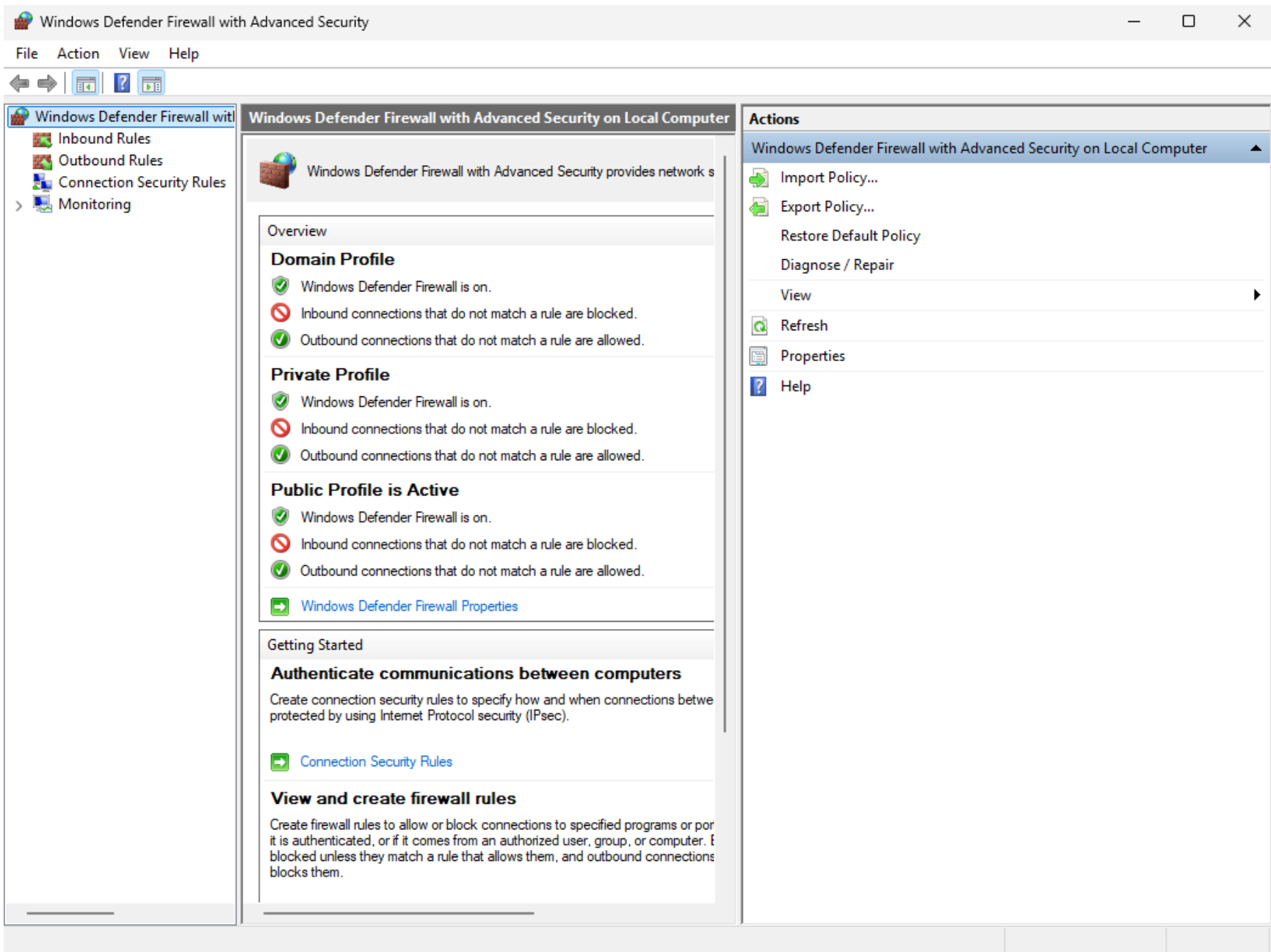
After that we have to turn all of these profiles off
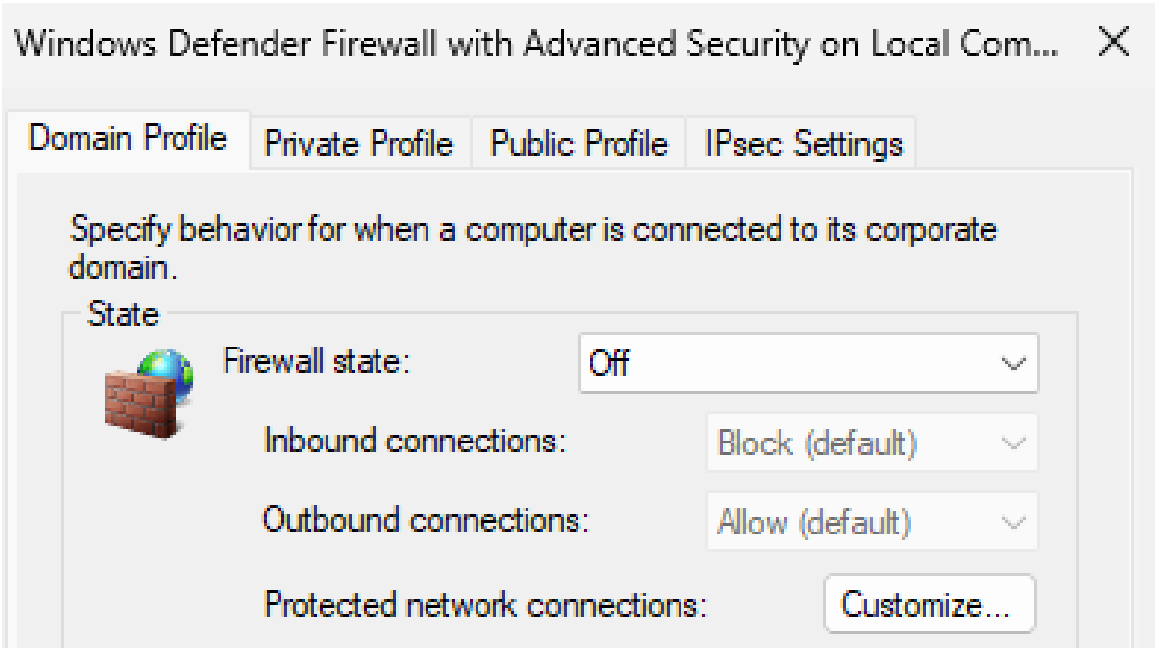
Now from my Physical Machine, lets ping the VM

