jamk.fi

Lab 03. Vulnerability scanFile

Author Adam Pawełek

Teacher: Markku Vajaranta
Date of Laboratory: 26.10.2020
Group: TTKS0700-3001
Jamk number: AA4917

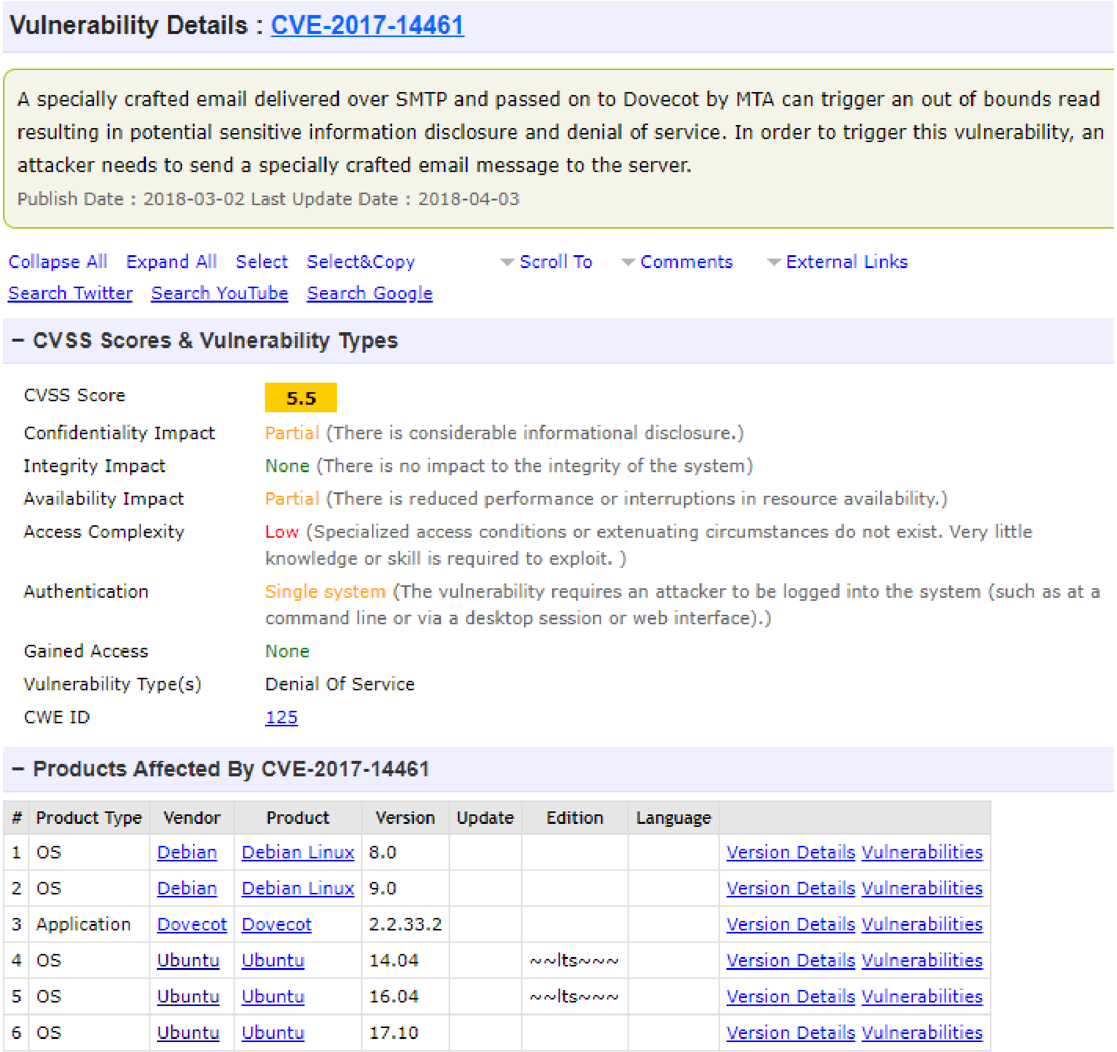
Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 Contents

1 Select one software from your computer

1.1 Use search to find vulnerabilities related to the software/vendor

I searched for vulnerabilities in ubuntu.



Vulnerability Details : CVE-2017-14461

A specially crafted email delivered over SMTP and passed on to Dovecot by MTA can trigger an out of bounds read resulting in potential sensitive information disclosure and denial of service. In order to trigger this vulnerability, an attacker needs to send a specially crafted email message to the server.

Publish Date : 2018-03-02 Last Update Date : 2018-04-03

Collapse All Expand All Select Select&Copy ▾ Scroll To ▾ Comments ▾ External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

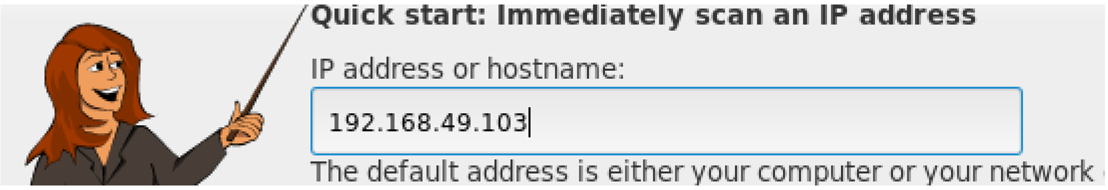
CVSS Score	5.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	125

– Products Affected By CVE-2017-14461

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Debian	Debian Linux	8.0				Version Details Vulnerabilities
2	OS	Debian	Debian Linux	9.0				Version Details Vulnerabilities
3	Application	Dovecot	Dovecot	2.2.33.2				Version Details Vulnerabilities
4	OS	Ubuntu	Ubuntu	14.04		~~lts~~~		Version Details Vulnerabilities
5	OS	Ubuntu	Ubuntu	16.04		~~lts~~~		Version Details Vulnerabilities
6	OS	Ubuntu	Ubuntu	17.10				Version Details Vulnerabilities

2 Run three different scans

2.1 EXTERNAL scan from outside the firewall

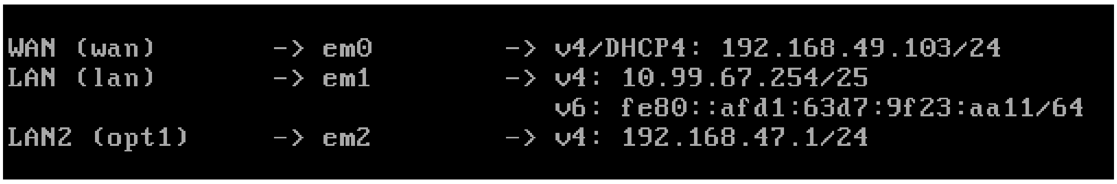


Quick start: Immediately scan an IP address

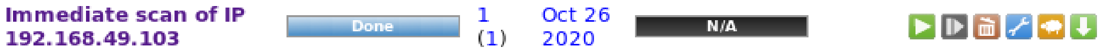
IP address or hostname:

