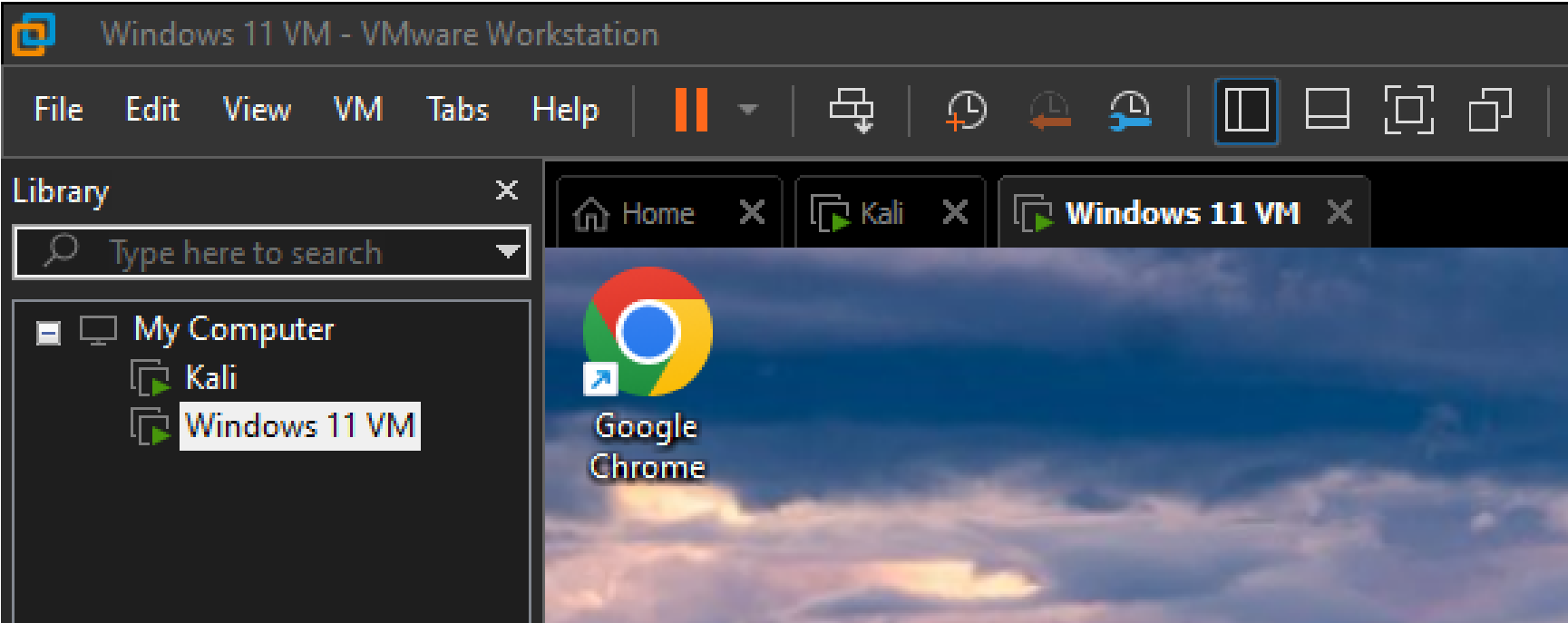


Nessus Vulnerability Management

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

```
PS C:\Users\yaser\OneDrive\Desktop> ipconfig

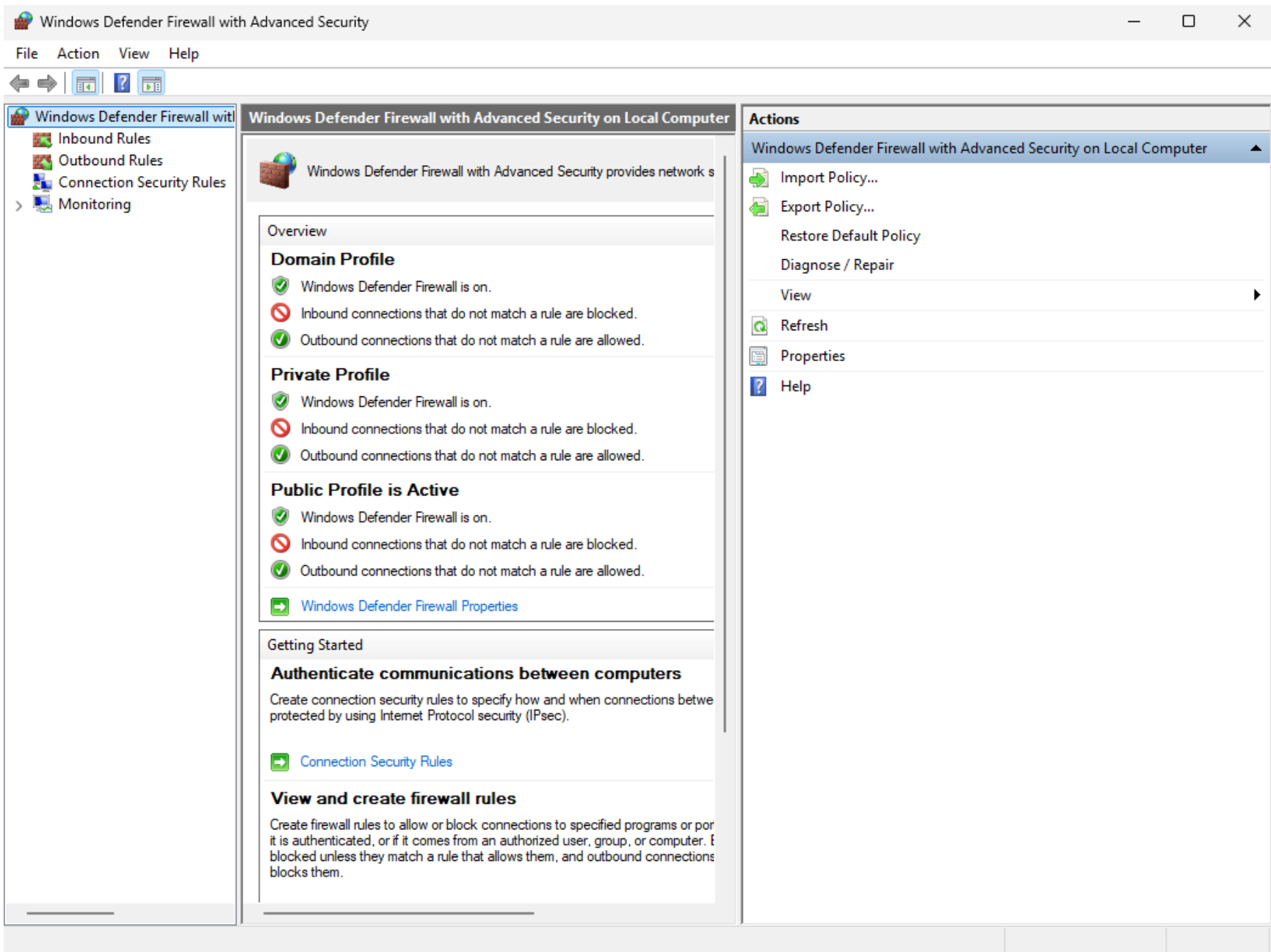
Windows IP Configuration

Ethernet adapter Ethernet0:

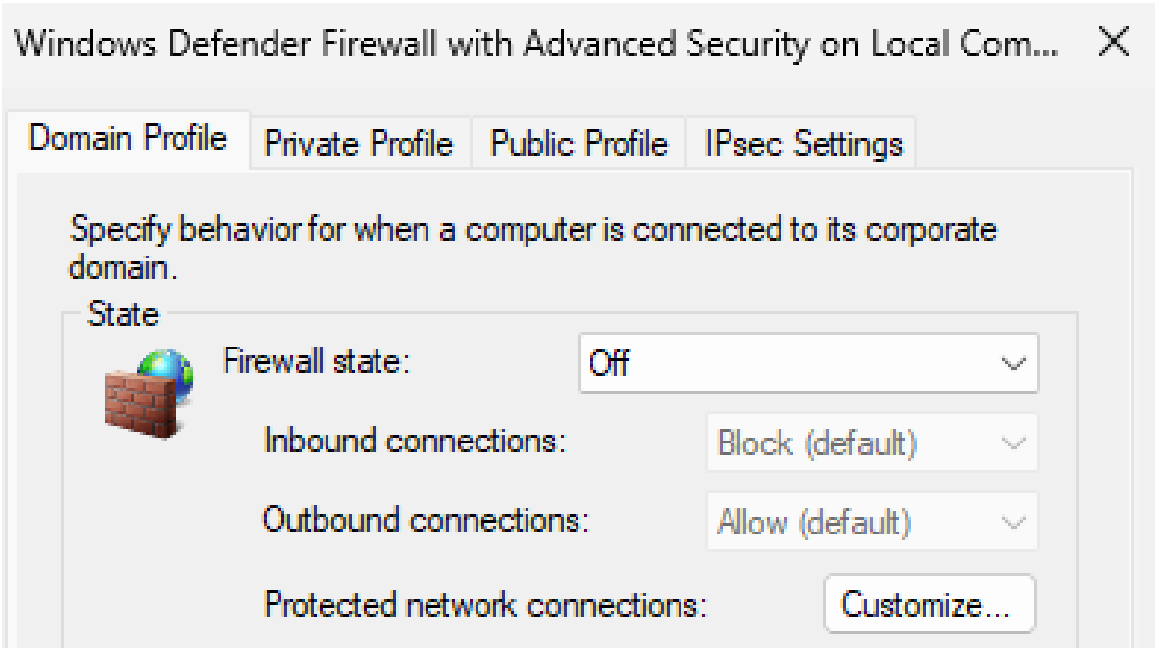
    Connection-specific DNS Suffix  . : phub.net.cable.rogers.com
    IPv6 Address. . . . . : 2607:fea8:4fa0:ac00::5aeb
    IPv6 Address. . . . . : 2607:fea8:4fa0:ac00:cabe:4ae3:8133:52fe
