Threat Modeling Report

Created on 2/28/2022 2:12:00 PM

Threat Model Name: Exploitation of vulnerable SMB service while pentesting

Owner: Noel Varghese

Reviewer: -

Contributors:

Description: A patched Kali VM is used by the attacker to exploit the SMB service (port 139/445) on the target host. Other services are also present within the respective hosts. Target host can be exploited, using the appropriate payload, from Metasploit or other exploits present on the Dark web/Clear web. Gain initial foothold and escalate privileges,as per the number of security misconfigurations on the victim machine. Appropriate steps to identify and justify the vulnerabilities and threats have been documented.Mitigation of threats has been performed, wherever applicable

Assumptions: Vulnerable SMB Server on the target host

External Dependencies:

Threat Model Summary:

Not Started	2
Not Applicable	2
Needs Investigation	5
Mitigation Implemented	3
Total	12
Total Migrated	0

Diagram: Diagram 1

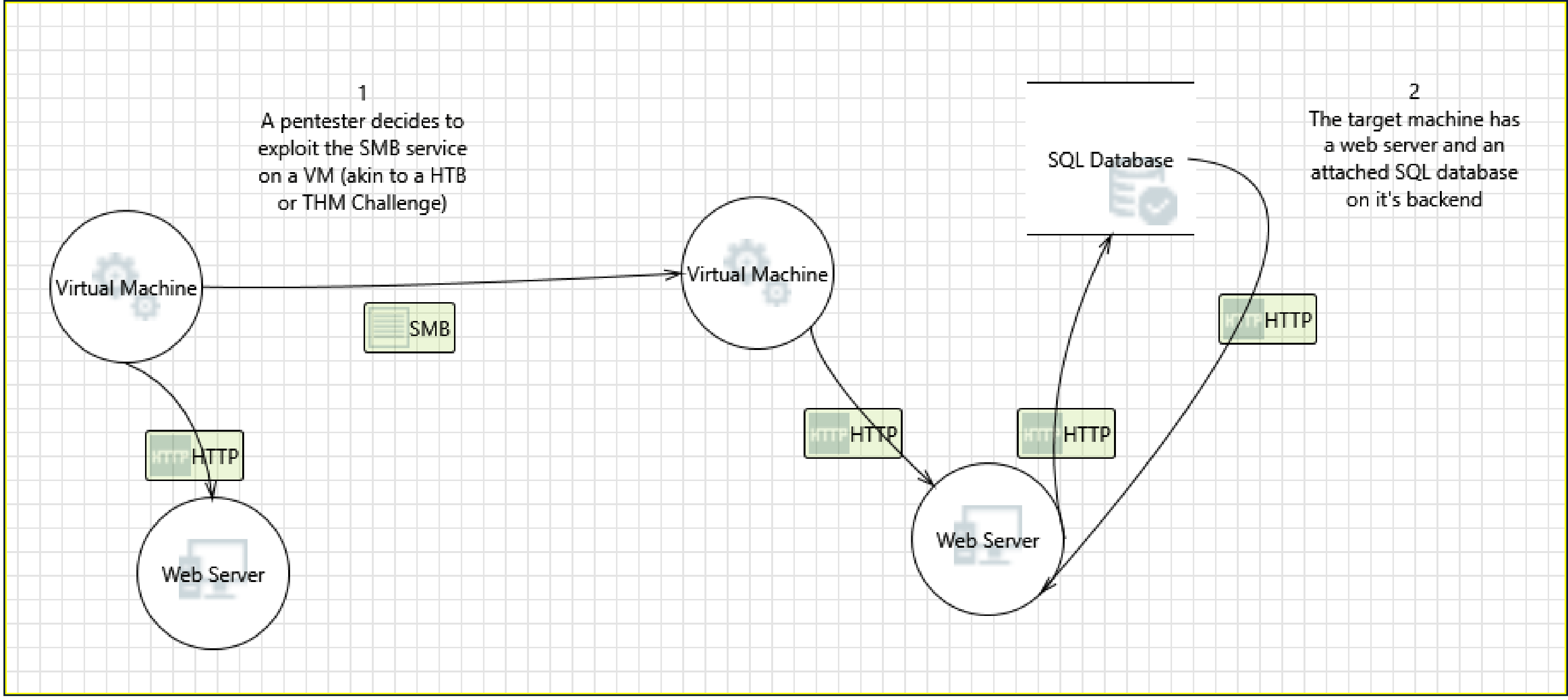
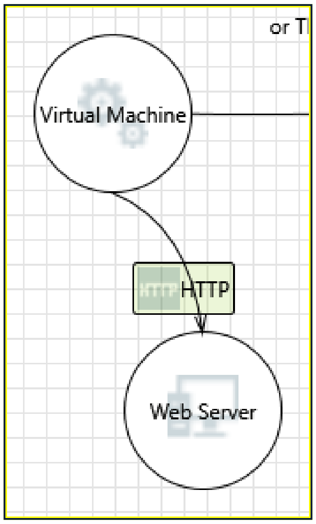

1
A pentester decides to exploit the SMB service on a VM (akin to a HTB or THM Challenge)
Virtual Machine
SMB
Virtual Machine
HTTP
Web Server
SQL Database
2
The target machine has a web server and an attached SQL database on it's backend
HTTP
HTTP
HTTP
Web Server