192.168.49.103

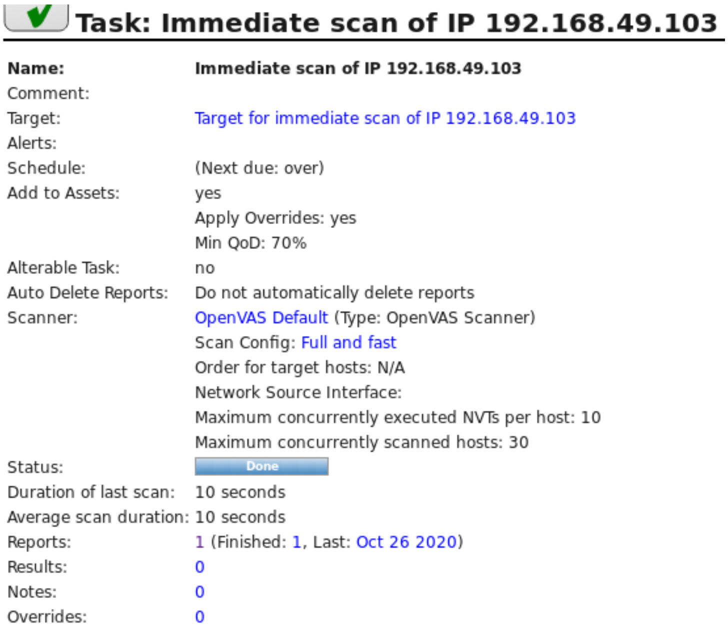
The default address is either your computer or your network



```
WAN (wan)        -> em0        -> v4/DHCP4: 192.168.49.103/24
LAN (lan)        -> em1        -> v4: 10.99.67.254/25
                                  v6: fe80::afd1:63d7:9f23:aa11/64
LAN2 (opt1)      -> em2        -> v4: 192.168.47.1/24
```



Immediate scan of IP 192.168.49.103 Done 1 (1) Oct 26 2020 N/A



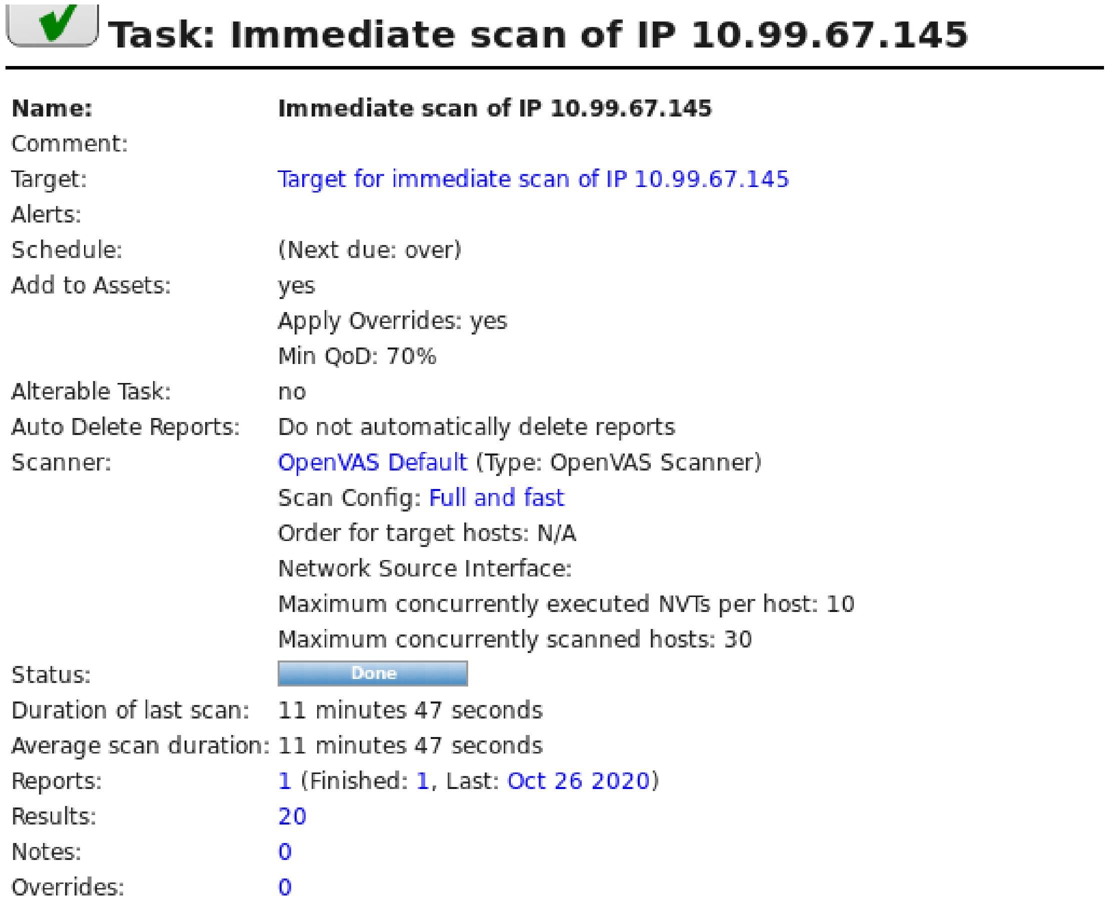
Task: Immediate scan of IP 192.168.49.103

Name:	**Immediate scan of IP 192.168.49.103**
Comment:	
Target:	Target for immediate scan of IP 192.168.49.103
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes Apply Overrides: yes Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner) Scan Config: Full and fast Order for target hosts: N/A Network Source Interface: Maximum concurrently executed NVTs per host: 10 Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	10 seconds
Average scan duration:	10 seconds
Reports:	1 (Finished: 1, Last: Oct 26 2020)
Results:	0
Notes:	0
Overrides:	0

2.2 INTERNAL scan from internal network

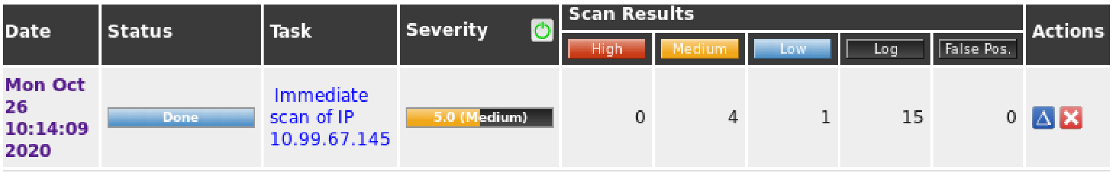
Linux:

For this scan I used default Task wizard with ip of Linux VM.



