2/c Ishimwe Vivine

Computer Networks and Security

23 September 2020

Collaboration: 2/c Tann

WINDOWS 10 OS HARDENING

Executive Summary

Security control assessment is essential in ensuring the security of our operating systems. There are many places in Windows where risk is greater than features, and hardening OS goes through them one by one. By using the STIG guide and SCAP, we did the evaluation and implementation of different technical controls on the windows10 Operating system. Win10 system has many controls, so we choose some which provides more security than the others. After hardening our system, we tested to see if the changes we made were implemented by comparing SCC results before the evaluation of controls and after remediation.

Introduction

In today's environment hackers attack by exploiting security problems and vulnerabilities of one's computer. This results in unauthorized access of personal data for theft purpose, and defamation, and install of ransomware. The solution to prevent these attacks is to reduce the attack surface so that we expose fewer opportunities for exploitation. We do this by hardening our OS. In other words, configuring our operating system so that it is only able to do what you normally do, and nothing else. Hardening is performed using STIG or SCAP tools in addition to windows and Microsoft tools. This documentation is intended to show how we used the STIG guide and SCAP to harden Windows 10 OS. It will give explanations of the methods we used to evaluate the technical controls and a full description of the extent to which these controls were implemented and produced the desired outcome for meeting the security requirements for the operating systems.

Background of practitioners

Vivine Ishimwe and Chanbopich Tann, 2/c cadets at U.S Coast Guard Academy. Both Ishimwe and Tann have used tools like STIG viewer before to configure a secure system. They are working on developing their knowledge about systems security.

Method – What standards and tools are being used and why

We used different tools to harden Windows 10 operating system. Those tools include STIG viewer, windows tools, Microsoft tools, and SCC. We used the STIG viewer to review the controls that we were going to implement, and it also provided us with the information on how to implement the fixes. STIG like windows 10 have many technical controls. We did not apply them all, however, we selected 38 controls and implement them. The reason we specifically chose them is that for the system to have advanced security, it needs to be configured using firewall GUI and have a strong password. A firewall provides a line of defense against attack. Thus, we choose controls that will enable firewalls to be effective and properly configured. Then, we evaluated the selected controls starting with CAT1 and CAT2 and then moved to CAT3. We then remediated controls by using Windows and Microsoft tools. however, there were some we were not able to fully remediate. Besides, we used SCC results and implement some other controls that were not detected by STIG. SCC results provided us the information about which controls we have to evaluate and remediate so that window firewalls can be properly configured. As we were hardening our system, we keep track of what we were doing and how we did it by saving screenshots of what we were able to implement, and making comments in the STIG checklist of what we found about the controls and the method we used to implement the fixes.

Assumptions

By the end of the evaluation and remediation of controls we will have an OS image for the security team.

Summary of actions taken including identifications of controls assessed

As we mentioned above, we evaluated different controls on each system, and they all have different functionality. Some weaknesses were discovered by windows STIG while others were discovered by SCAP. Since windows have many controls, we selected the important ones according to their level of functionality, and then evaluated them. Most of the time, we were able to make the necessary changes. However, they were some controls that we were not able to fully remediate.

Although, we did plan of Action and Milestone of how we are planning to fix that. On the other hand, for the weaknesses that were discovered by SCAP, we were able to fully remediate them and our results changed from 25% which we had in the beginning to 100%. We did this by checking every single control among selected, and then we had to check if it was a concern or not (a finding). If it was a finding, we had to follow the fix test, implement all the changes necessary, make comments and then check it to “not a finding”. If not a finding, we did not do anything about it. The controls which we were not able to implement, we left them open. Below is the table that shows some of the actions taken.