    Temporary IPv6 Address. . . . . : 2607:fea8:4fa0:ac00:6c71:49eb:60a3:a825
    Link-local IPv6 Address . . . . . : fe80::7b90:ae04:cd83:9cd9%13
    IPv4 Address. . . . . : 10.0.0.211
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c650:9cff:fea0:8e57%13
                                10.0.0.1
```

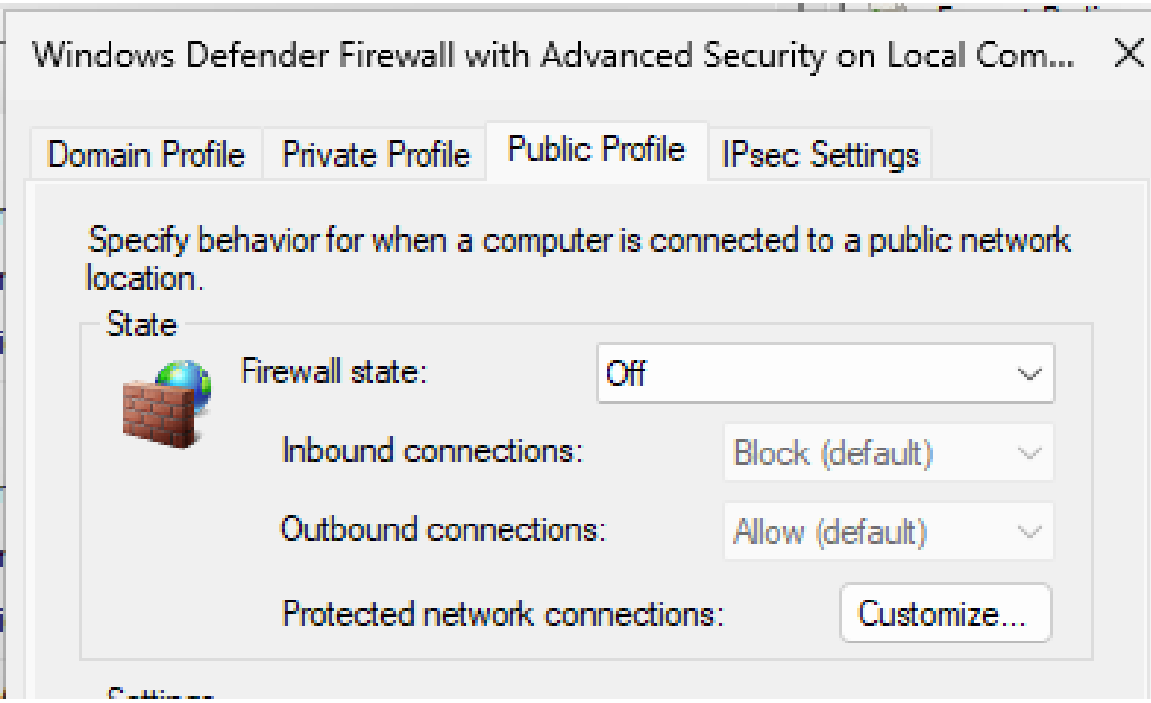
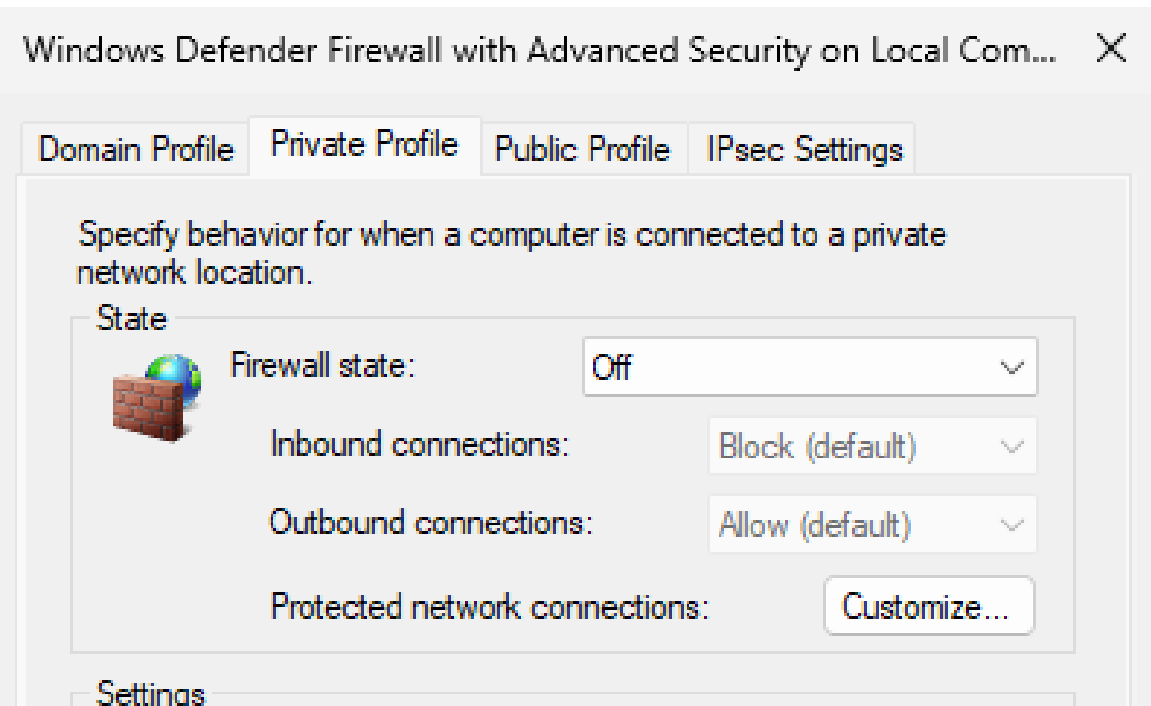
Now to make sure that we are able to ping the Windows VM, we have to disable the firewall in it