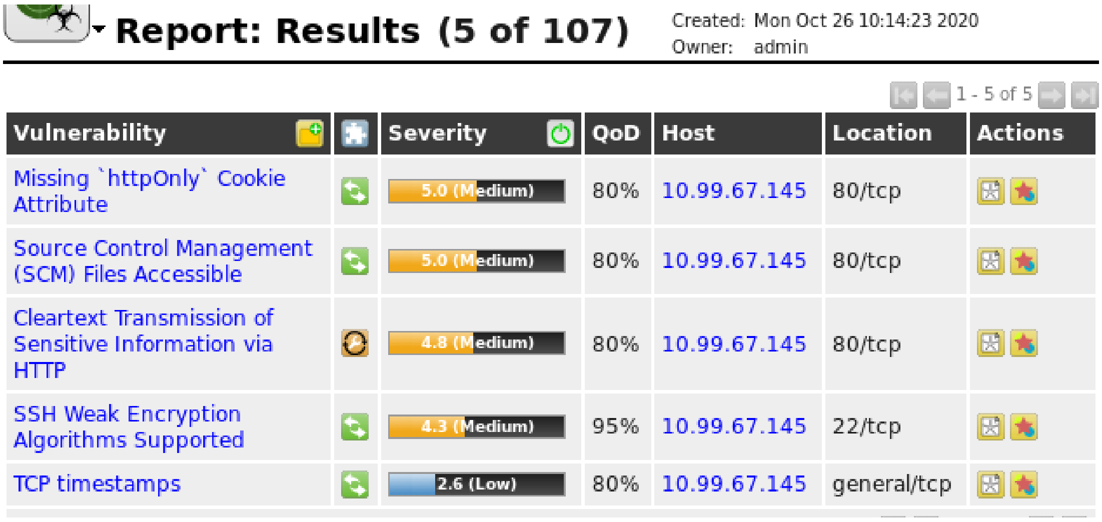
Task: Immediate scan of IP 10.99.67.145

Name:	**Immediate scan of IP 10.99.67.145**
Comment:	
Target:	Target for immediate scan of IP 10.99.67.145
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: Full and fast
	Order for target hosts: N/A
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 10
	Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	11 minutes 47 seconds
Average scan duration:	11 minutes 47 seconds
Reports:	1 (Finished: 1, Last: Oct 26 2020)
Results:	20
Notes:	0
Overrides:	0



Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Mon Oct 26 10:14:09 2020	Done	Immediate scan of IP 10.99.67.145	5.0 (Medium)	0	4	1	15	0	△ ✕

Scan Report:



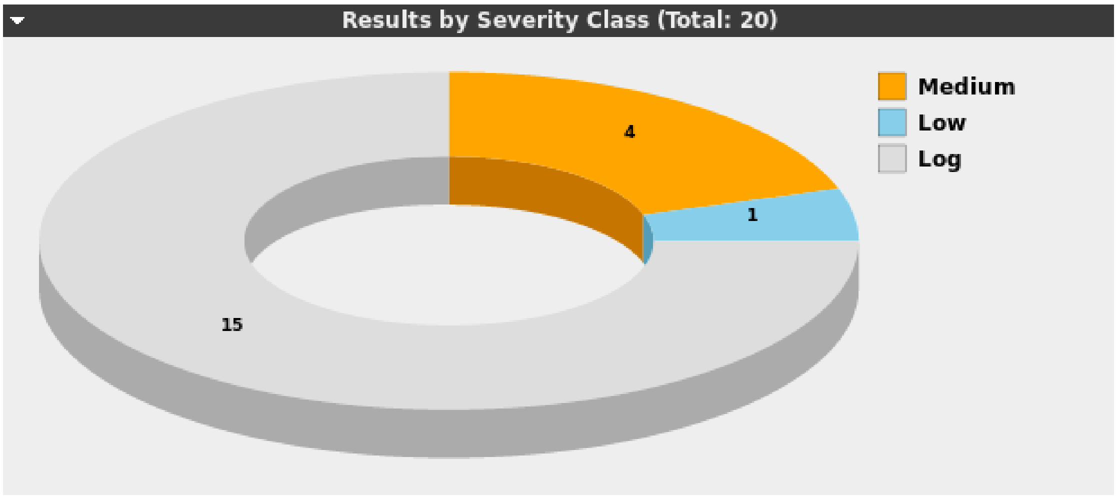
Report: Results (5 of 107)

Created: Mon Oct 26 10:14:23 2020
Owner: admin

1 - 5 of 5

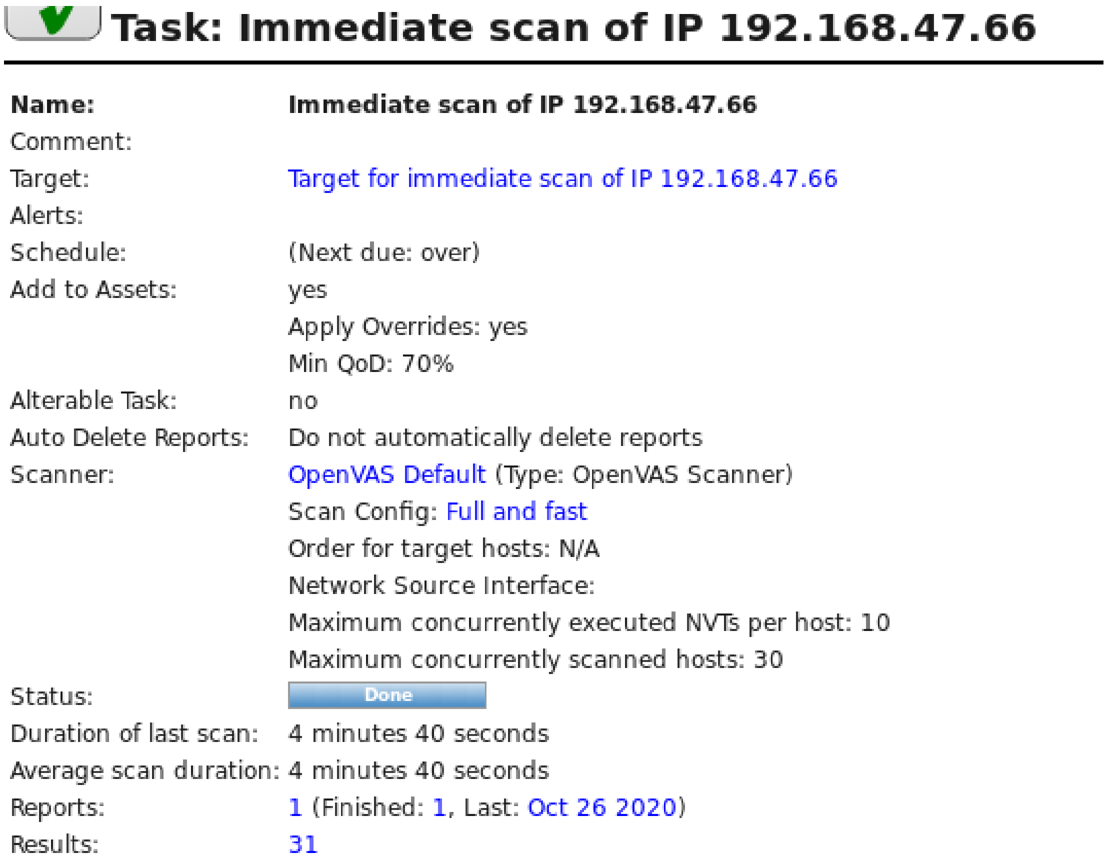
Vulnerability		Severity	QoD	Host	Location	Actions
Missing `httpOnly` Cookie Attribute		5.0 (Medium)	80%	10.99.67.145	80/tcp	
Source Control Management (SCM) Files Accessible		5.0 (Medium)	80%	10.99.67.145	80/tcp	
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80%	10.99.67.145	80/tcp	
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95%	10.99.67.145	22/tcp	
TCP timestamps		2.6 (Low)	80%	10.99.67.145	general/tcp	