N	Status	Controls	Findings and Fixes
CAT1			
1	NF	V-63325	The registry path does not exist. We followed the fix text and then disable "Always Install with elevated privileges".
2	NF	V-63335	We followed the registry path and we did not find Window Remote Management. We followed the fix text, and then we finally disabled Allow Basic Authentication.
3	NF	V-63347	The registry path does not exist. We fixed by setting "Allow Basic authentication" to "Disabled".
4	NF	V-63349	My Microsoft Windows Version is currently 2004. It is already the greatest version for now. We do not need to fix.
5	NF	V-63353	We found only two volumes with NTFS among the three volumes on Disk Management. However, the volume with no NTFS was (Disk 0 partition 1) EFI System Partition. We did not fix anything.
6	NF	V-63361	We did not have prohibited accounts as members of the local administrators group. We did not fix anything.
7	NF	V-63377	We saw that Internet Information Services and Internet Information Services Hostable Web Core were not selected. We did not fix anything.
8	NF	V-63429	We found that the value for "Store password using reversible encryption" is set to "Disabled", this is not a finding. We did not fix anything.
9	NF	V-63651	The registry path existed, but there is no Value Name: fAllowToGetHelp. We fixed it by disabling "Configure Solicited Remote Assistance"
10	NF	V-63667	The registry path did not exist. We fixed it by enabling "Disallow Autoplay for non-volume devices".
11	NF	V-63671	The registry path existed, but there is no Value Name: NoAutorun. We fixed it by setting "Set the default behavior for AutoRun" to "Enabled: Do not execute any autorun commands".
12	NF	V-63673	The registry path existed, but there is no Value Name: No Autorun. We fixed it by setting "Turn off AutoPlay" to "Enabled: All Drives".

13	NF	V-63739	We found that “Network access: Allow anonymous SID/Name translation" is set to "Disabled", this is not a finding. We did not fix anything.
14	NF	V-63745	The registry path existed, and everything is correct. We did not fix anything.
15	NF	V-63749	The registry path exists. We do not fix anything.
16	O	V-63351	There is no anti-virus program installed on the system. We did not fix anything because we are not allowed to install anything like anti-virus protection which is not authorized by the cadet admin.
CAT 2			
17	NF	V-63321	The registry path does not exist. We fixed it by disabling "Allow user control over installs".
18	NF	V-63333	The registry path existed but there is no the value name: DisableAutomaticRestartSignOn. We fixed by disabling "Sign-in last interactive user automatically after a system-initiated restart".
19	NF	V-63339	The registry path does not exist. We followed the fixt text and diabled "Allow unencrypted traffic".
20	NF	V-63341	The registry path does not exist. We followed the fix text and then enabled "Disallow Digest authentication".
21	NF	V-63355	We found that there is no any operating system other than Windows 10. We did not fix anything.
22	NF	V-63357	We found an extra share, print$, which is my own printer. It is a wireless printer which is already a pin owned by me. We kept the non-system-created share because it is necessary.
23	NF	V-63369	The registry path did not exist. We fixed by disabling "Allow unencrypted traffic".
24	NF	V-63371	We found that there were "Password never expires" of some active accounts which were selected. We unchecked "Password never expires" on all active accounts and clicked Apply.
25	O	V-63319	After we did the checking, we found that Edition is not "Window 10 Enterprise", but System type is "64-bit operating system..." We are not allowed to update our window to Windows 10 Enterprise without permission from Cadet Admin.
CAT 3			
26	NF	V-63653	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: pass "Domain member: Disable machine account password changes" is already diabled.
27	NF	V-63659	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: pass We fixed it by enabling "Allow Microsoft accounts to be optional".

28	NF	V-63661	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: pass
29	NF	V-63663	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: pass We fixed it by enabling "Turn off Inventory Collector".
30	NF	V-63681	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: fail We fixed it by adding "DoD Notice and Consent Banner" as a site-defined equivalent.
31	NF	V-63687	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: pass
32	NF	V-63691	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: pass
33	NF	V-63815	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: pass
34	O	V-63563	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: fail We could not fix it because there is no MSS (Legacy) in Administrative Templates.
35	O	V-63567	Tool: cpe:/a:spawar:scc:5.2.1 Time: 2020-09-23T19:59:14 Result: fail We could not fix it because there is no MSS (Legacy) in Administrative Templates.

