jamk.fi

LAB 3 Vulnerability scan

Data security testing

Jere Pesonen TTV18S1
m3227@student.jamk.fi

LAB-03-Vulnerability Scan
10-20
Tieto- ja viestintätekniikka
Tekniikan ja Liikenteen ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

I am not very confident doing external scan from wan, so I focus on these internal scans. Also, I couldn't figure out what is the credential scan?

Linux scan:

Anonymous XML
Done

Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (6 of 133)

ID: 0e520e79-7bcd-443e-a75c-bcd6a76ceae6
Modified: Wed Oct 28 21:37:36 2020
Created: Wed Oct 28 21:15:47 2020
Owner: admin

1 - 6 of 6

Vulnerability	Severity	QoD	Host	Location	Actions
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97%	10.99.67.145	general/tcp	
Source Control Management (SCM) Files Accessible	5.0 (Medium)	80%	10.99.67.145	80/tcp	
Missing `httpOnly` Cookie Attribute	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	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 6 of 6

Windows scan:

Report: Results (11 of 38)

ID: f8af2292-dd6b-4b6a-81f9-e918bf4be3eb
Modified: Wed Oct 28 21:55:12 2020
Created: Wed Oct 28 21:44:30 2020
Owner: admin

1 - 11 of 11

Vulnerability	Severity	QoD	Host	Location	Actions
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97%	10.99.67.150	general/tcp	
Check for discard Service	10.0 (High)	80%	10.99.67.150	9/tcp	
Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)	10.0 (High)	99%	10.99.67.150	3389/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	10.99.67.150	445/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.99.67.150	135/tcp	
Check for Chargen Service (TCP)	5.0 (Medium)	80%	10.99.67.150	19/tcp	
Check for Quote of the Day (qotd) Service (TCP)	5.0 (Medium)	80%	10.99.67.150	17/tcp	
echo Service Reporting (TCP + UDP)	5.0 (Medium)	80%	10.99.67.150	7/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	10.99.67.150	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	10.99.67.150	3389/tcp	
TCP timestamps	2.6 (Low)	80%	10.99.67.150	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 11 of 11

Backend operation: 7.95s

1 Vulnerability 1

Result: Cleartext Transmission of Sensitive Information via HTTP

Vulnerability		Severity	QoD	Host	Location	Actions
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80%	10.99.67.145	80/tcp	

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):

http://10.99.67.145/login.php:password
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

From Metrics:

Access Vector:	Adjacent
Access Complexity:	Low
Authentication:	None
Confidentiality:	Partial
Integrity:	Partial
Availability:	None

Calculate

CVSS Metrics is 4.8 (Medium). It is calculated from metric values above. Value descriptions are straight copies from internet.

- Access vector – Adjacent = The attacker must have access to the broadcast or collision domain of the vulnerable system
- Access complexity – Low = There are no special conditions for exploiting the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.
- Authentication – None = There is no requirement for the attacker to authenticate.
- Confidentiality – Partial = There is considerable disclosure of information, but the scope of the loss is constrained such that not all the data is available.
- Integrity – Partial = Modification of some data or system files is possible, but the scope of the modification is limited.
- Availability – None = There is no impact on the availability of the system.

The impact here is that an attacker could perform a man in the middle attack, when the credentials are passed through http in plaintext. So, the hacker could get access to sensitive information.

The solution for this is to force the data to pass through encrypted connection. For example, redirecting http connections to https page. Also, the credentials itself could be encrypted before transmission. This does not say so in the openvas, but just my idea, do not know if actually possible or necessary.

For vulns detection method it says that script checks HTTP basic authentication, and HTTP Forms with input field of type ‘password’. This is pretty clear since it gets the result by only determining, that there is a sensitive form, that asks for credentials, and the connection doesn’t use any encryption.

2 Vulnerability 2:

Result: Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)

Vulnerability		Severity	QoD	Host	Location	Actions
Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)		10.0 (High)	99%	10.99.67.150	3389/tcp	

Summary
This host is running Microsoft Windows Remote Desktop Services and is prone to the remote code execution vulnerability known as 'BlueKeep'.