Result by Severity Class:



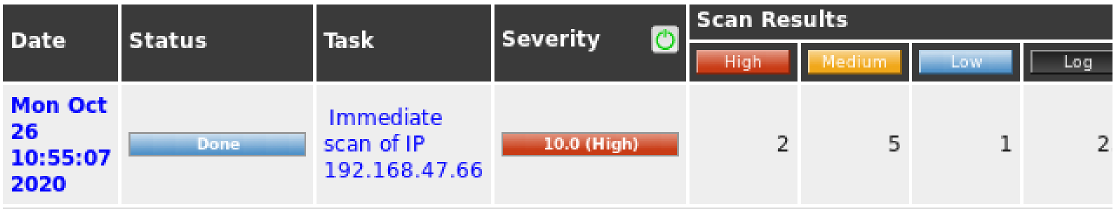
Windows:

For this scan I used default Task wizard with ip of Windows VM.



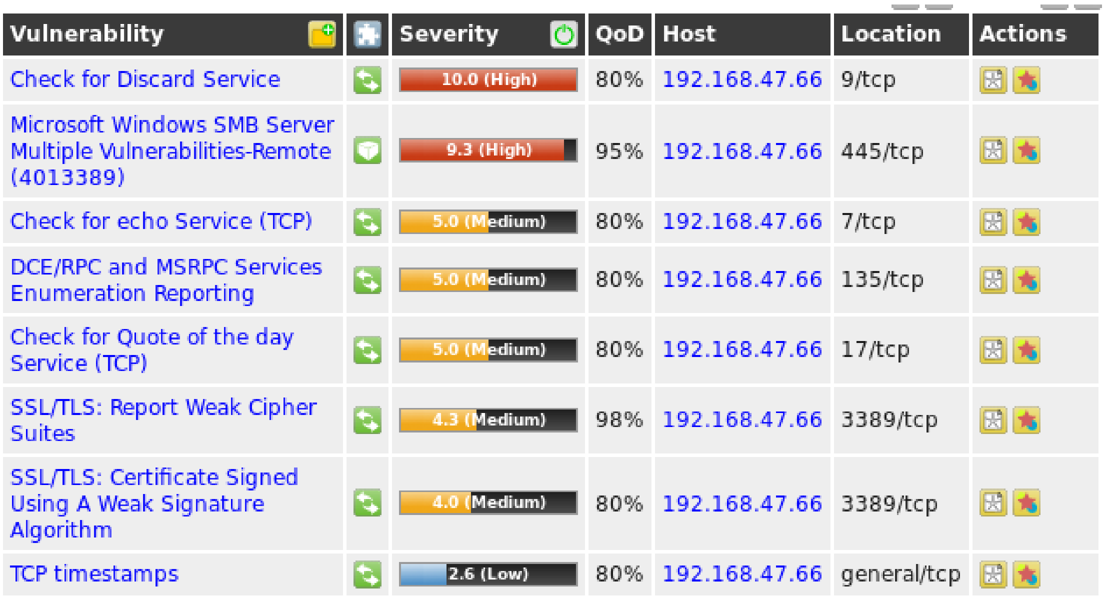
Task: Immediate scan of IP 192.168.47.66

Name:	**Immediate scan of IP 192.168.47.66**
Comment:	
Target:	Target for immediate scan of IP 192.168.47.66
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes Apply Overrides: yes Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner) Scan Config: Full and fast Order for target hosts: N/A Network Source Interface: Maximum concurrently executed NVTs per host: 10 Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	4 minutes 40 seconds
Average scan duration:	4 minutes 40 seconds
Reports:	1 (Finished: 1, Last: Oct 26 2020)
Results:	31



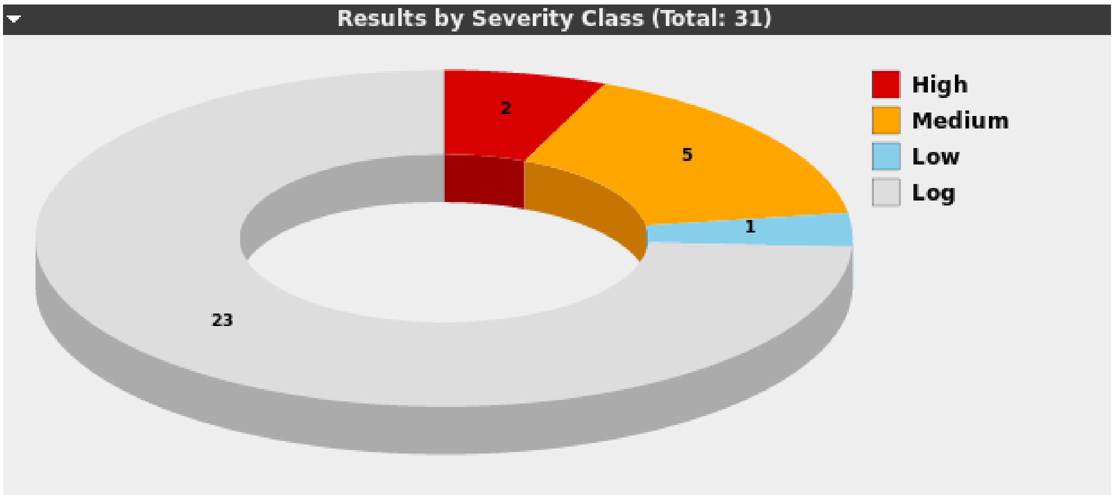
Date	Status	Task	Severity	Scan Results			
				High	Medium	Low	Log
Mon Oct 26 10:55:07 2020	Done	Immediate scan of IP 192.168.47.66	10.0 (High)	2	5	1	2

Scan Report Results (8 of 32):