As we can see, we can ping the Windows VM from our Kali Machine. Now lets go over to Nessus to create a scan for the Windows VM

This was all I used for this lab. What I wanted to do is a simple port scan just to see if it's working and if we can any information to work on

After Running the script this is what I found in the Windows VM

Scan Details

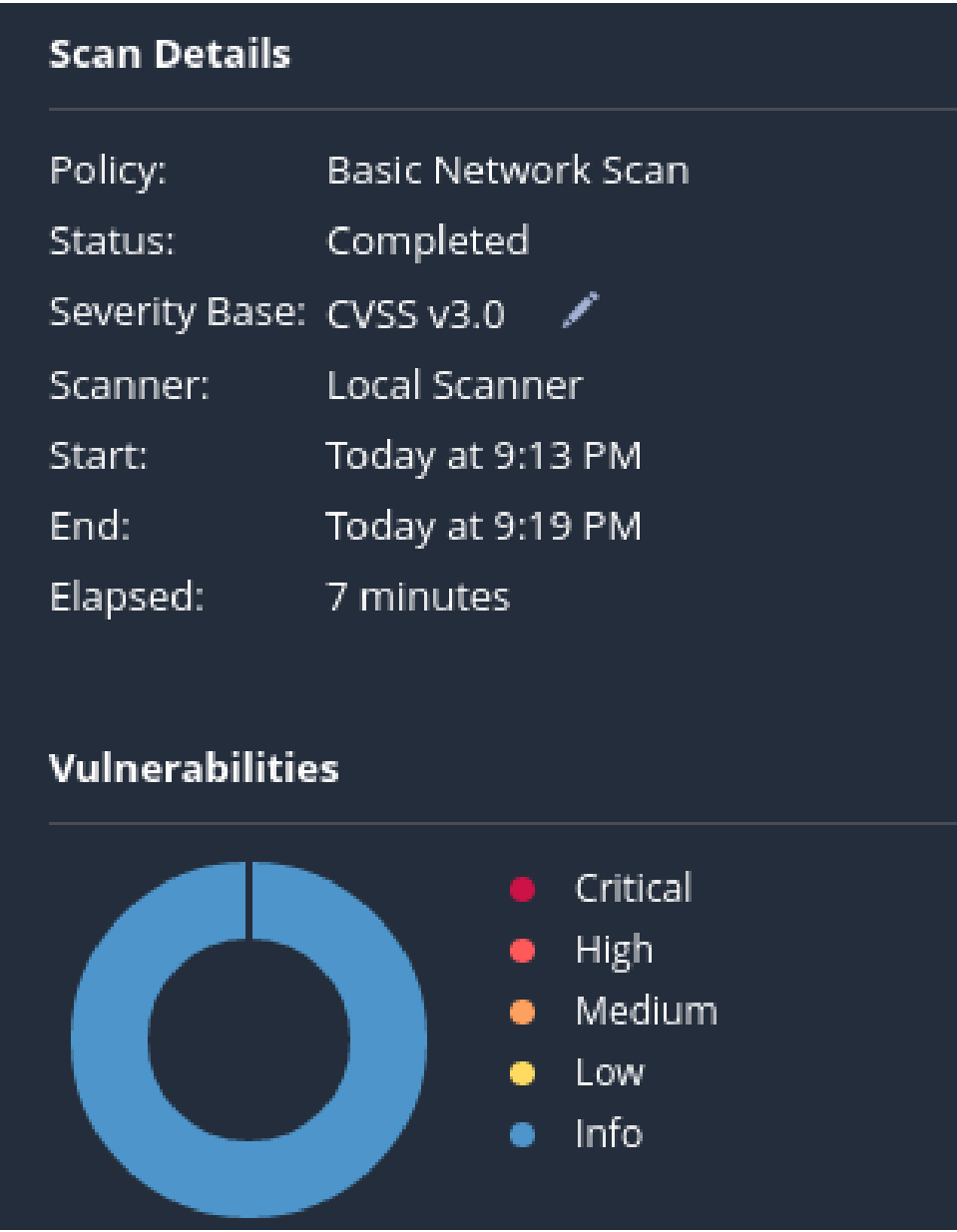Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:13 PM
End: Today at 9:19 PM
Elapsed: 7 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

