jamk

SCAP – compliance checker 5.9

Ryhmä 3

Anthony Bäckström

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Harjoitustyö

Huhtikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Tässä tehtävässä testasimme SCAPia. Alkuun yritimme ajaa sitä labraympäristön työasemalla, mutta onnistuneiden kovennusten jälkeen oli helpompi hakea se vain yhden ryhmäläisen koneelle. Käytössä oli vanha todellisuuspakoa varten hankittu sotaratsu, joka opintojen aikana on saanut uuden viran työkoneena. Eli minkään näköisiä kovennuksia laitteelta ei löydy.

SCAPin käyttäminen oli helppoa. Ensimmäiseltä sivulta naksuteltiin kohdat, jotka sen haluttiin tarkistavan. Tässä tapauksessa Local scan -> select content (jolle oli oma ikkunansa.) -> Start scan. Ohjelma suoritti skannauksen annetuilla parametreillä ja sitä pääsi lukemaan pääsivun View result napista.

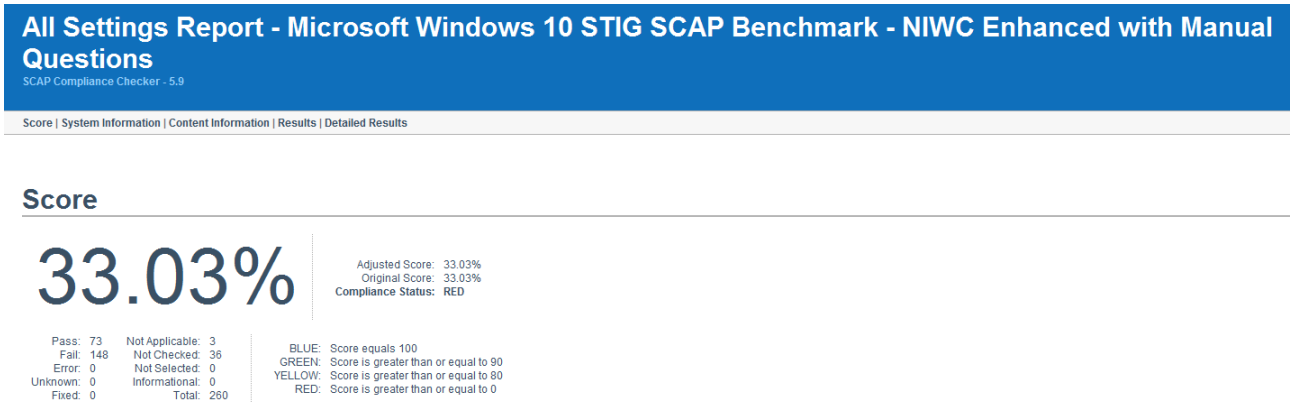
2 Skannaus ja tulokset

Tulosten pääsivulta skannauksia pystyi valitsemaan Sessions- listasta. Alla näkyvässä kuvassa on tulokset tätä tehtävää varten tehdystä tarkistuksesta. (ks. Kuvio 1.)