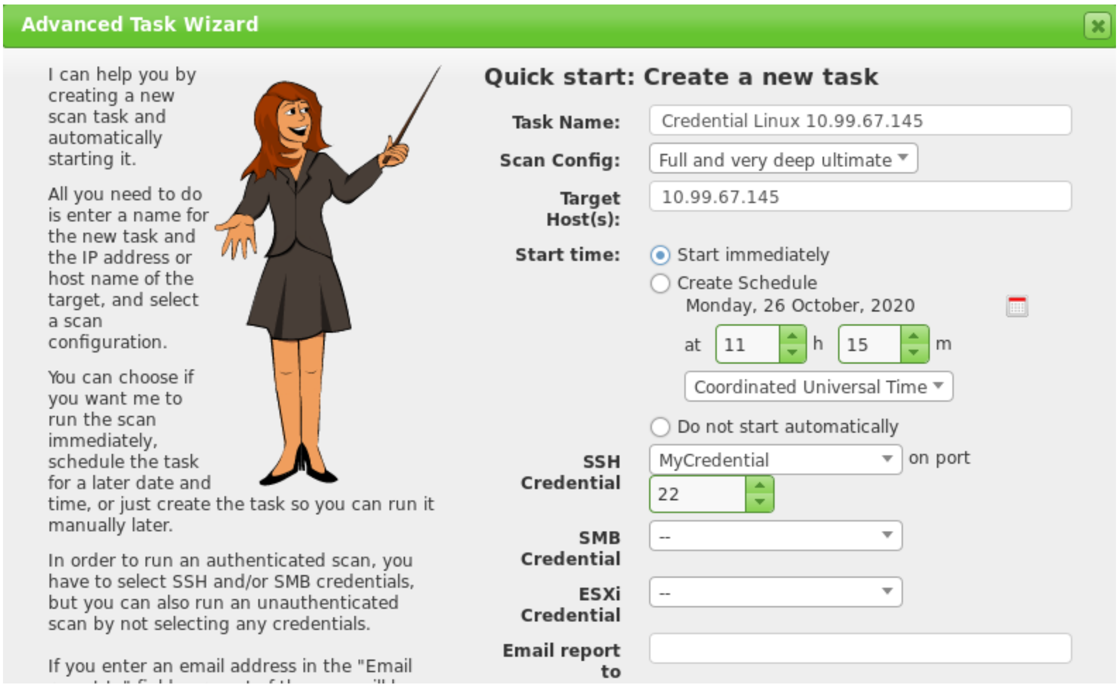
Vulnerability		Severity	QoD	Host	Location	Actions
Check for Discard Service		10.0 (High)	80%	192.168.47.66	9/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	192.168.47.66	445/tcp	
Check for echo Service (TCP)		5.0 (Medium)	80%	192.168.47.66	7/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	192.168.47.66	135/tcp	
Check for Quote of the day Service (TCP)		5.0 (Medium)	80%	192.168.47.66	17/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.47.66	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	192.168.47.66	3389/tcp	
TCP timestamps		2.6 (Low)	80%	192.168.47.66	general/tcp	

Result by Severity Class



2.3 RUN Credential scan

Linux Settings



I can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose if you want me to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

If you enter an email address in the "Email

Quick start: Create a new task

Task Name: Credential Linux 10.99.67.145

Scan Config: Full and very deep ultimate

Target Host(s): 10.99.67.145

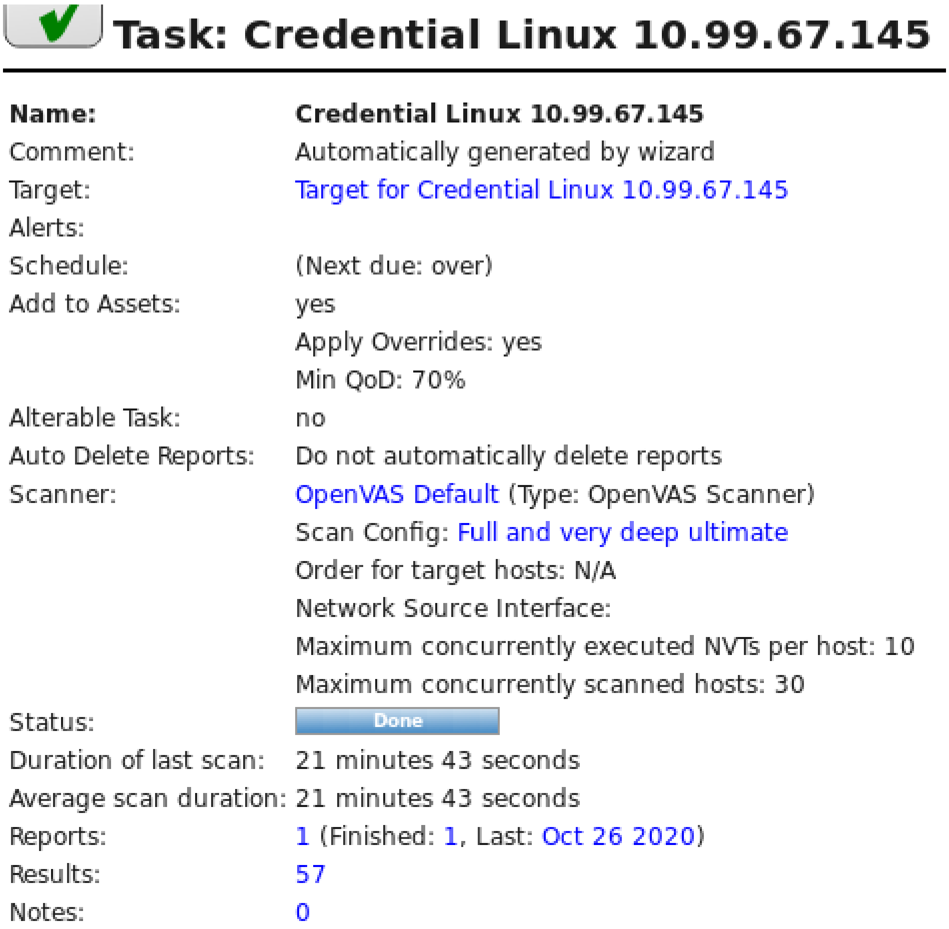
Start time:
● Start immediately
○ Create Schedule
Monday, 26 October, 2020
at 11 h 15 m
Coordinated Universal Time
○ Do not start automatically