As we can see this was the result of the scan, the findings are labeled as "INFO" they're not necessarily vulnerabilities but they are information about the system that we should be aware of. Also I found some cool information from the scans

| | INFO | | VMware Virtual Machine Detection |

INFO VMware Virtual Machine Detection

Description
According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution
Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Output

```
The remote host is a VMware virtual machine.
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	10.0.0.211

It found out that the Windows Machine that it was scanned is a VM from VMWARE.

As we can see, we have the Traceroute information which means that this machine accepts ICMP requests

We can see that "**SMB**" was detected and is listening on Port 445, also in the description says that Nessus was not able to authenticate to the remote target, this is only because we did not provide any credentials to the

machine

Now for the next scan, what I will do is I will make sure that the Windows WM is able to accept authenticated scans, as well, we will provide credentials to Nessus.

What I did is I went to "*services*"
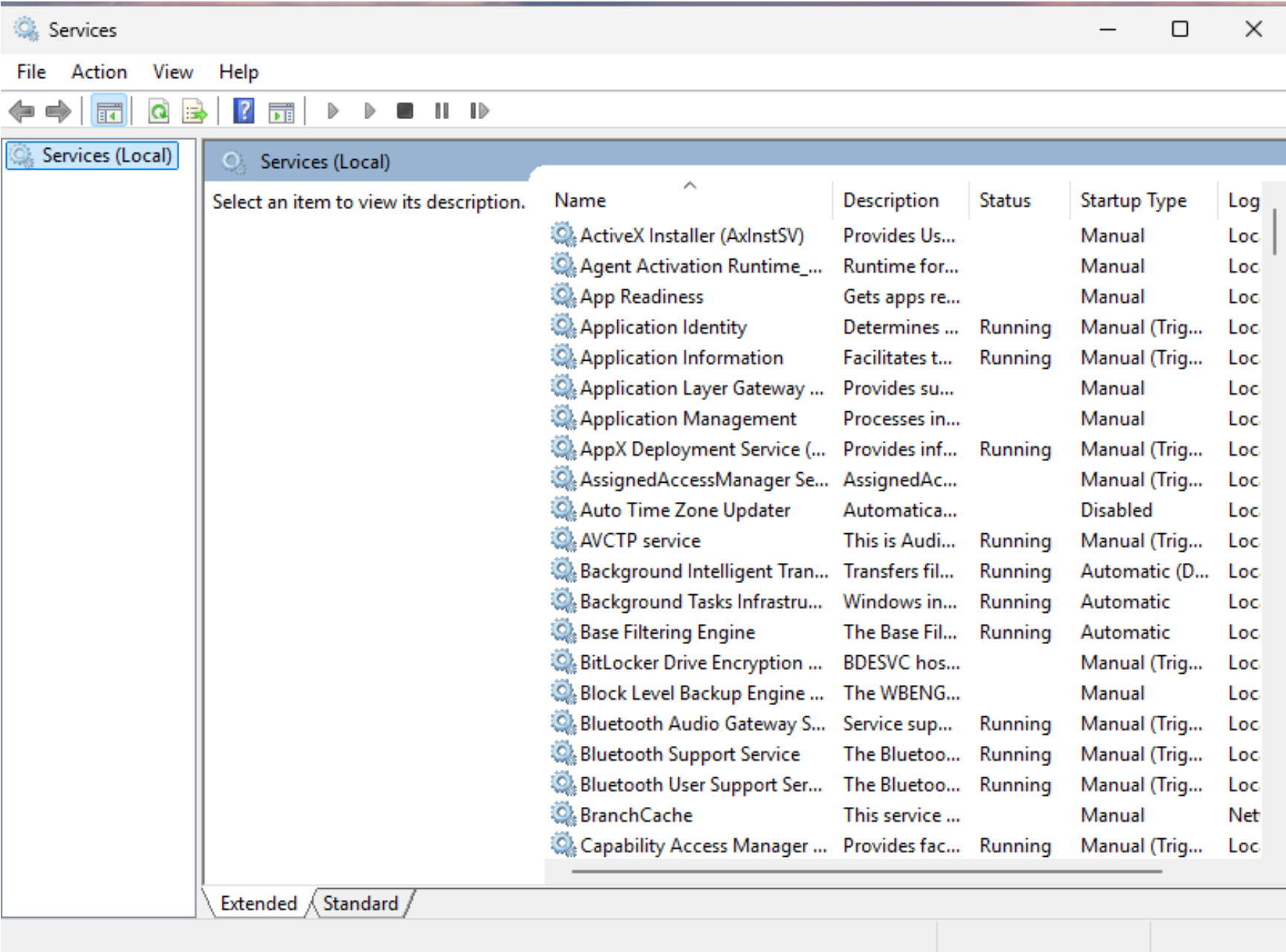
First what we allow is the "*Remote Registry*", it allows for the scanner to connect to the computers registry and go through the registry and look for poor/insecure configurations