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

```
kali@Kali: ~  
File Actions Edit View Help  
(kali@Kali)-[~]  
$ ping 10.0.0.211  
PING 10.0.0.211 (10.0.0.211) 56(84) bytes of data.  
64 bytes from 10.0.0.211: icmp_seq=1 ttl=128 time=0.970 ms  
64 bytes from 10.0.0.211: icmp_seq=2 ttl=128 time=0.426 ms  
64 bytes from 10.0.0.211: icmp_seq=3 ttl=128 time=0.455 ms  
64 bytes from 10.0.0.211: icmp_seq=4 ttl=128 time=0.457 ms  
64 bytes from 10.0.0.211: icmp_seq=5 ttl=128 time=0.418 ms  
^C  
— 10.0.0.211 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4116ms  
rtt min/avg/max/mdev = 0.418/0.545/0.970/0.212 ms  
(kali@Kali)-[~]  
$
```

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

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Windows 11 Basic Scan (Personal Lab)

Description

Folder

My Scans

Targets

10.0.0.211

Upload Targets

Add File

Save

Cancel

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

Hosts1

Vulnerabilities14

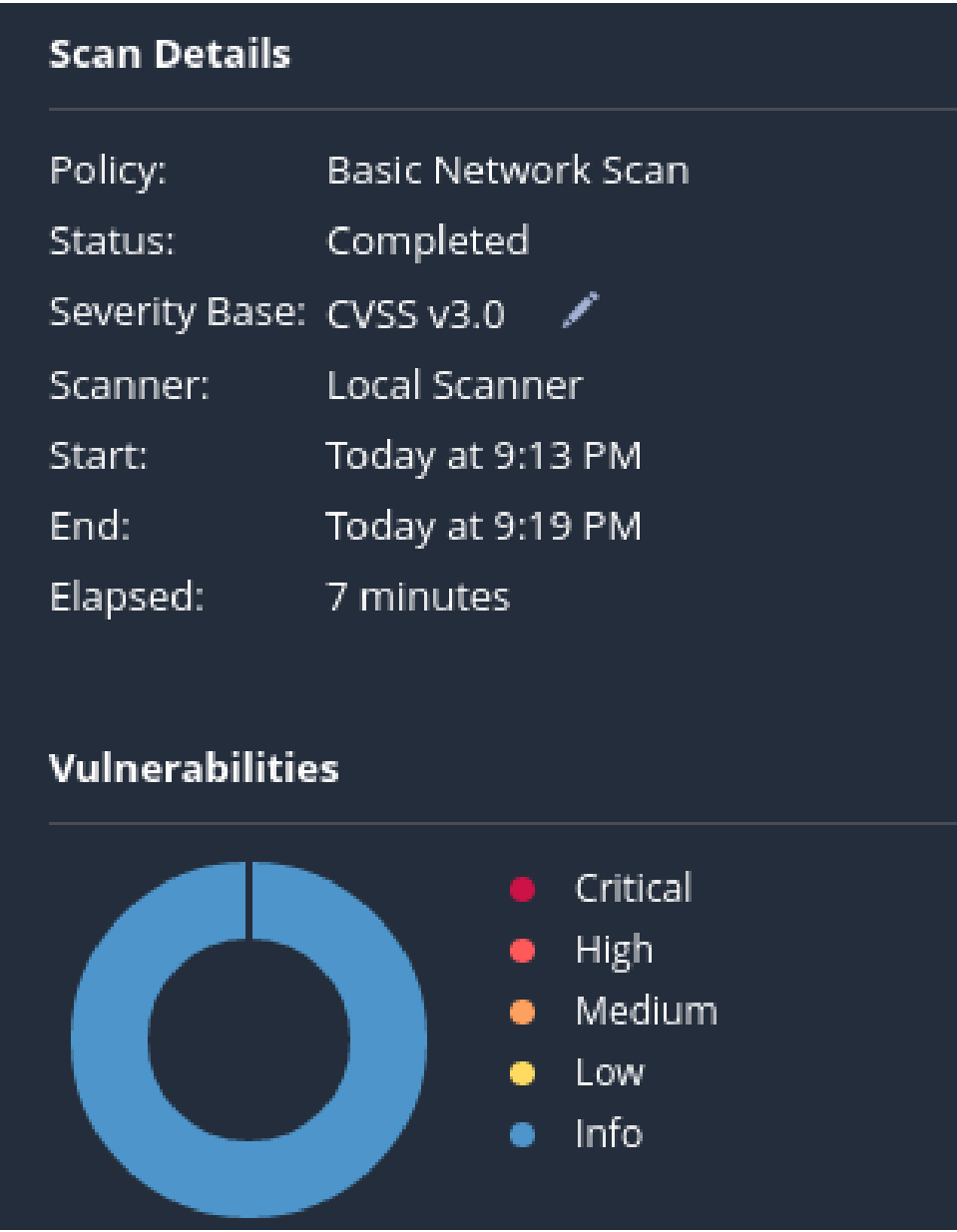
History4

Filter

Search Vulnerabilities

14 Vulnerabilities

	Sev	CVSS	VPR	EPSS	Name
<input type="checkbox"/>	INFO	<div>5</div> SMB (Multiple Issues)
<input type="checkbox"/>	INFO				DCE Services Enumeration
<input type="checkbox"/>	INFO				Nessus SYN scanner
<input type="checkbox"/>	INFO				Common Platform Enumeration (CPE)
<input type="checkbox"/>	INFO				Device Type



INFO

Traceroute Information

Description

Makes a traceroute to the remote host.

Output

For your information, here is the traceroute from 192.168.60.128 to 10.0.0.211 :

192.168.60.128

192.168.60.2

10.0.0.211

Hop Count: 2

To see debug logs, please visit individual host

Port ▲

Hosts

0 / udp

10.0.0.211

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

Windows 11 Basic Scan (Personal Lab) / Plugin #110723

< Back to Vulnerabilities

Hosts1

Vulnerabilities14

History1

INFO

Target Credential Status by Authentication Protocol - No Credentials Provided

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Output

SMB was detected on port 445 but no credentials were provided.

SMB local checks were not enabled.