Discussion on highest impact controls encountered

As stated above, we evaluated and implemented different controls on windows 10. All controls play an important role in ensuring the system's security, although some have the highest impact than the others. Attackers use every opportunity to attack user's systems. For example, users with easy passwords make it easy for the attacks to effortlessly guess their combinations which in result leads to unauthorized access to the information. We selected those controls that establish good passwords lives, and those that make firewalls effective. Below is the SCC scan results before implementing controls.

The score os the system is 25%

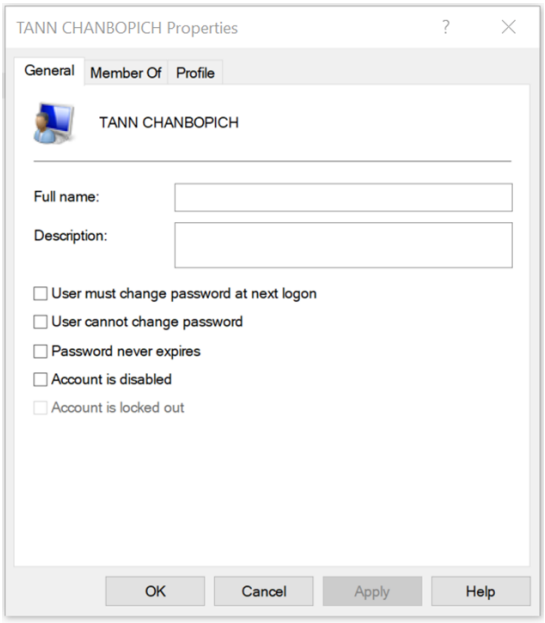
Score

25%		
	Adjusted Score:	25%
	Original Score:	25%
	Compliance Status:	**RED**

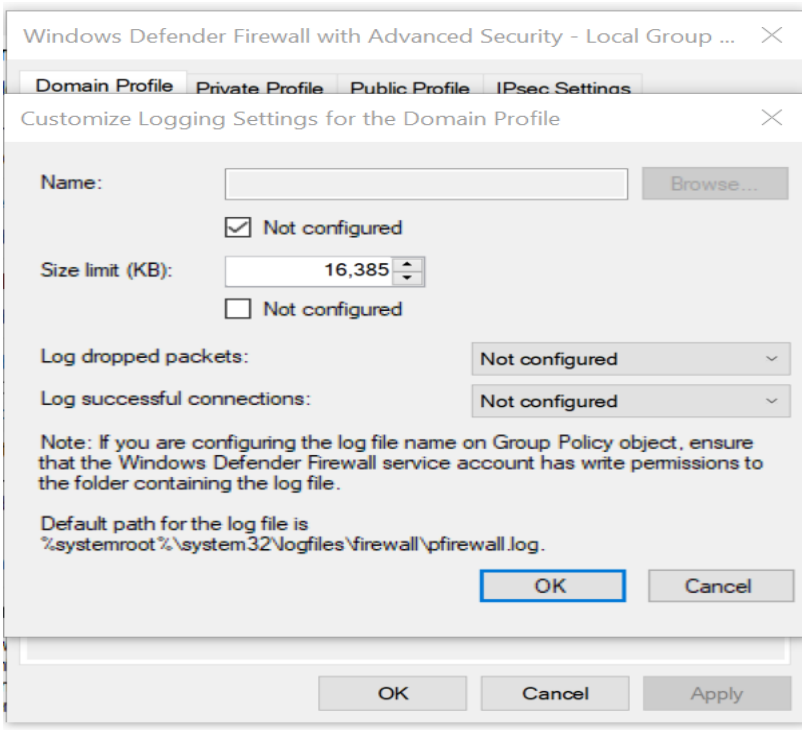
Pass:	5	Not Applicable:	0	BLUE:	Score equals 100
Fail:	15	Not Checked:	0	GREEN:	Score is greater than or equal to 90
Error:	0	Not Selected:	0	YELLOW:	Score is greater than or equal to 80
Unknown:	0	Informational:	0	RED:	Score is greater than or equal to 0
Fixed:	0	Total:	20		

These are the highest impact controls

V-63371: Password is main factor for security maintenance. But if our passwords are short, weak, easy to remember or expired, we may face a greater probability of being discovered or cracked. So, accounts must be configured to require password expiration. While we are having many active accounts and busy works, we usually do not remember or care of password update. It is a dangerous carelessness. To avoid it, we can set regular alert for you to update your password for your active accounts. We can run "Computer Management".
Navigate to System Tools >> Local Users and Groups >> Users, then double click each active account. And unselect "Password never expires".