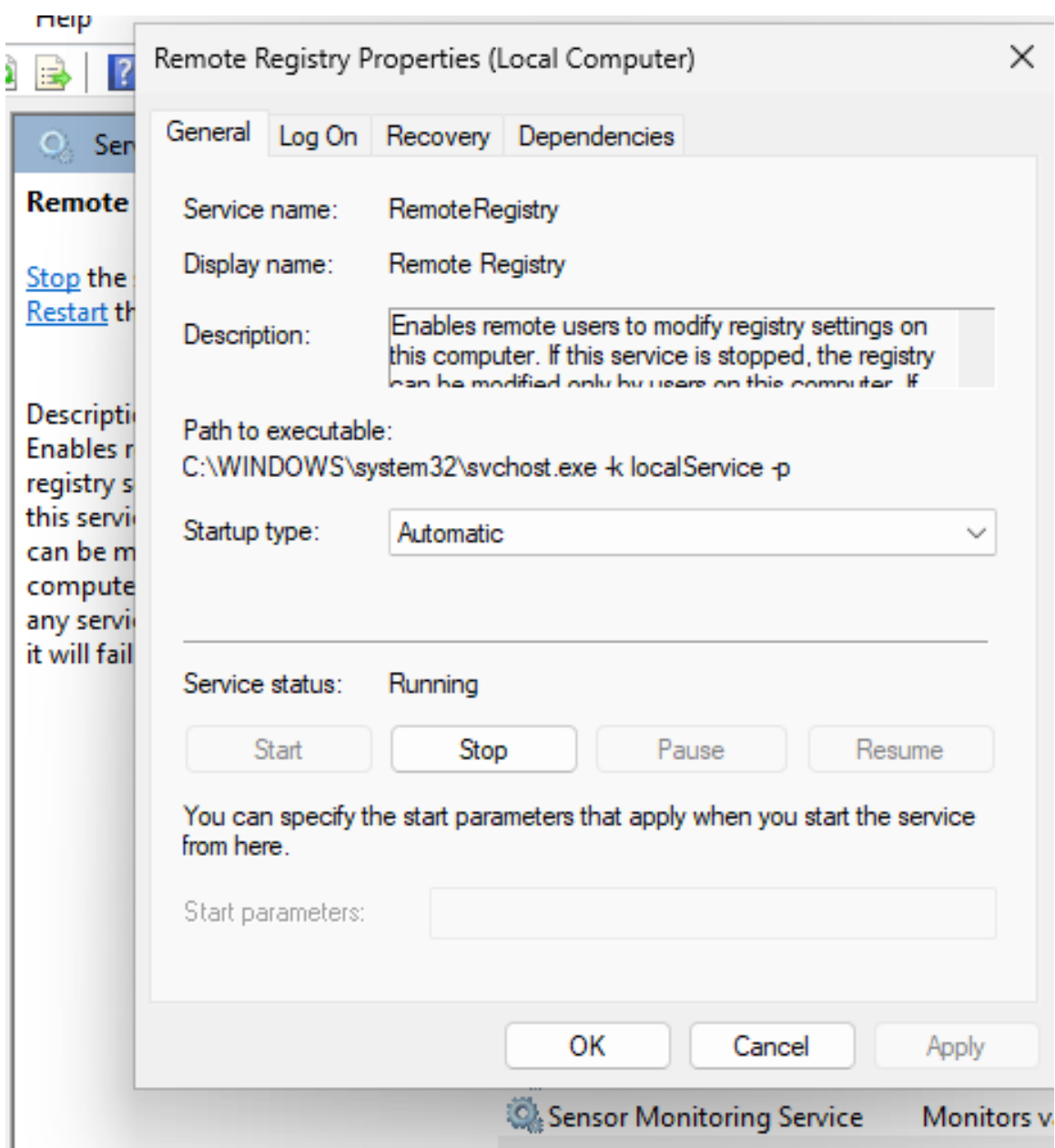
Also I double checked if the file and printer sharing, and Network discovery was on, which it was.
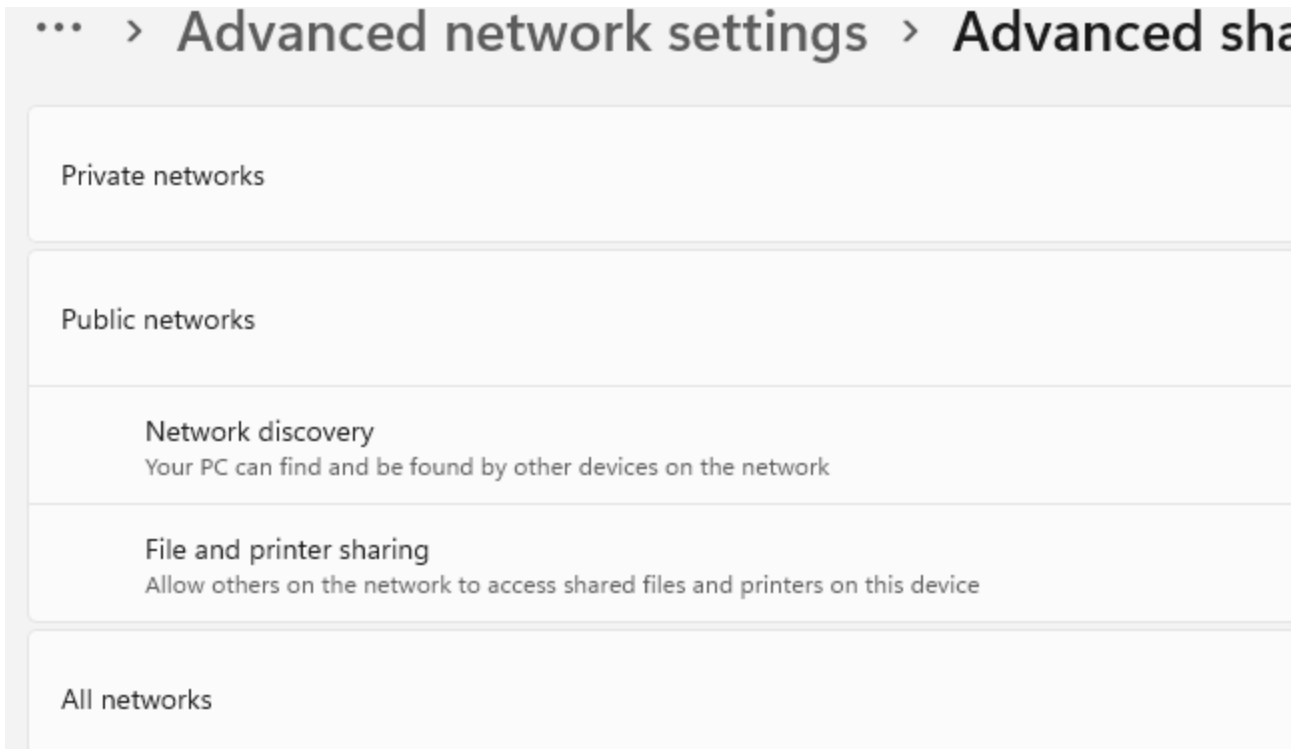
I disabled this, which is not recommended at all to do, but I did it only because we need this off in order to scan the machine with no issues.

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

ⓘ Not recommended.

Never notify

I went to the registry editor, this is just because we want to add a key and this is supposed to further disable user account control for the remote account
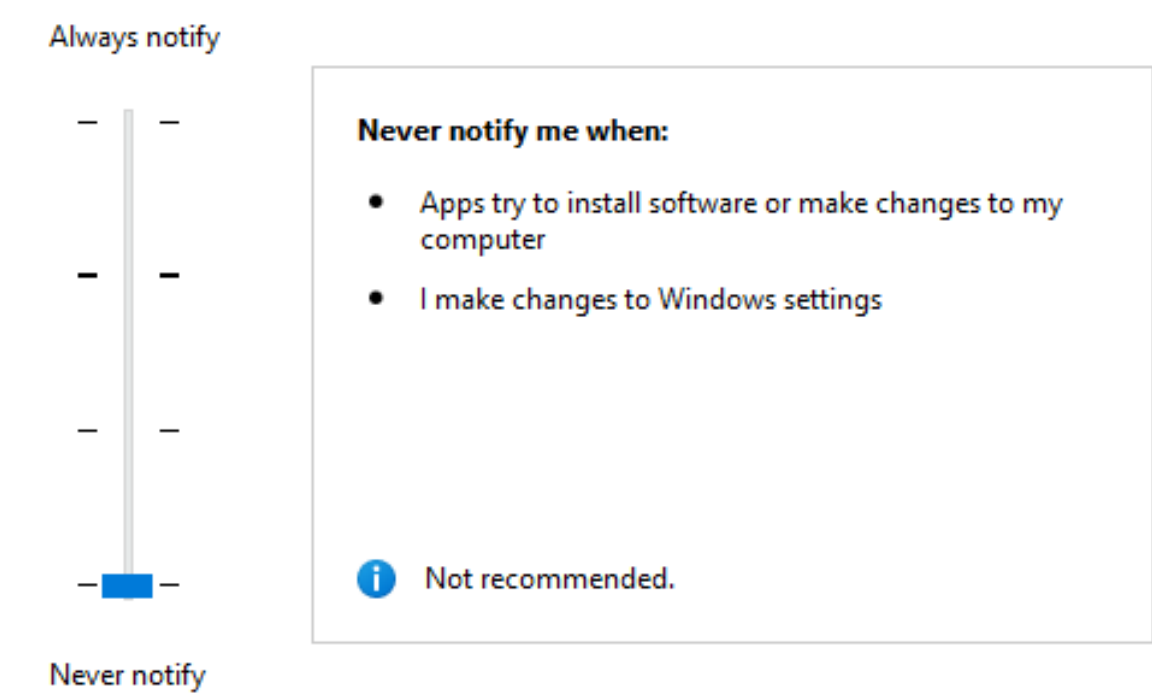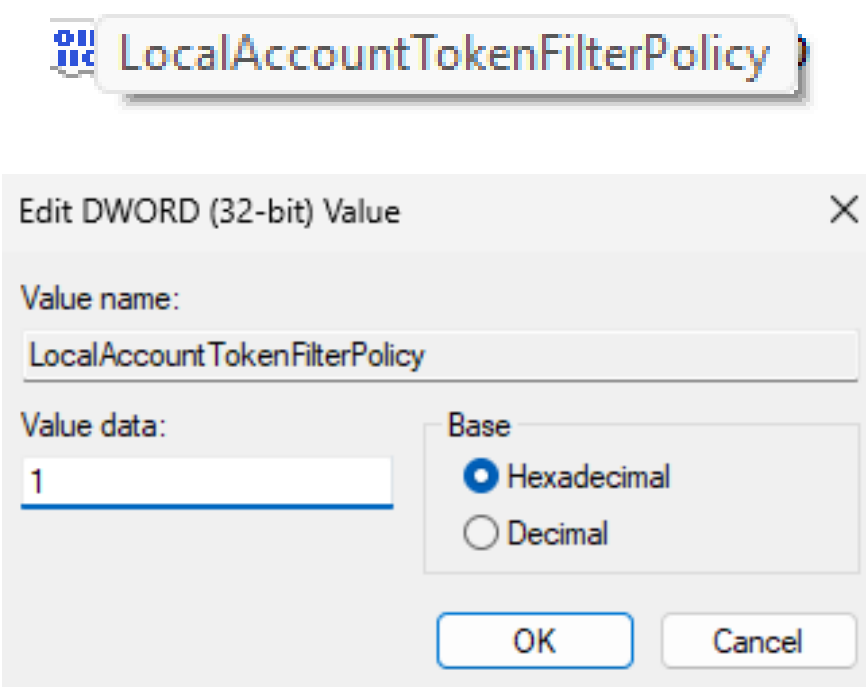
We went to this directory in the registry

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

We added this account token and the, and we set the value to 1, it was originally 0

LocalAccountTokenFilterPolicy

Edit DWORD (32-bit) Value   ✕

Value name:

LocalAccountTokenFilterPolicy

Value data: Base
1   ⦿ Hexadecimal
                             ◯ Decimal

           OK   Cancel

After that I just restarted the machine just to make sure that all the configurations that I made in the VM were set

Now we're ready to scan the machine again! What I did is that I edited the previous scan and I added the credentials to Nessus

After running the scan this was the result!

Because we used the credentials we were able to look for vulnerabilities inside the machine because we were authenticated in the machine, this way we were able to get more "info" based vulnerabilities

We found a "High" vulnerability!

The CVE-2013-3900 is basically a vulnerability is a remote code execution vulnerability that exists because just the way "**WinVerifyTrust**" authenticates.

In a attack scenario, the threat actor may send a fishing email and if the user opens this "**PE**" file, which in short, comparing to "**.EXE**", are files that contain important information for the operating system to correctly load the executable code, and "**.EXE**" we know it is the file format for a executable file.

For more information about this vulnerability, her is the windows security updates link:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

Windows 11 Basic Scan (Personal Lab) / Plugin #166555
‹ Back to Vulnerabilities

| Hosts 1 | **Vulnerabilities 42** | History 4 |

HIGH   WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Description
The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

Solution
Add and enable registry value EnableCertPaddingCheck:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

See Also
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900
http://www.nessus.org/u?9780b9d2

Output