To see debug logs, please visit individual host

Port ▲

Hosts

N/A

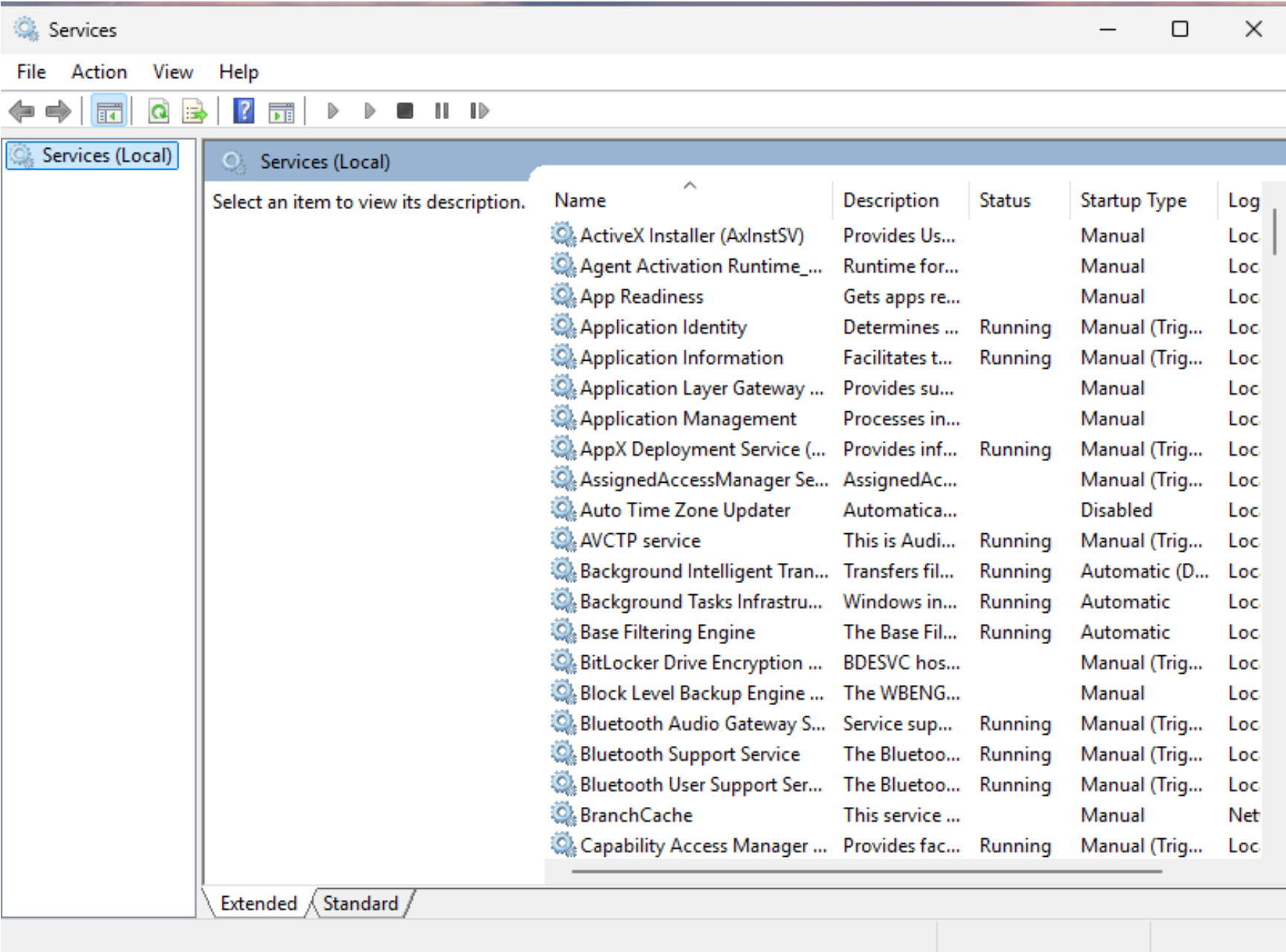
10.0.0.211

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

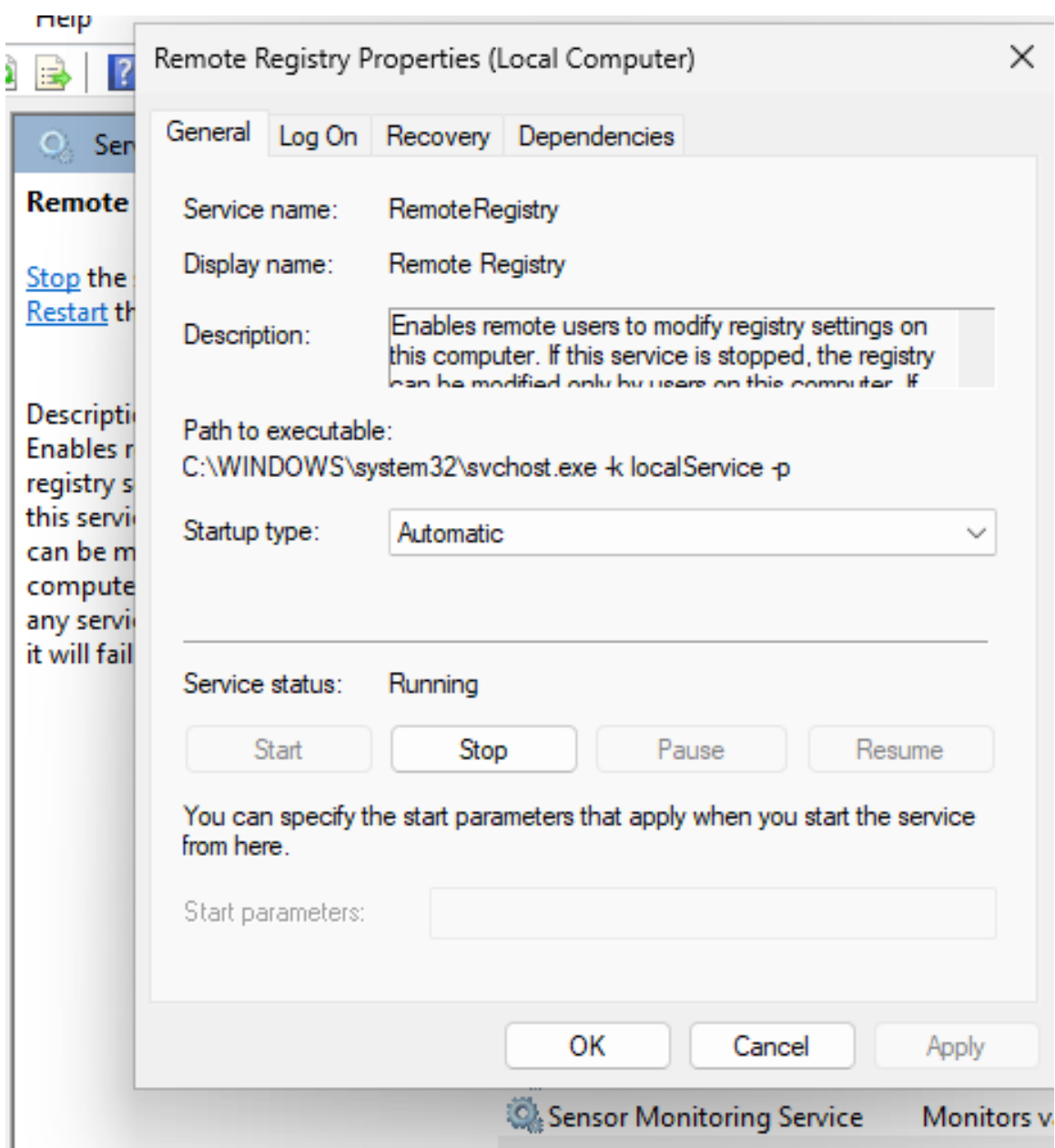
machine

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.