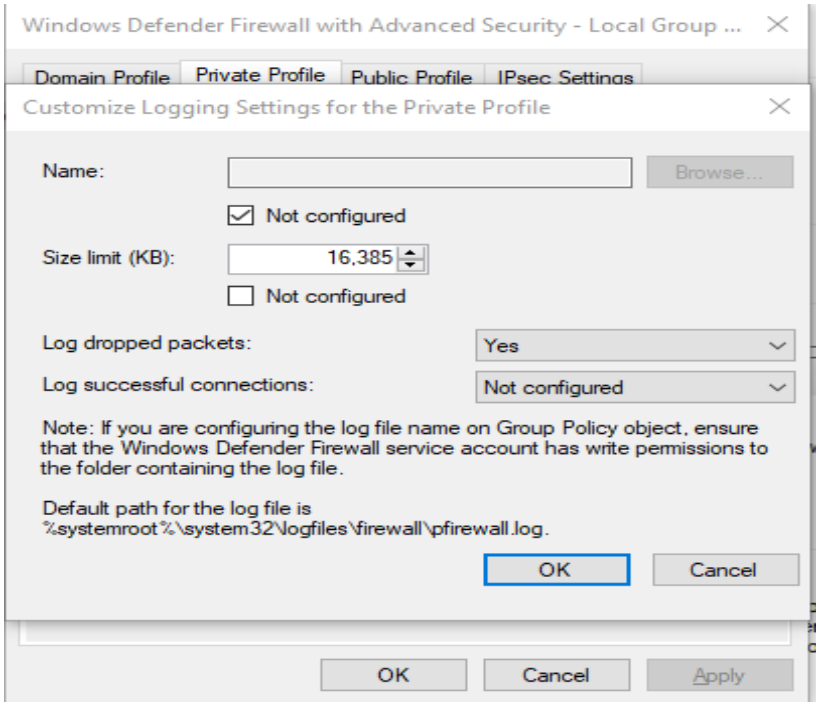


V-17425: The Windows Firewall with Advanced Security log size must be configured for domain connections. To be effective in providing a line of defense against attack, firewall must be enabled and properly configured. Its file size for a domain connection will be set to ensure enough capacity is allocated for audit data. The size limit (KB) should be 16,384 or greater.

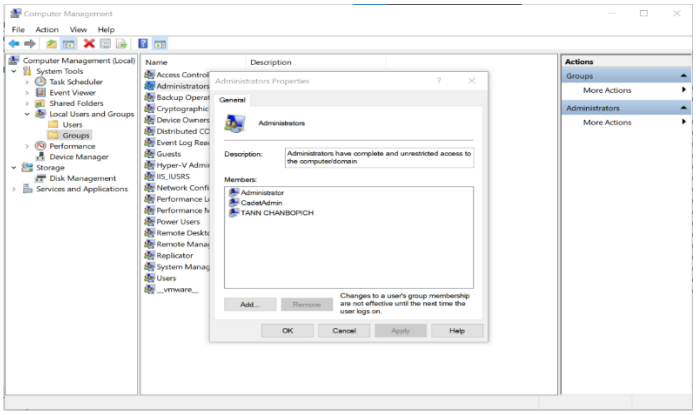


V-63349: This control is that Windows 10 systems must be maintained at a supported servicing level. Why it is important is because computer systems at unsupported servicing levels do not receive more security updates so that it can be protected. New versions of window update are recommended to be made very often. If we figure out our Microsoft Window Version out of date, we can click Window button > Setting > Window Update > Check for updates. Here is the current Window 10 systems Version 2004.