```
Nessus detected the following potentially insecure registry key configuration:
    - Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the registry.
    - Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the registry.
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	10.0.0.211

As well when running this scan it found the device hostname

Windows 11 Basic Scan (Personal Lab) / Plugin #55472

‹ Back to Vulnerabilities

| Hosts 1 | **Vulnerabilities** 42 | History 4 |

INFO **Device Hostname**

Description

This plugin reports a device's hostname collected via SSH or WMI.

Output

```
    Hostname : WINDOWSXPLOIT
       WINDOWSXPLOIT (WMI)
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	10.0.0.211

Also, it found my OS version

Windows 11 Basic Scan (Personal Lab) / Plugin #11936

‹ Back to Vulnerabilities

| Hosts 1 | **Vulnerabilities** 42 | History 4 |

INFO OS Identification

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Output

```
  Remote operating system : Microsoft Windows 11 Pro Build 26100
  Confidence level : 101
  Method : Misc


  The remote host is running Microsoft Windows 11 Pro Build 26100
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	10.0.0.211

And lastly, another information that I thought it was really cool is that found all the usernames in the system

Now for the last part, as my Windows VM seemed that it did not have a lot of vulnerabilities or that we did not see more medium to critical vulnerabilities, what I decided is downloading a very or software just to see if Nessus would find any vulnerabilities associated with it