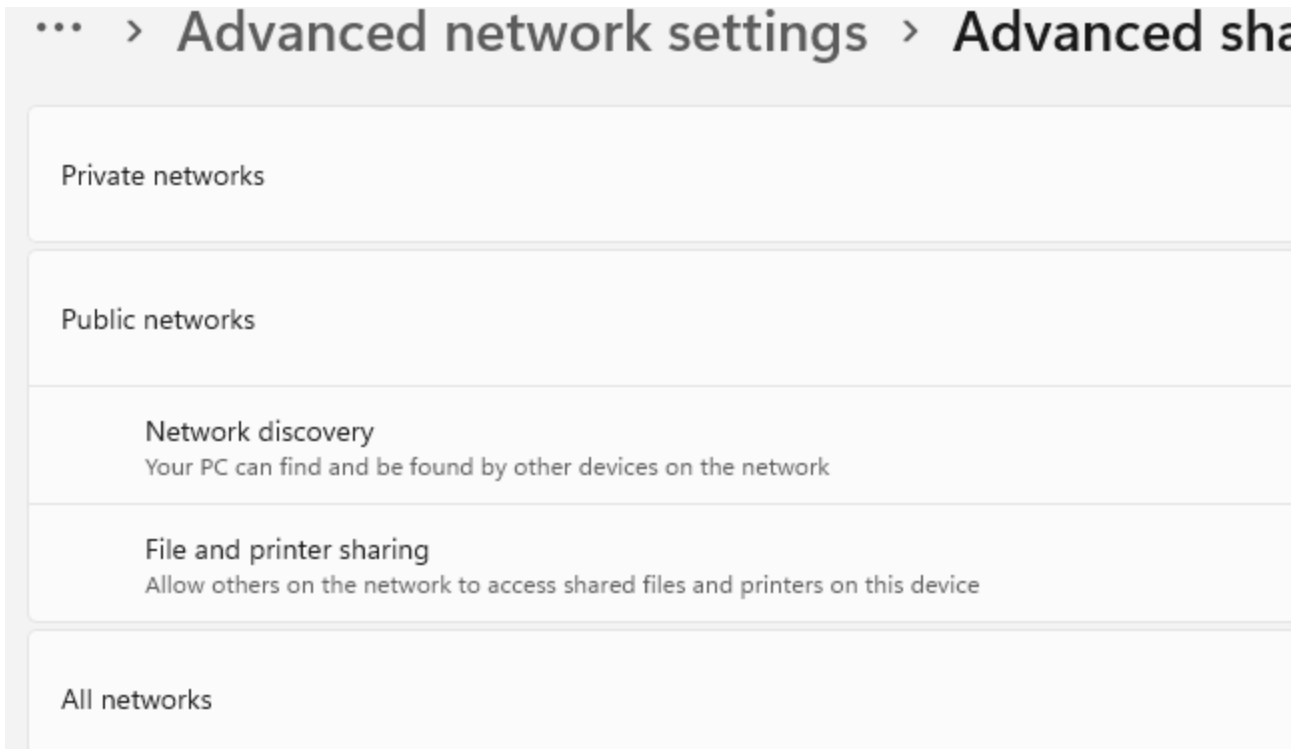
What I did is I went to **"services"**



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



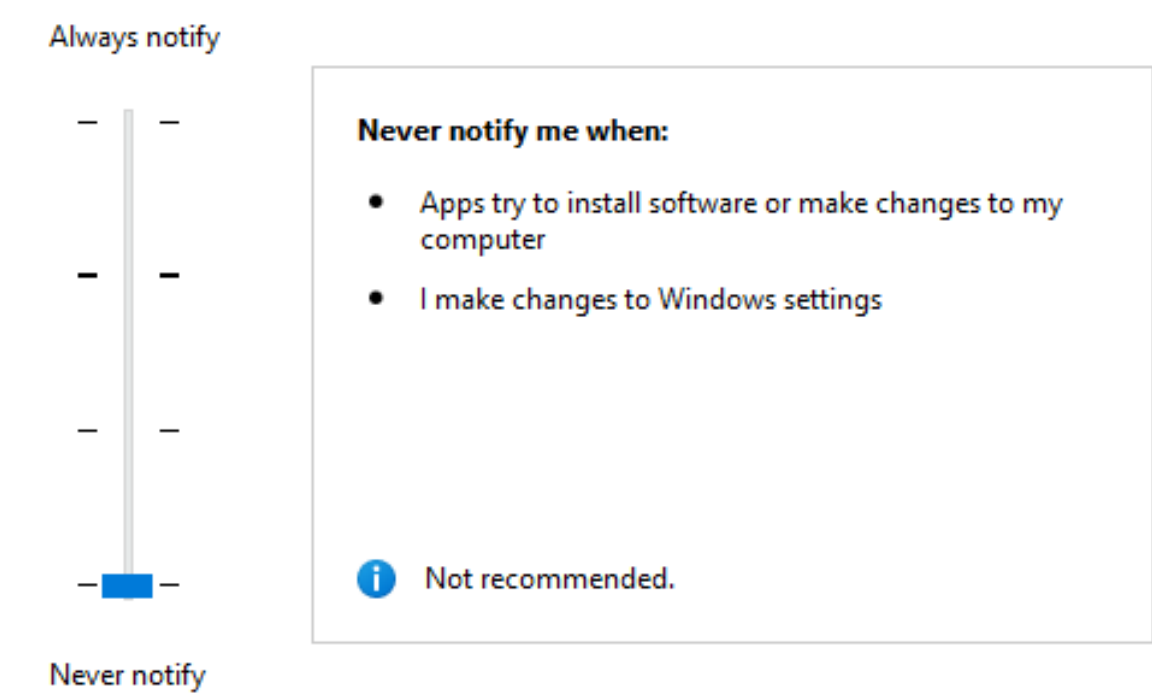
Also I double checked if the file and printer sharing, and Network discovery was on, which it was.



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](#)

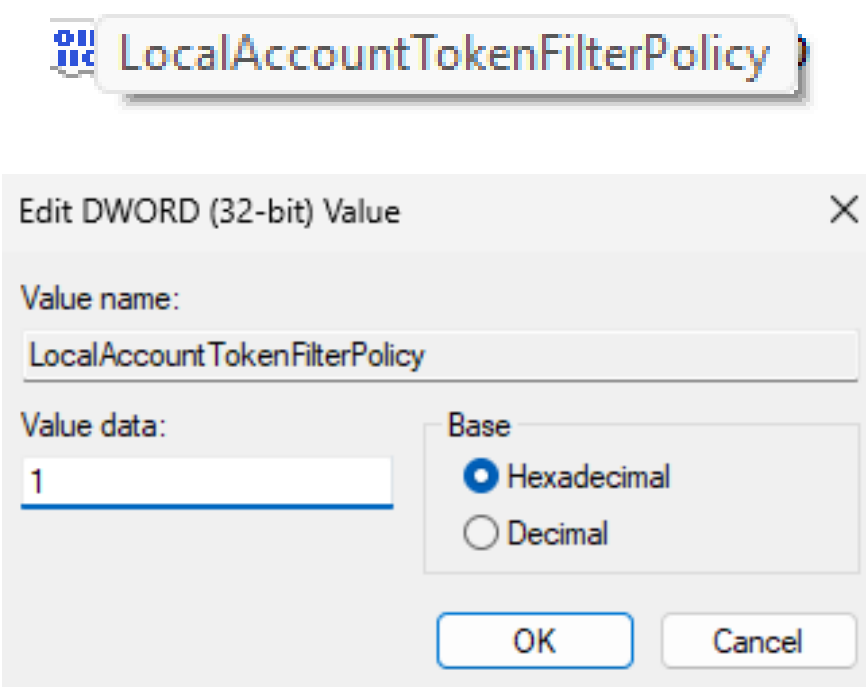


I went to the registry editor, this is just because we want to add a key and this is supposed to further disable user account control for the remote account

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



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

▼ Windows

User: admin, Auth method: Password

Authentication method

Password

Username

admin

Password

●●●●●●●●

Domain

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

Hosts1Vulnerabilities42History4

Filter▼Search Vulnerabilities42 Vulnerabilities

Sev▼	CVSS▼	VPR▼	EPSS▼	Name▲
<input type="checkbox"/> HIGH	8.8	8.9	0.6487	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
<input type="checkbox"/> INFO	63 Microsoft Windows (Multiple Issues)
<input type="checkbox"/> INFO	16 SMB (Multiple Issues)
<input type="checkbox"/> INFO	5 Microsoft Windows (Multiple Issues)
<input type="checkbox"/> INFO	3 Windows (Multiple Issues)

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>

[◀ Back to Vulnerabilities](#)

Hosts1

Vulnerabilities42

History4

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](#)

Hosts1

Vulnerabilities42

History4

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](#)

Hosts1

Vulnerabilities42

History4

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

Hosts1Vulnerabilities42History4

INFO

SMB Use Host SID to Enumerate Local Users

Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

Output

- Administrator (id 500, Administrator account)

- Guest (id 501, Guest account)

- yaser (id 1001)

- admin (id 1002)

Note that, in addition to the Administrator, Guest, and Kerberos accounts, Nessus has enumerated local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Enumerate Local Users: Start UID' and/or 'End UID' preferences under 'Assessment->Windows' and re-run the scan. Only UIDs between 1 and 2147483647 are allowed for this range.

To see debug logs, please visit individual host

Port▲

Hosts

445 / tcp / cifs

10.0.0.211

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

Google

download old firefox

×

AllImagesVideosNewsShoppingWebBooksMoreTools




Mozilla Support

https://support.mozilla.org › en-US › install-older-versi...

Install an older version of Firefox | Firefox Help

Downgrading to a previous Firefox version doesn't solve most problems. This article links to older versions and provides some alternatives.