SSH Credential MyCredential on port 22

SMB Credential --

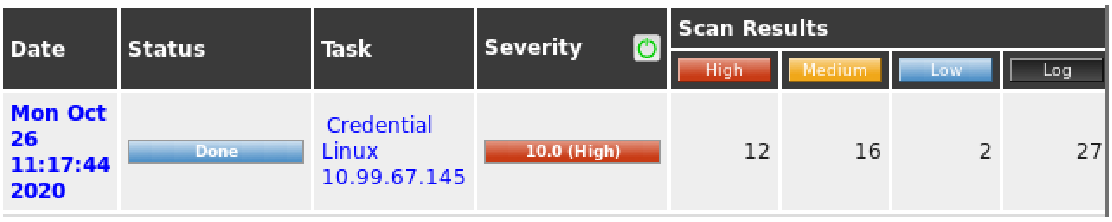
ESXi Credential --

Email report to



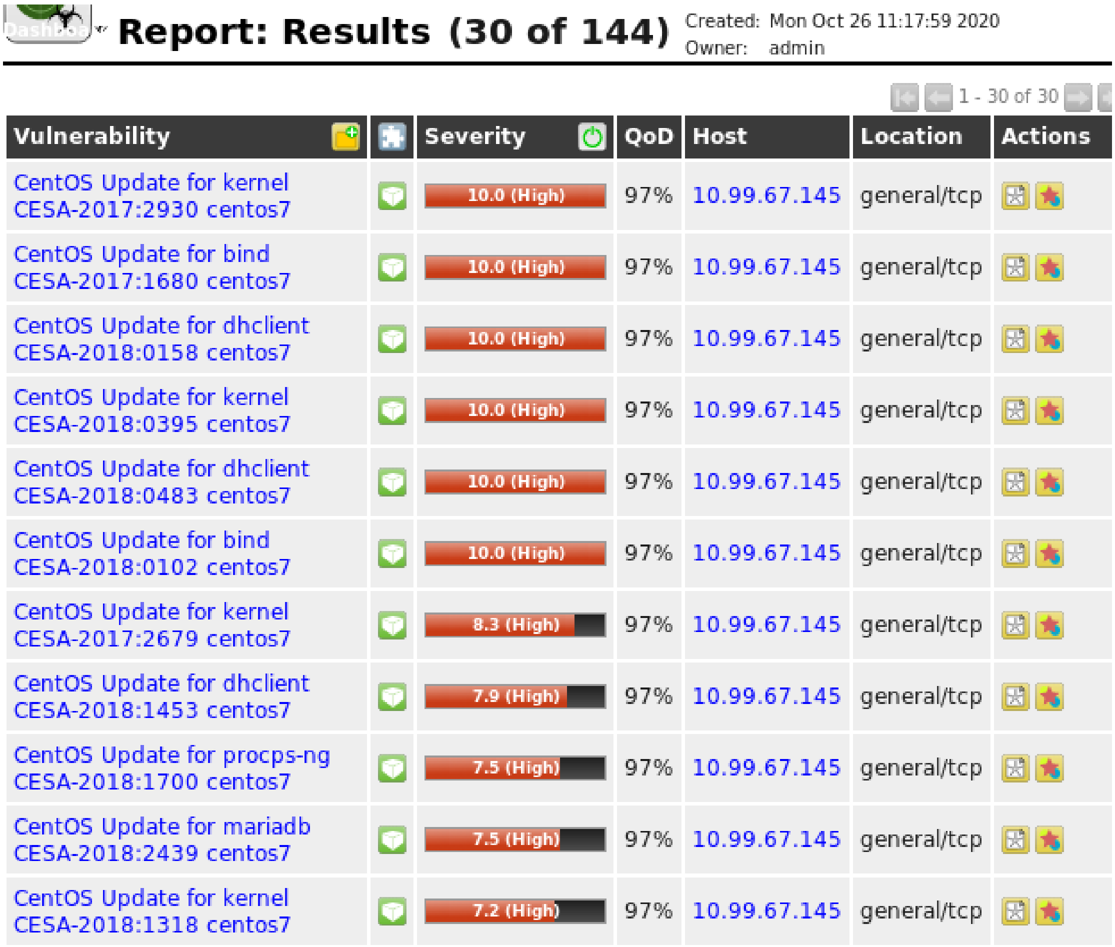
Task: Credential Linux 10.99.67.145

Name:	**Credential Linux 10.99.67.145**
Comment:	Automatically generated by wizard
Target:	Target for Credential Linux 10.99.67.145
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes Apply Overrides: yes Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner) Scan Config: Full and very deep ultimate Order for target hosts: N/A Network Source Interface: Maximum concurrently executed NVTs per host: 10 Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	21 minutes 43 seconds
Average scan duration:	21 minutes 43 seconds
Reports:	1 (Finished: 1, Last: Oct 26 2020)
Results:	57
Notes:	0



Date	Status	Task	Severity	Scan Results			
				High	Medium	Low	Log
Mon Oct 26 11:17:44 2020	Done	Credential Linux 10.99.67.145	10.0 (High)	12	16	2	27

Some of Scan Report Results:

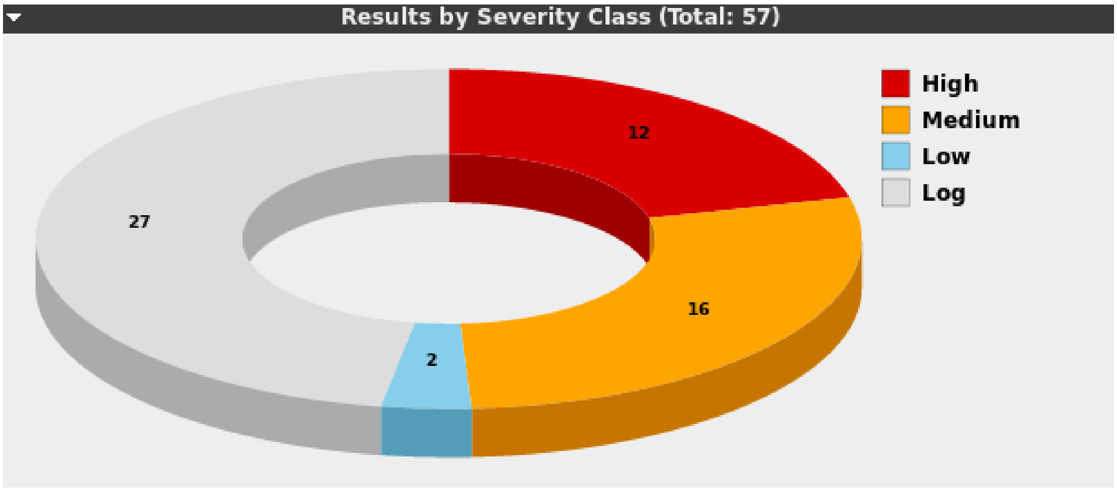


Report: Results (30 of 144)

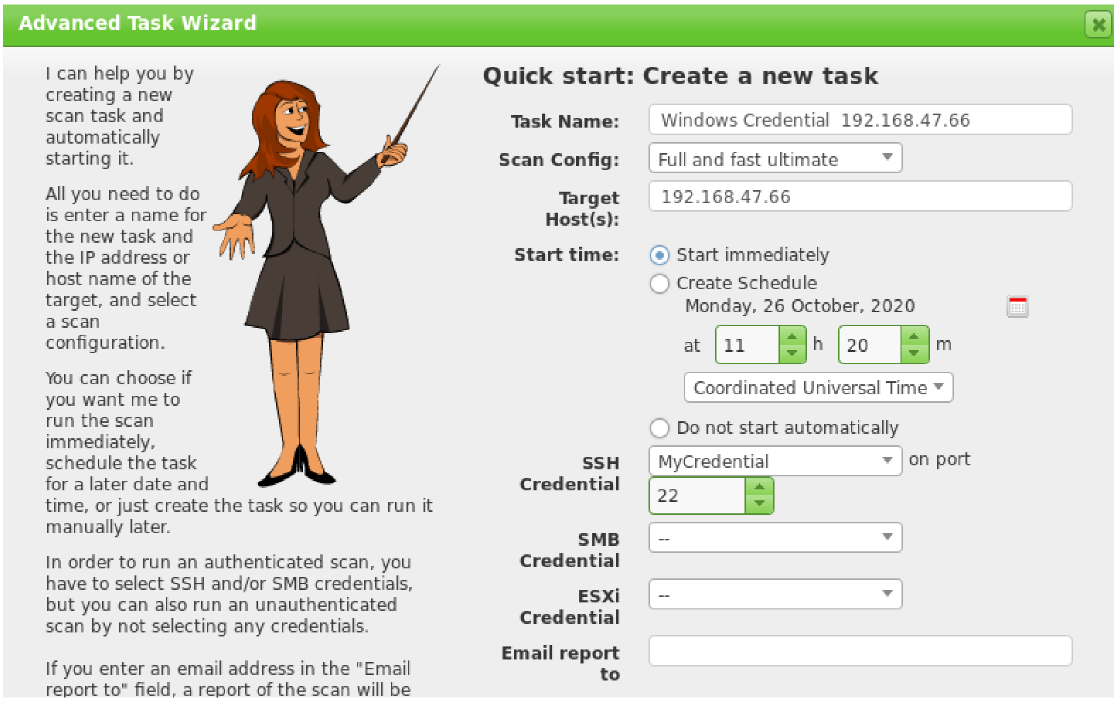
Created: Mon Oct 26 11:17:59 2020
Owner: admin