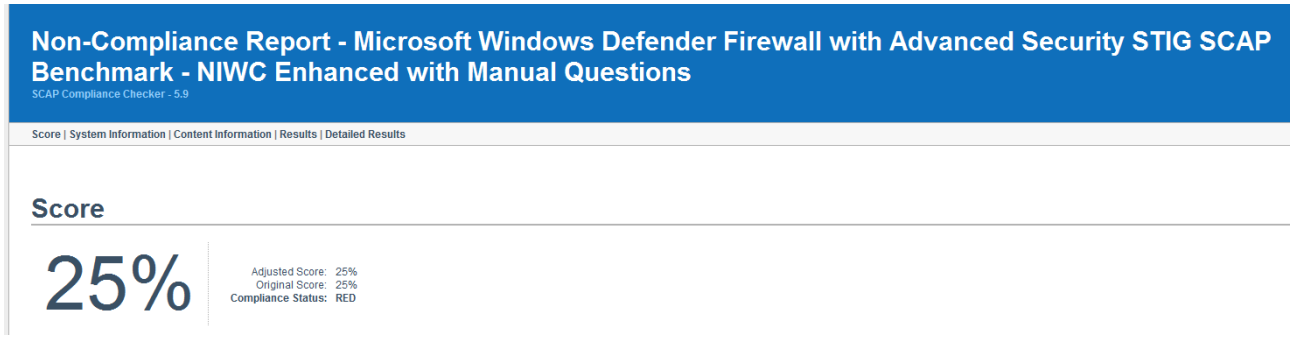
Host Name	Content	Score	Errors	Warnings
DESKTOP-S57456R	Windows_Firewall...Advanced_Security	25	10	1
DESKTOP-S57456R	MS_Windows_10_STIG	33.03	67	10
DESKTOP-S57456R	MS_Office_365_ProPlus_STIG	10.87	10	1
DESKTOP-S57456R	MS_Edge_STIG	0	10	1
DESKTOP-S57456R	MS_Dot_Net_Framework	75	10	1
DESKTOP-S57456R	MS_Defender_Antivirus	43.9	9	0
DESKTOP-S57456R	MOZ_Firefox_Windows	0	10	1
DESKTOP-S57456R	Microsoft_OneDrive_STIG	0	10	1
DESKTOP-S57456R	IE_11_STIG	0.73	9	0
DESKTOP-S57456R	Google_Chrome_Current_Windows	0	11	1

Kuvio 1 Skannaustulosten pääsivu

Viereisessä ikkunassa oli mahdollista valita erilaisia raportteja mm. HTML ja XML -muodoissa. Lisäksi raportti oli mahdollista saada DISA (Defence Information Systems Agency) -checklistinä. Tutustuimme perusraporttiin, joka oli mahdollista saada All Setting tai Non-Compliance raporttina. (ks. Kuvio 2 ja Kuvio 3)



Kuvio 2 All Settings Report



Kuvio 3 Non-Compliance Report

All Settings Report näyttää kaikki ajetut skannaukset ja niiden tulokset (ks. Kuvio 4). Siinä missä Non- Compliance näyttää vain tulokset, jotka eivät ole läpäisseet testejä. Jokainen testin kohta on myös luettavissa yksityiskohtaisena kuvauksena (ks. Kuvio 5) tehdyistä testeistä, syistä miksi testi epäonnistui sekä tarvittavista korjausehdotuksista.

Results: High Severity (CAT I)

Automated Checks

- V-220706 - Windows 10 systems must be maintained at a supported servicing level. - Pass
- V-220708 - Local volumes must be formatted using NTFS. - Pass
- V-220718 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation. - Pass
- V-220726 - Data Execution Prevention (DEP) must be configured to at least OptOut. - Fail
- V-220727 - Structured Exception Handling Overwrite Protection (SEHOP) must be enabled. - Pass
- V-220747 - Reversible password encryption must be disabled. - Pass
- V-220812 - Credential Guard must be running on Windows 10 domain-joined systems. - Not Applicable
- V-220823 - Solicited Remote Assistance must not be allowed. - Fail
- V-220827 - Autoplay must be turned off for non-volume devices. - Fail
- V-220828 - The default autorun behavior must be configured to prevent autorun commands. - Fail
- V-220829 - Autoplay must be disabled for all drives. - Fail
- V-220857 - The Windows Installer Always install with elevated privileges must be disabled. - Fail
- V-220862 - The Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-220865 - The Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-220929 - Anonymous enumeration of SAM accounts must not be allowed. - Pass
- V-220930 - Anonymous enumeration of shares must be restricted. - Fail
- V-220932 - Anonymous access to Named Pipes and Shares must be restricted. - Pass
- V-220937 - The system must be configured to prevent the storage of the LAN Manager hash of passwords. - Pass
- V-220938 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM. - Fail
- V-220958 - The Act as part of the operating system user right must not be assigned to any groups or accounts. - Pass
- V-220963 - The Create a token object user right must not be assigned to any groups or accounts. - Pass
- V-220967 - The Debug programs user right must only be assigned to the Administrators group. - Fail

Manual Checks

- V-220707 - The Windows 10 system must use an anti-virus program. - Not Checked
- V-220712 - Only accounts responsible for the administration of a system must have Administrator rights on the system. - Not Checked
- V-220737 - Administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email. - Not Checked
- V-220928 - Anonymous SID/Name translation must not be allowed. - Not Checked

Kuvio 4 All Settings Results

V-241992 - Windows Defender Firewall with Advanced Security must block unsolicited inbound connections when connected to a domain.