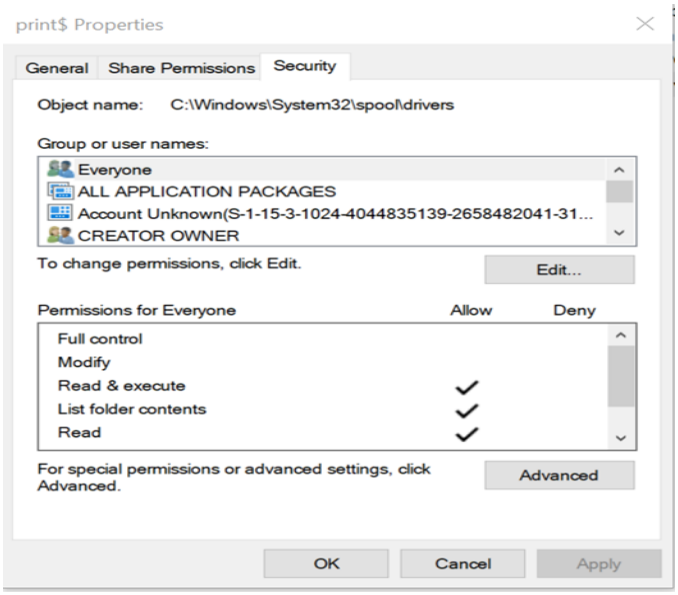
V-17436: The Windows Firewall with Advanced Security must log dropped packets when connected to a private network. Why log dropped packets need to be Yes is to main an audit trail of potential issues. The logs can provide valuable information like source and destination IP addresses, port numbers, and protocols. These information are important for us as cyber security guards.



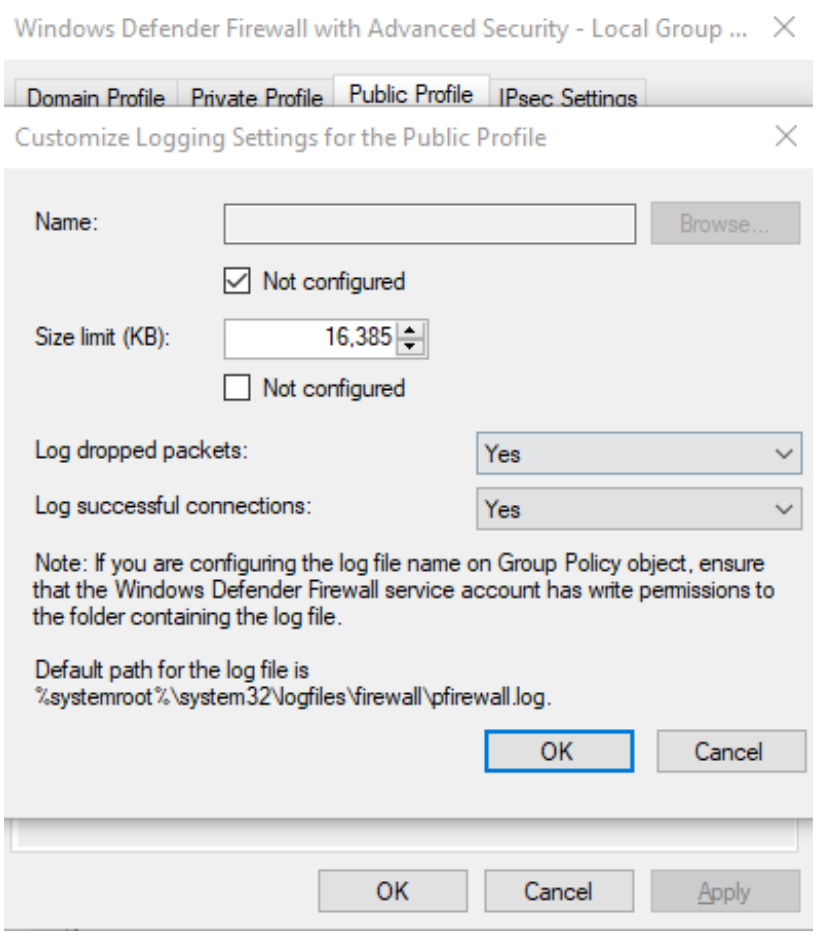
V-63361: This control is to ensure that only accounts responsible for the administration of a system must have Administrator rights on the system. Accounts with administrator rights can operate more than the standard accounts. Even though standard user can edit Ms. Office files, edit images, search the web and many more, they still face restrictions not to be able to create, edit, view, or delete system files. This right limitation also takes part in security maintenance, management, data access and problem solving.