For that I just downloaded a old firefox

I went to the website and I downloaded a random old one

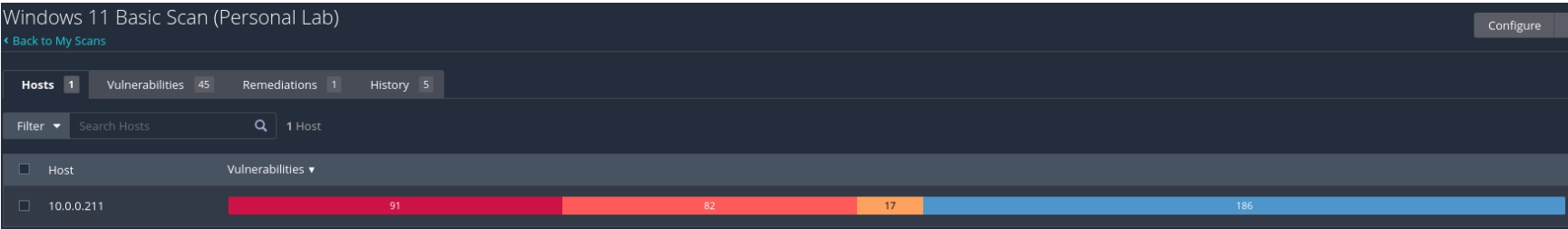This is how it looks (in the website it says that it was last updated in 2023 but its a pretty old Firefox, here is the GUI for example)
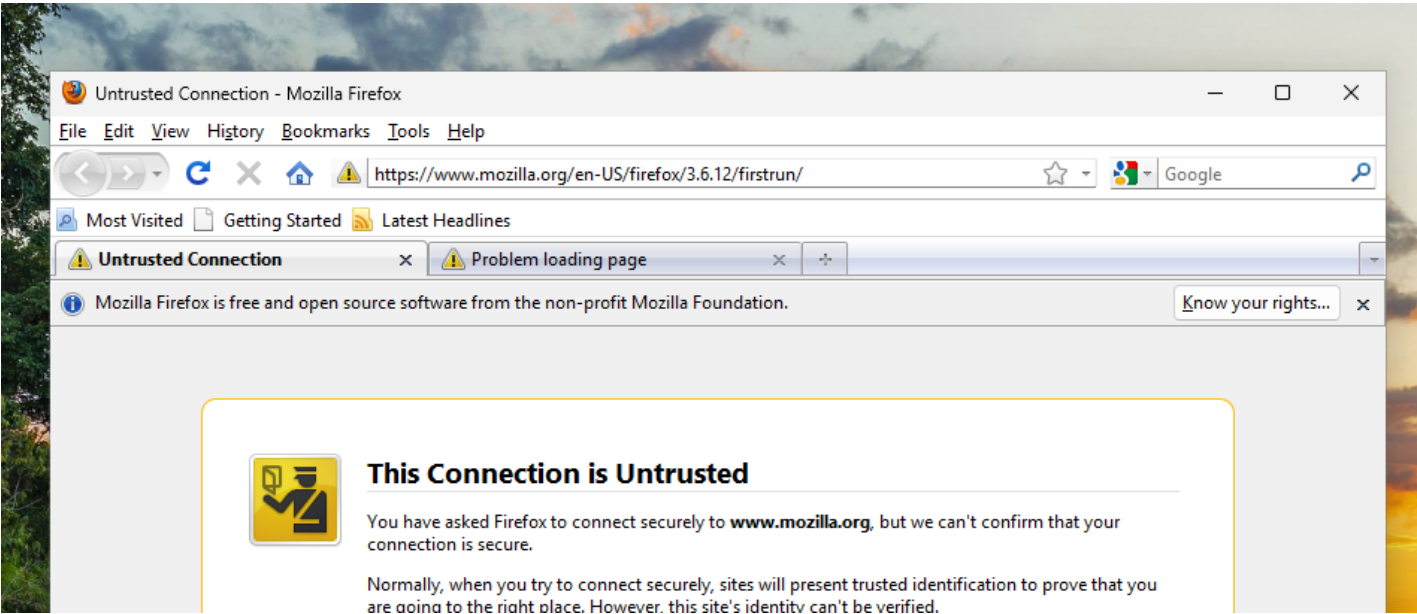
As we can see is really old

Now what we do is we just run our Nessus scan again!

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:12 PM
End:	Today at 8:24 PM
Elapsed:	12 minutes