Rule ID:	xccdf_mil.disa.stig_rule_SV-241992r922934_rule
Test Type:	Automated
Result:	Fail
Version:	WNFWA-000004
Identities:	V-17418 SV-54859 CCI-000382 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (iii); NIST SP 800-53 Rev 4: CM-7 b; NIST SP 800-53 Rev 5: CM-7 b)
Description:	A firewall provides a line of defense against attack. To be effective, it must be enabled and properly configured. Unsolicited inbound connections may be malicious attempts to gain access to a system. Unsolicited inbound connections, for which there is no rule allowing the connection, will be blocked in the domain.
Fix Text:	The preferred method of configuring the firewall settings is with a policy, particularly in a domain environment. Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Windows Defender Firewall with Advanced Security >> Windows Defender Firewall with Advanced Security >> Windows Defender Firewall Properties (this link will be in the right pane) >> Domain Profile tab >> State, "Inbound connections" to "Block (default)". In addition to using policies, systems may also be configured using the firewall GUI or Netsh commands. These methods may be more appropriate for standalone systems. The configuration settings in the GUI are the same as those specified in the policy above. Microsoft Defender Firewall Properties will be a link in the center pane after opening Microsoft Defender Firewall with Advanced Security. The following Netsh commands may also be used to configure this setting: "Netsh advfirewall set domainprofile firewallpolicy blockinbound,allowoutbound". or "Netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound". Both inbound and outbound parameters must be specified to execute this command.
Severity:	high
Weight:	10.0
Reference:	Title: DPMS Target Windows Defender Firewall with Advanced Security Publisher: DISA Type: DPMS Target Subject: Windows Defender Firewall with Advanced Security Identifier: 5363
Definitions:	Definition ID: oval:mil.disa.fso.windows:def:4801 Result: false Title: Inbound Connections - Domain Profile Description: Inbound Connections - Domain Profile Class: compliance Tests: • false (All child checks must be true.) ○ false (One or more child checks must be true.) ▪ false (All child checks must be true.) ▪ true (defaultinboundaction non existent) ▪ false (HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile!DefaultInboundAction value equals variable) ▪ false (HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile!DefaultInboundAction value equals variable) ○ true (One or more child checks must be true.) ▪ true (All child checks must be true.) ▪ true (HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile!EnableFirewall non existent) ▪ true (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile!EnableFirewall value equals variable) ▪ false (HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile!EnableFirewall value equals variable)

Kuvio 5 Detailed result

Tältä koneelta SCAP nosti korkeina riskeinä esiin etenkin MS Defenderin ja Firewallin konfiguraatioita, joissa etenkin sisään tulevan liikenteen konfiguraatiot olisi pitänyt asettaa tarkemmin. Myös käyttöjärjestelmälle tehty STIG (Security Technical Implementation Guide) nosti esiin etenkin pääsynhallintaan, etäkäyttöön ja automaattiseen käynnistämiseen liittyviä asetuksia.

Kaikkineen SCAP on ohjelma, joka on helppo asentaa ja se antaa selkeästi luettavassa muodossa testiensä perusteella tehdyt havainnot ja niihin liittyvät korjausehdotukset. Esimerkiksi High Severity kovennusten läpikäyminen ja uudelleenarvioiminen SCAPin parametreja vastaan ei ota paljoa aikaa ja se voisi olla helppo tapa lähteä tekemään muutoksia asetuksiin hallitusti.

Labraympäristöön tehty Workstation kone ei enää peruskäyttäjän oikeuksilla antanut SCAPia asennella. Voisi olla mielenkiintoista katsoa mitä hälytteitä nousee esiin ja mitkä ovat korjaantuneet, kun ympäristöön on tehty Security Compliance Tookittiä käyttäen Windows 11 baseline-kovennukset