1 - 30 of 30

Vulnerability		Severity	QoD	Host	Location	Actions
CentOS Update for kernel CESA-2017:2930 centos7		10.0 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for bind CESA-2017:1680 centos7		10.0 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for dhclient CESA-2018:0158 centos7		10.0 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for kernel CESA-2018:0395 centos7		10.0 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for dhclient CESA-2018:0483 centos7		10.0 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for bind CESA-2018:0102 centos7		10.0 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for kernel CESA-2017:2679 centos7		8.3 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for dhclient CESA-2018:1453 centos7		7.9 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for procps-ng CESA-2018:1700 centos7		7.5 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for mariadb CESA-2018:2439 centos7		7.5 (High)	97%	10.99.67.145	general/tcp	
CentOS Update for kernel CESA-2018:1318 centos7		7.2 (High)	97%	10.99.67.145	general/tcp	



Windows Settings:



I can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose if you want me to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

If you enter an email address in the "Email report to" field, a report of the scan will be

Quick start: Create a new task

Task Name: Windows Credential 192.168.47.66

Scan Config: Full and fast ultimate

Target Host(s): 192.168.47.66

Start time: ● Start immediately

○ Create Schedule
Monday, 26 October, 2020
at 11 h 20 m
Coordinated Universal Time

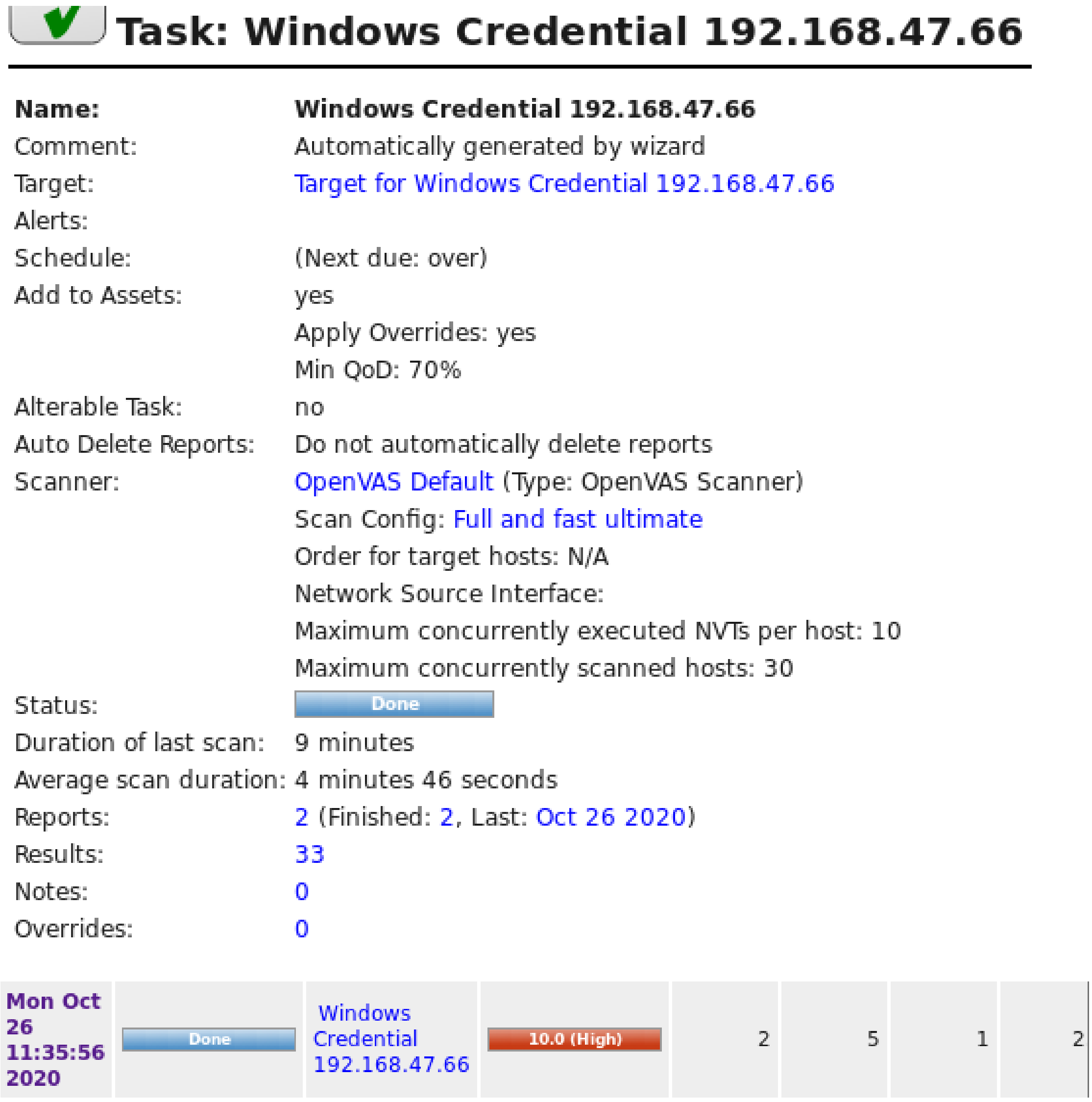
○ Do not start automatically

SSH Credential: MyCredential on port 22

SMB Credential: --

ESXi Credential: --

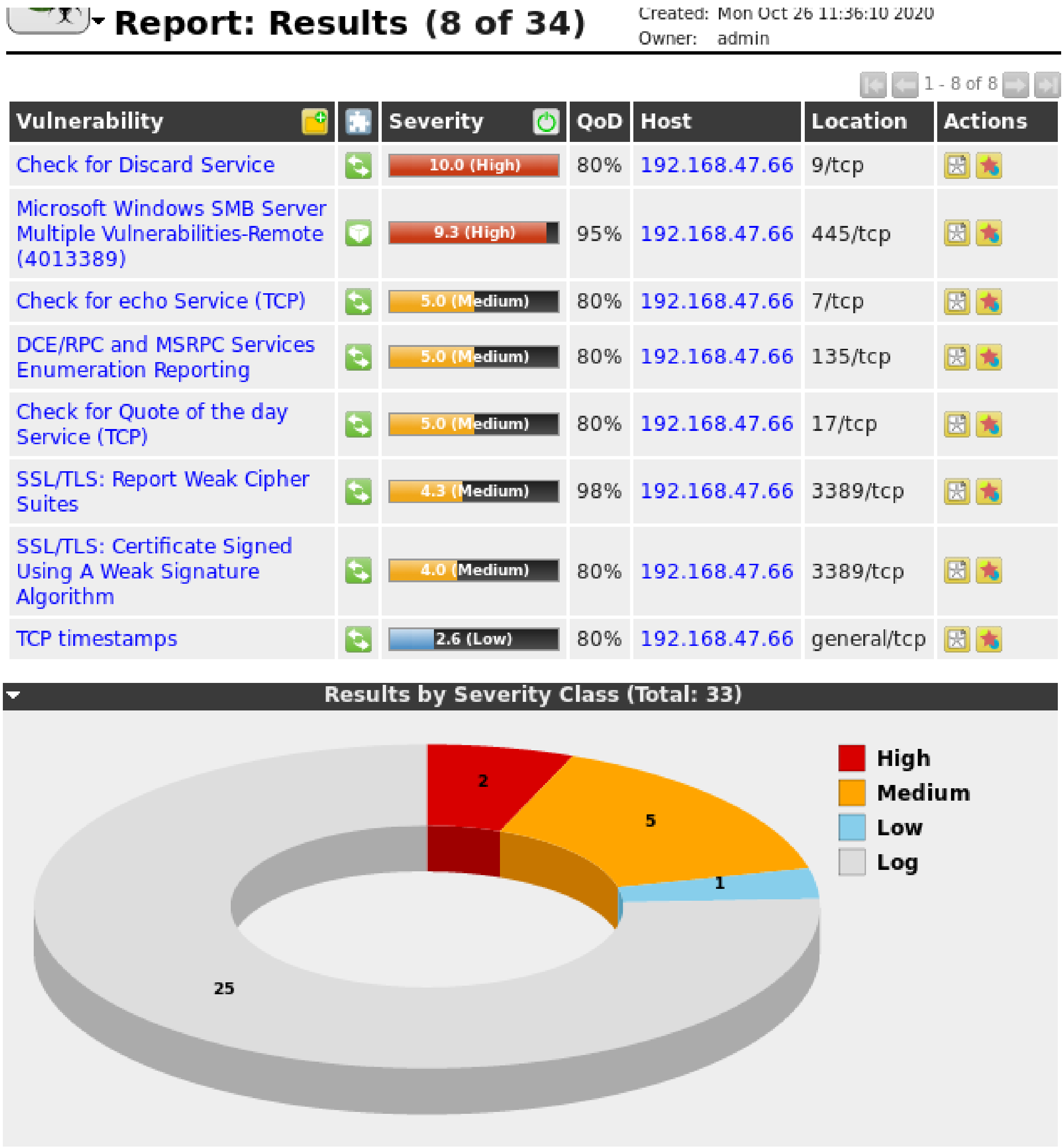
Email report to:



Task: Windows Credential 192.168.47.66

Name:	**Windows Credential 192.168.47.66**
Comment:	Automatically generated by wizard
Target:	Target for Windows Credential 192.168.47.66
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: Full and fast ultimate
	Order for target hosts: N/A
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 10
	Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	9 minutes
Average scan duration:	4 minutes 46 seconds
Reports:	2 (Finished: 2, Last: Oct 26 2020)
Results:	33
Notes:	0
Overrides:	0

Mon Oct 26 11:35:56 2020	Done	Windows Credential 192.168.47.66	10.0 (High)	2	5	1	2



Report: Results (8 of 34)

Created: Mon Oct 26 11:36:10 2020
Owner: admin

1 - 8 of 8

Vulnerability		Severity	QoD	Host	Location	Actions