Vulnerabilities

- Critical
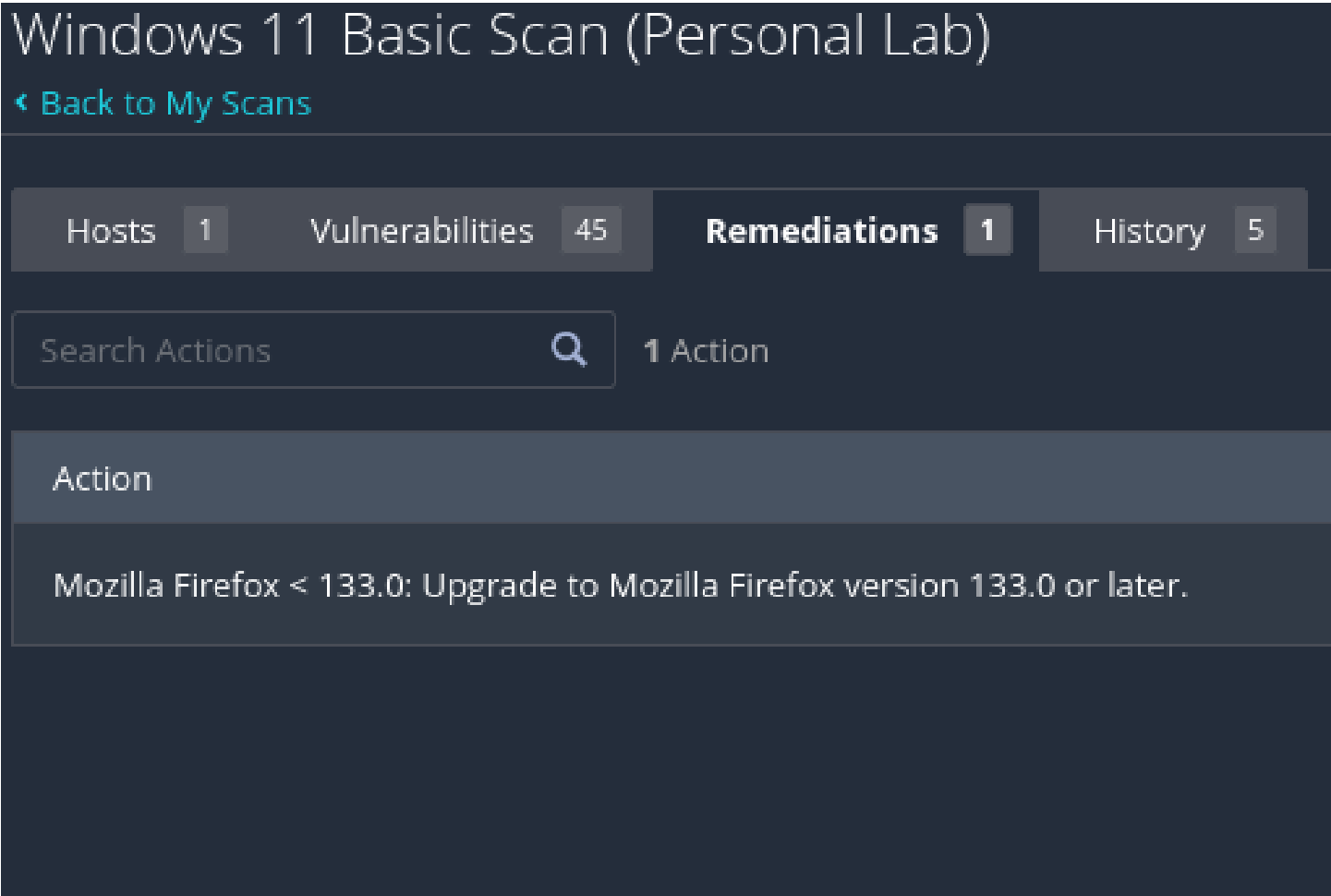- High
- Medium
- Low
- Info

We found a lot of vulnerabilities related to Firefox!

Most of them are High to Critical

And we know the reason why Nessus has found a lot of vulnerabilities, is due to the fact that this Firefox is really old and there is a lot of known vulnerabilities about it.

The easiest way to fix it is of course upgrade the Firefox to the newest version, or just deleting it completely

If we go to remediations this is the only option that it gives us

Windows 11 Basic Scan (Personal Lab)
‹ Back to My Scans

| Hosts 1 | Vulnerabilities 45 | **Remediations 1** | History 5 |

Search Actions 🔍 **1** Action

Action

Mozilla Firefox < 133.0: Upgrade to Mozilla Firefox version 133.0 or later.

This is example of one of the critical vulnerabilities reported by Nessus about this old Firefox

Windows 11 Basic Scan (Personal Lab) / Plugin #63551
‹ Back to Vulnerability Group

| Hosts 1 | **Vulnerabilities 45** | Remediations 1 | History 5 |

CRITICAL Firefox < 18.0 Multiple Vulnerabilities

Description
The installed version of Firefox is earlier than 18.0 and thus, is potentially affected by the following security issues :

- Multiple, unspecified use-after-free, out-of-bounds read and buffer overflow errors exist. (CVE-2012-5829, CVE-2013-0760, CVE-2013-0761, CVE-2013-0762, CVE-2013-0763, CVE-2013-0766, CVE-2013-0767, CVE-2013-0771)

- Two intermediate certificates were improperly issued by TURKTRUST certificate authority. (CVE-2013-0743)

- A use-after-free error exists related to displaying HTML tables with many columns and column groups. (CVE-2013-0744)

Now what I will do is I will try my best to remediate the vulnerabilities found by Nessus, and what I will do is simply is just delete Firefox and then I will see if there is any updates available for my Windows VM

Its updated!

And this is the new scan!

It is the same as the previous scan that we added the credentials, but we far less vulnerabilities than when we downloaded the old Firefox