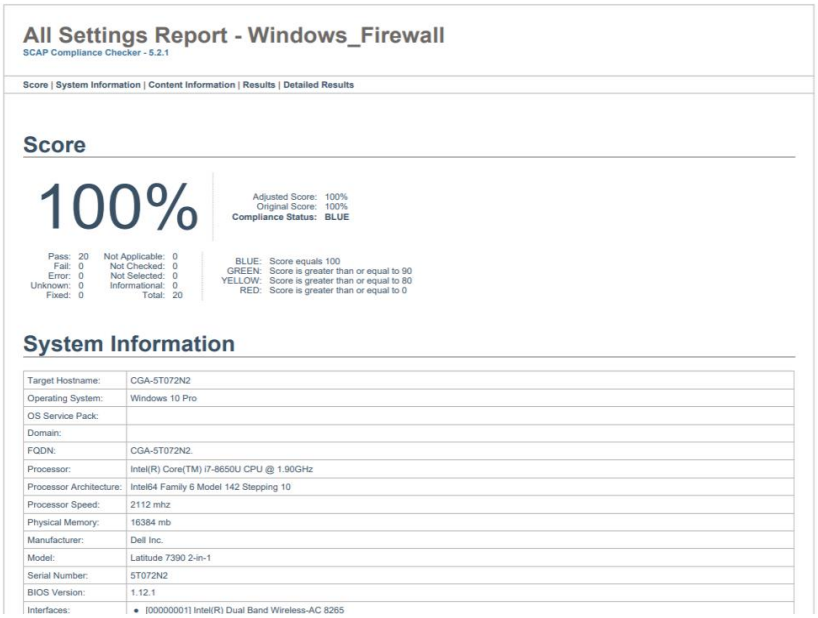
V-63357: Non system-created file shares on a system must limit access to groups that require it. We should ensure that there are non-system-created file shares as less as possible in our systems. If we have few of them, we should limit their access to specific groups of users in order to protect security and unauthorized shares. Verify the necessity of any non-system-created file shares and delete them if they are unnecessary.



V-17447- The Windows Firewall with Advanced Security must log successful connections when connected to a public network. This connection will be enabled to maintain an audit trail if issues are discovered.



After remediating controls, we ran back the SCC scan and below are the results. Changed from 25% to 100%



All Settings Report - Windows_Firewall

SCAP Compliance Checker - 5.2.1

Score | System Information | Content Information | Results | Detailed Results

Score

100%

Adjusted Score: 100%
Original Score: 100%
Compliance Status: BLUE

Pass: 20 Not Applicable: 0
Fail: 0 Not Checked: 0
Error: 0 Not Selected: 0
Unknown: 0 Informational: 0
Fixed: 0 Total: 20

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

System Information

Target Hostname:	CGA-5T072N2
Operating System:	Windows 10 Pro
OS Service Pack:	
Domain:	
FQDN:	CGA-5T072N2.
Processor:	Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
Processor Architecture:	Intel64 Family 6 Model 142 Stepping 10
Processor Speed:	2112 mhz
Physical Memory:	16384 mb
Manufacturer:	Dell Inc.
Model:	Latitude 7390 2-in-1
Serial Number:	5T072N2
BIOS Version:	1.12.1
Interfaces:	• [00000001] Intel(R) Dual Band Wireless-AC 8265

Conclusion

In conclusion, this evaluation helped to see which parts of security measures we were quite weak on, it showed us parts of the systems that can be targeted by the attackers and as a result, the technical controls were upgraded and made them more efficient and effective. Throughout the entire work, I practiced different steps necessary for hardening the OS, I learned more about OS hardened tools, and I believe I can do this perfectly in the future.