Vulnerability Detection Result

By sending a crafted request the RDP service answered with a 'MCS Disconnect Provider Ultimatum PDU - 2.2.2.3' response which indicates that a RCE attack can be executed.

Impact
Successful exploitation would allow an attacker to execute arbitrary code on the target system. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights.

Solution
Solution type: VendorFix

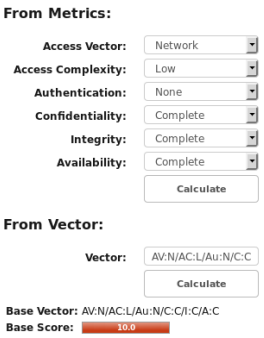
The vendor has released updates. Please see the references for more information.

As a workaround enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2.

NOTE: After enabling NLA affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

Affected Software/OS
- Microsoft Windows 7

- Microsoft Windows Server 2008 R2



CVSS score is 10.0, and high. Value descriptions are straight copies from internet.

- Access vector – Network = The vulnerable interface is working at layer 3 or above of the OSI Network stack. These types of vulnerabilities are often described as remotely exploitable (e.g. a remote buffer overflow in a network service)
- Access complexity – Low = There are no special conditions for exploiting the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.
- Authentication – None = There is no requirement for the attacker to authenticate.
- Confidentiality – Complete = There is total information disclosure, providing access to any / all data on the system. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.
- Integrity – Complete = There is total loss of integrity; the attacker can modify any files or information on the target system.
- Availability – Complete = There is total loss of availability of the attacked resource.

Impact would basically be, that hacker gets the full privileges to system, and so could examine or change data, execute code and programs, and basically everything.

Solution is just to update windows remote desktop service to newest official release. Backdoor stays vulnerable if attacker can still authenticate with valid credentials.

Vuln is detected by sending crafted message to remote desktop service. Service answers with its update release version, which tells if vulnerable is still active (2.2.2.3 or older).

3 Vulnerability 3:

Result: Check for Chargen Service (TCP)

ID: 600fd718-2a2c-4590-b747-a14189ac2acc
Created: Wed Oct 28 21:53:45 2020
Modified: Wed Oct 28 21:53:45 2020
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
Check for Chargen Service (TCP)	5.0 (Medium)	80%	10.99.67.150	19/tcp	

Summary
The remote host is running a 'chargen' service.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution
Solution type: Mitigation

- Under Unix systems, comment out the 'chargen' 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\EnableTcpChargen

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

Then launch cmd.exe and type :

net stop simptcp

net start simptcp

To restart the service.

Vulnerability Insight
When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via TCP, it will continue spewing characters until the client closes the connection.

The purpose of this service was to mostly to test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third party host using this host as a relay.

Vulnerability Detection Method
Details: Check for Chargen Service (TCP) (OID: 1.3.6.1.4.1.25623.1.0.10043)

CVSS Base Score Calculator

From Metrics:

Access Vector:	Network
Access Complexity:	Low
Authentication:	None
Confidentiality:	None
Integrity:	None
Availability:	Partial

Calculate

From Vector:

Vector: AV:N/AC:L/Au:N/C:N

Calculate

Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Base Score: 5.0

CVSS score is 5.0, and medium. Value descriptions are straight copies from internet.

- Access vector – Network = The vulnerable interface is working at layer 3 or above of the OSI Network stack. These types of vulnerabilities are often described as remotely exploitable (e.g. a remote buffer overflow in a network service)
- Access complexity – Low = There are no special conditions for exploiting the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.
- Authentication – None = There is no requirement for the attacker to authenticate.
- Confidentiality – None = There is no impact on the confidentiality of the system.
- Integrity – None = There is no impact on the integrity of the system.
- Availability – Partial = There is reduced performance or loss of some functionality.

Impact is ping pong attack where attacker spoofs packet between two computers. They send packets back and forth on and on, and this slows systems and the whole network.

Since this is a windows machine, you must modify registry keys to 0 as seen in the screenshot. After that you must restart the simptcp service

Vulnerability detection method is not informed.