Mozilla

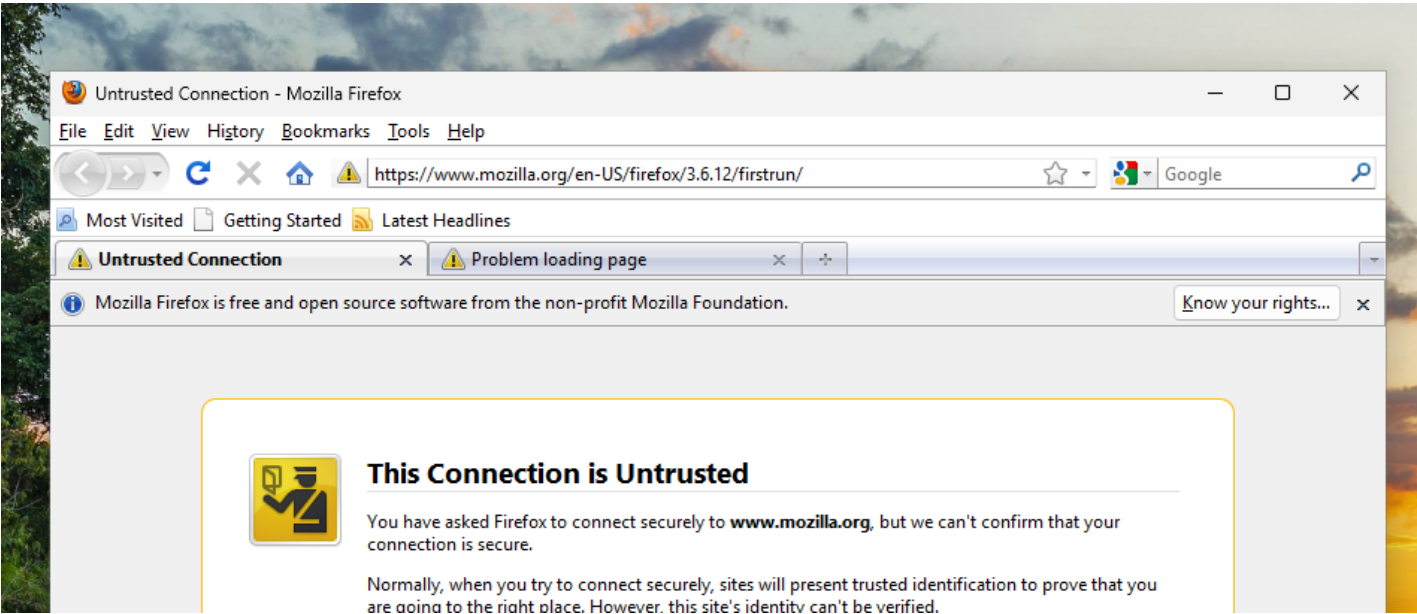
https://archive.mozilla.org › pub › firefox › releases

pub/firefox/releases

Index of /pub/firefox/releases/ Type Name Size Last Modified Dir Dir 0.40.4/ Dir 0.40.4/ Dir

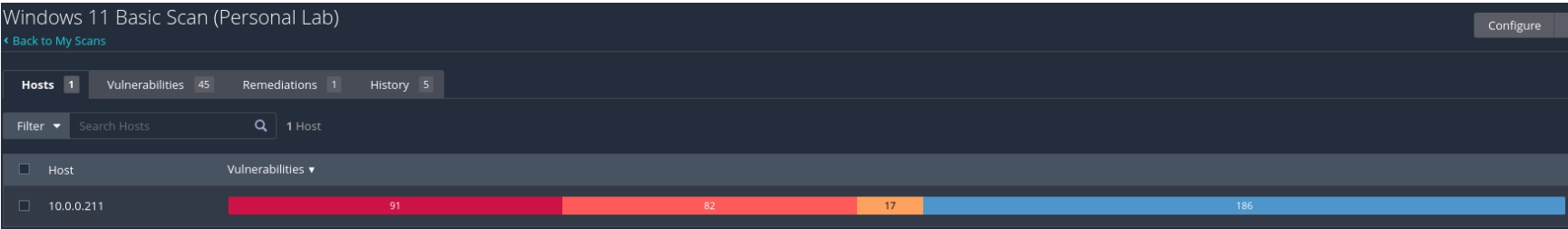
I went to the website and I downloaded a random old one

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!



Windows 11 Basic Scan (Personal Lab) / Mozilla Firefox (Multiple Issues)

[Back to Vulnerabilities](#)