Check for Discard Service		10.0 (High)	80%	192.168.47.66	9/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	192.168.47.66	445/tcp	
Check for echo Service (TCP)		5.0 (Medium)	80%	192.168.47.66	7/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	192.168.47.66	135/tcp	
Check for Quote of the day Service (TCP)		5.0 (Medium)	80%	192.168.47.66	17/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.47.66	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	192.168.47.66	3389/tcp	
TCP timestamps		2.6 (Low)	80%	192.168.47.66	general/tcp	

Results by Severity Class (Total: 33)

3 SELECT 3 different vulnerabilities that you found, and analyze

3.1 Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) Host 192.168.47.66

Vulnerability Details: CVE-1999-0636

(source -> https://www.cvedetails.com/cve/CVE-2017-0143/)

3.1.1 CVSS metrics

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)

Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

3.1.2 IMPACTS

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.
Impact Level: System

3.1.3 Solution

Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010

3.1.4 VULNERABILITY DETECTION METHODS

Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

3.2 Check for Quote of the day Service (TCP) host 192.168.47.66

3.2.1 CVSS metrics

Source -> https://www.cvedetails.com/cve/CVE-1999-0103/

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None

Vulnerability Type(s)	-
CWE ID	CWE id is not defined for this vulnerability

3.2.2 Impacts

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

3.2.3 SOLUTIONS

Solution type: Mitigation Mitigation

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd

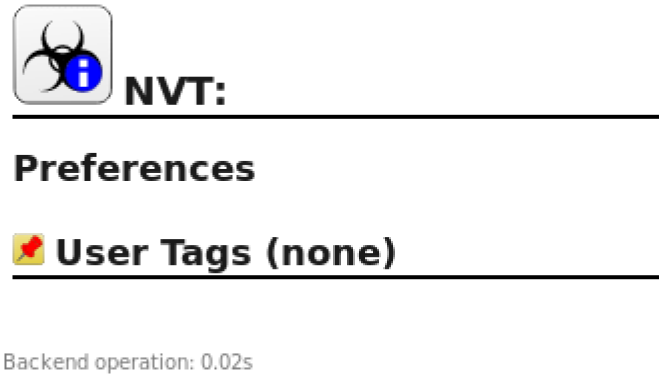
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd

Then launch cmd.exe and type :

```
net stop simptcp net start simptcp
```

To restart the service.

3.2.4 VULNERABILITY DETECTION METHODS



NVT:

Preferences

User Tags (none)

Backend operation: 0.02s

Grrenbone didn’t returned the details of Vulnerability Detection Method.

3.3 CentOS Update for kernel CESA-2018:1965 centos7 host 10.99.67.145

Vulnerability Details : CVE-2017-11600

Source -> https://www.cvedetails.com/cve/CVE-2017-11600/

3.3.1 CVSS metrics

CVSS Score	6.9
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)

Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	125

3.3.2 IMPACTS

---------------(Greenbone didn’t return the impact)----------------------------

3.3.3 SOLUTIONS

Solution type: VendorFix

Please install the updated packages.

3.3.4 VULNERABILITY DETECTION METHODS

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.