Diagram 1 Diagram Summary:

Not Started	2
Not Applicable	2
Needs Investigation	5
Mitigation Implemented	3
Total	12
Total Migrated	0

Interaction: HTTP



1. Cross Site Scripting [State: Not Applicable] [Priority: High]

Category:	Abuse
Description:	The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification:	Web server belongs to attacker&#39;s own VM

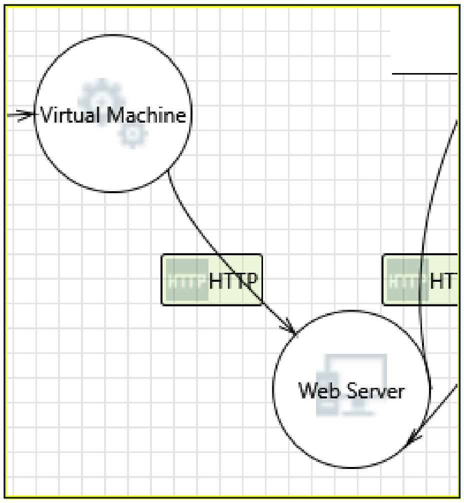
2. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Web Server may be able to impersonate the context of Virtual Machine in order to gain additional privilege.

Justification: Web server belongs to attacker&#39;s own VM

Interaction: HTTP



3. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: Vulnerable attack vector

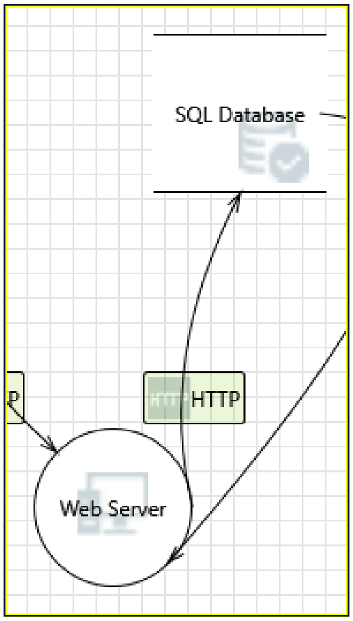
4. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

Description: Web Server may be able to impersonate the context of Virtual Machine in order to gain additional privilege.

Justification: Gain additional privileges on target machine

Interaction: HTTP



5. Spoofing of Destination Data Store SQL Database [State: Not Started] [Priority: High]

Category: Spoofing

Description: SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Possible attack vector

6. Potential SQL Injection Vulnerability for SQL Database [State: Needs Investigation] [Priority: High]

Category: Tampering

Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

Justification: Vulnerable attack vector

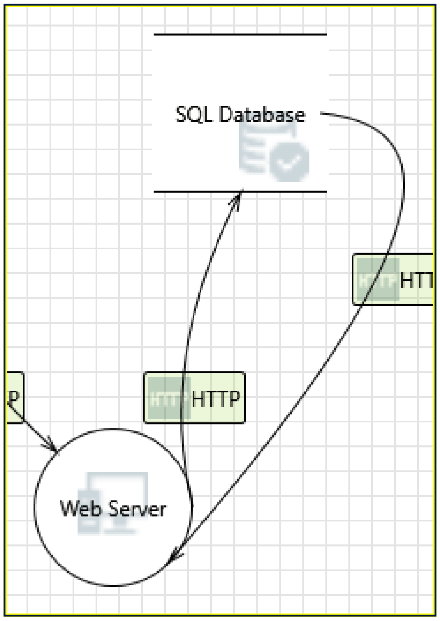
7. Potential Excessive Resource Consumption for Web Server or SQL Database [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Web Server or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Not possible,unless the server or database are under a DDOS attack

Interaction: HTTP



8. Spoofing of Source Data Store SQL Database [State: Needs Investigation] [Priority: High]

Category: Spoofing

Description: SQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to Web Server. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

9. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category:	Tampering
Description:	The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification:	XSS is not a possible attack vector that can be used to exfiltrate data from a database

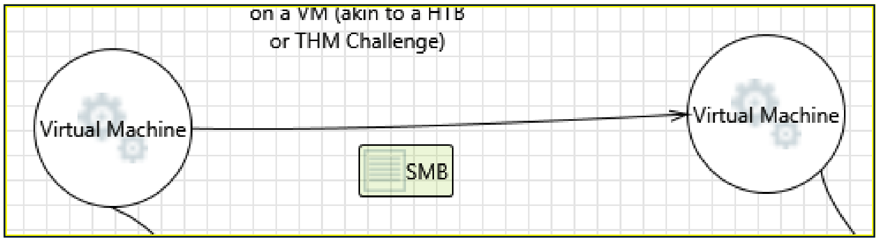
10. Persistent Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category:	Tampering
Description:	The web server 'Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'SQL Database' inputs and output.
Justification:	XSS is not a possible attack vector that can be used to exfiltrate data from a database

11. Weak Access Control for a Resource [State: Needs Investigation] [Priority: High]

Category:	Information Disclosure
Description:	Improper data protection of SQL Database can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification:	Database can possibly be exploited,resulting in a breach

Interaction: SMB



12. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category:	Elevation Of Privilege
Description:	Virtual Machine may be able to impersonate the context of Virtual Machine in order to gain additional privilege.
Justification:	Attack vector exploitation to gain access into a foreign host