Hosts1

Vulnerabilities45

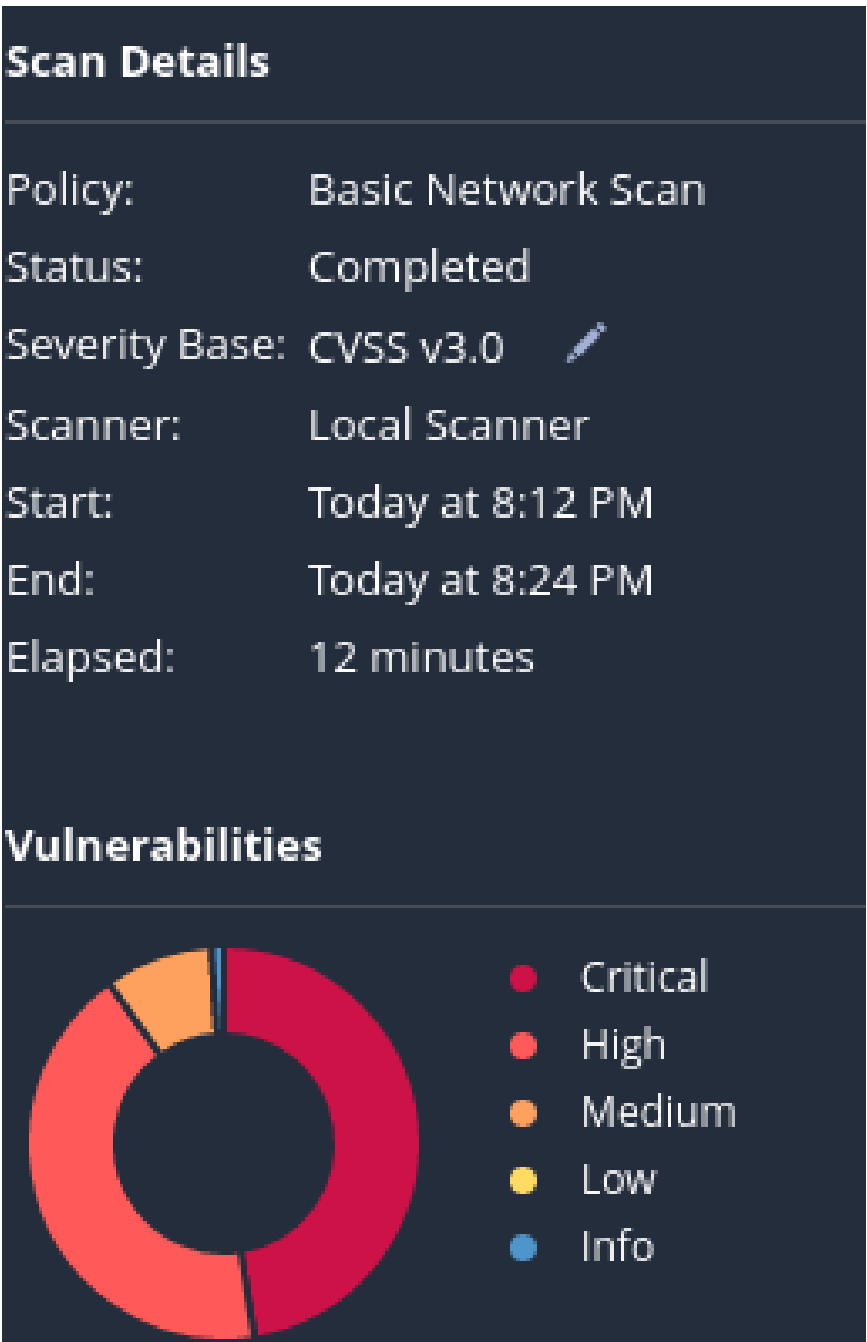
Remediations1

History5

Search Vulnerabilities

190 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	9.5	0.9691	Firefox < 18.0 Multiple Vulnerabilities
<input type="checkbox"/>	CRITICAL	10.0 *	9.5	0.9186	Firefox < 23.0 Multiple Vulnerabilities
<input type="checkbox"/>	CRITICAL	10.0 *	9.5	0.2222	Firefox < 22.0 Multiple Vulnerabilities
<input type="checkbox"/>	CRITICAL	10.0 *	8.9	0.7149	Firefox < 16.0 Multiple Vulnerabilities
<input type="checkbox"/>	CRITICAL	10.0	8.9	0.1727	Mozilla Firefox < 65.0
<input type="checkbox"/>	CRITICAL	10.0	8.1	0.0181	Mozilla Firefox < 67.0.4
<input type="checkbox"/>	CRITICAL	10.0 *	7.3	0.0971	Firefox < 38.0 Multiple Vulnerabilities



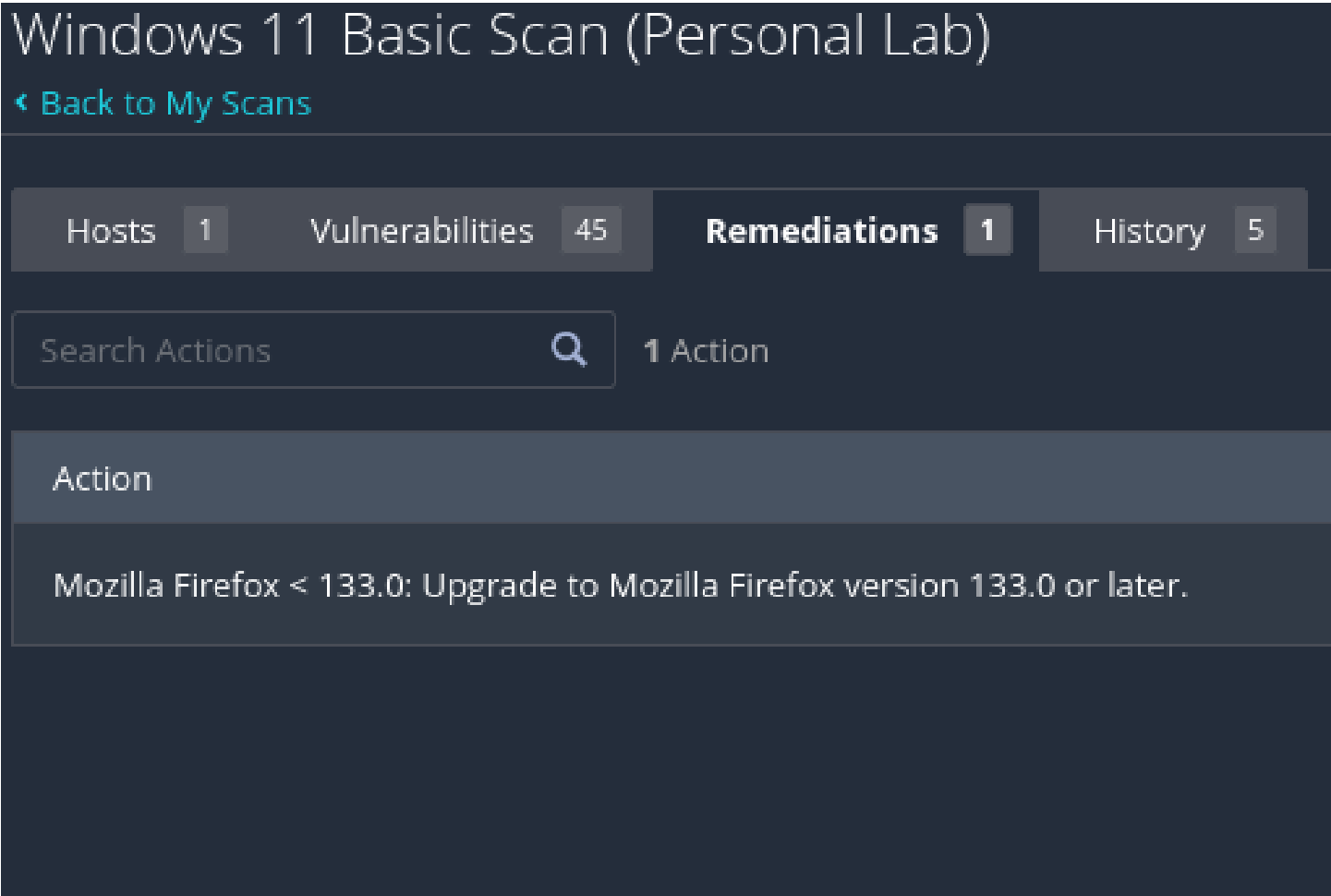
We found a lot of vulnerabilities related to Firefox!

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




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



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!

Windows Update




You're up to date


Last checked: Today, 9:06 PM

Check for updates









More options



Get the latest updates as soon as they're available
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. [Learn more](#)

On 

And this is the new scan!

Filter	Search Vulnerabilities	42 Vulnerabilities			
<input type="checkbox"/> Sev	CVSS	VPR	EPSS	Name	
<input type="checkbox"/> HIGH	8.8	8.9	0.6487	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	
<input type="checkbox"/> INFO	 Microsoft Windows (Multiple Issues)	
<input type="checkbox"/> INFO	 SMB (Multiple Issues)	
<input type="checkbox"/> INFO	 Microsoft Windows (Multiple Issues)	
<input type="checkbox"/> INFO	 Windows (Multiple Issues)	
<input type="checkbox"/> INFO	 Google Chrome (Multiple Issues)	
<input type="checkbox"/> INFO	 Microsoft Edge (Multiple Issues)	
<input type="checkbox"/> INFO	 Microsoft Internet Explorer (Multiple Issues)	
<input type="checkbox"/> INFO	 SMB (Multiple Issues)	
<input type="checkbox"/> INFO				Netstat Portscanner (WMI)	

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