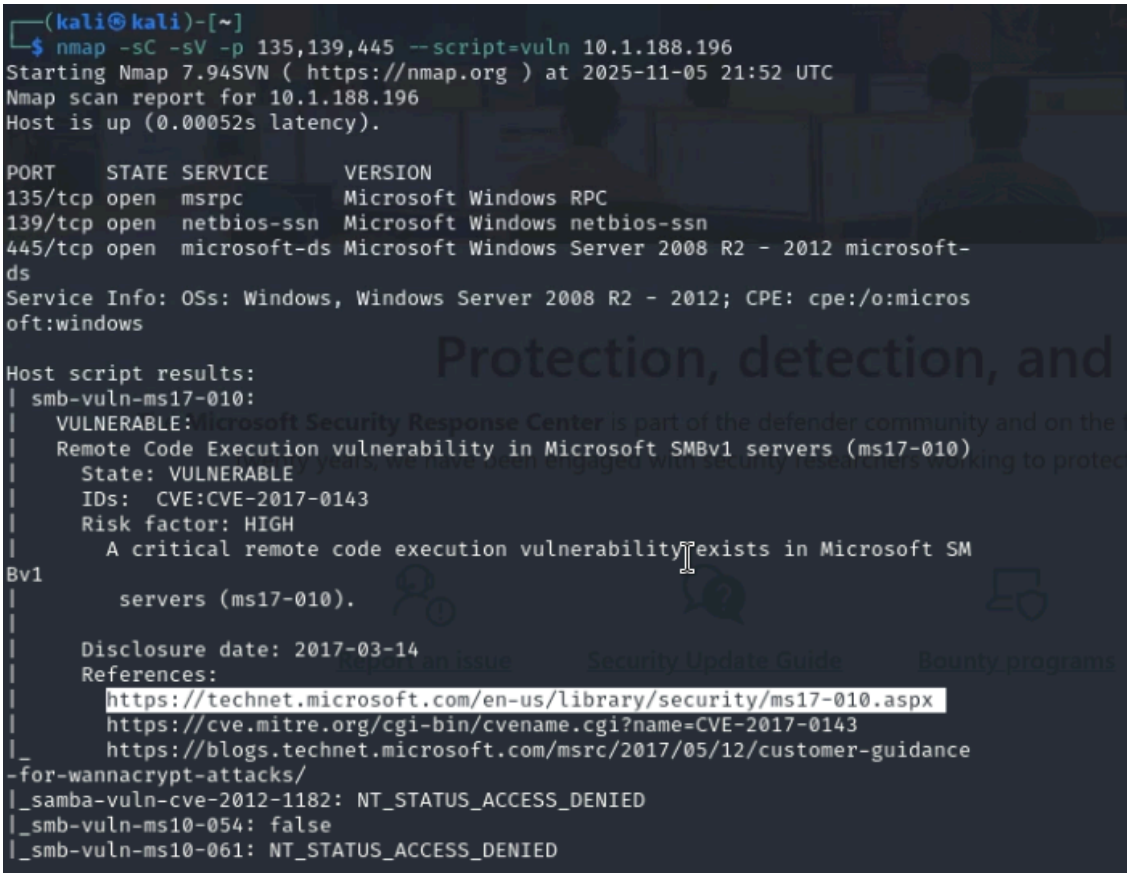
FINDING #1	SMB RCE
HOST NAME	metawindows.goodcorp.lab
IP ADDRESS	10.1.188.196

LIKELIHOOD	IMPACT	SEVERITY
Critical	Critical	Critical

DESCRIPTION
During the scan, I recognized that there is a Remote Code Execution (RCE) vulnerability in Microsoft SMBv1 servers running on the host machine. RCE in Windows environments allow remote attackers to execute arbitrary code via specially crafted packets as SYSTEM, potentially allowing for complete compromise of the affected machine. The vulnerability falls under CWE-20 (Improper Input Validation) and stems from SMBv1 receiving malformed or crafted SMB packets as a result of its mishandling of untrusted inputs. The vulnerability is triggered when packet sizes are not checked correctly. Due to a mathematical error in how SMBv1 calculates size and boundaries of buffers allocated for incoming transaction data, the server can allocate too little memory for what is actually needed. Attacker submits an initial large transaction and follows it with a secondary packet that is smaller than needed which causes the server to allocate insufficient memory. The server then trusts and processes more data than the buffer can hold. This out-of-bounds write hijacks program execution by modifying critical data structures in kernel memory allowing the attacker to control the flow of execution within the operating system kernel. Because the server trusts the data from the network and fails to ensure the proper size, order and integrity of secondary SMB packets, attackers can overwrite memory achieving the code execution to fully compromise the system. This vulnerability exposes the host to significant security risks allowing the attacker unfettered access to the system giving them access to login credentials, financial information, confidential documents and altering data. Ultimately this could lead to data breaches, financial loss, and severe reputational damage.

VALIDATION

During the scan it was identified as a possible vulnerability with the following command: “nmap -sC -sV -p 135,139,445 –script=vuln 10.1.188.196”



The vulnerability was confirmed and tested through Metasploit with the following command: “set RHOSTS 10.1.188.196”

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.1.188.196
RHOSTS ⇒ 10.1.188.196
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                Required
   ----         ---------------                                --------
   CHECK_ARCH   true                                           no
   CHECK_DOPU   true                                           no
   CHECK_PIPE   false                                          no
   NAMED_PIPES  /usr/share/metasploit-framework/data/word      yes
                lists/named_pipes.txt
   RHOSTS       10.1.188.196                                   yes

   RPORT        445                                            yes
   SMBDomain    .                                              no
   SMBPass                                                     no
   SMBUser                                                     no
   THREADS      1                                              yes
```

REMEDIATION

The following steps are recommended for remediation:

Apply security patches

1. Deploy Microsoft MS17-010 security update to all affected Windows systems immediately.

Disable SMBv1 Protocol

1. Where possible, completely disable the SMBv1 protocol on all Windows machines
    a. It is outdated and no longer necessary for most environments
2. Use powershell or Group Policy settings to ensure SMBv1 is not enabled or running.
    a. Ensures additional protection even if vulnerable system is present

Verify and Audit Patch Deployment

1. Use endpoint management tools or vulnerability scanners to confirm patch has been applied everywhere and that SMBv1 is not available on the network.

Network Segmentation and Firewalls

1. Block inbound and outbound traffic to TCP port 445 (SMB)
    a. Particularly at network perimeters and between network zones where SMB traffic not required.
2. Minimize lateral movement opportunities by limiting exposure to file sharing services internally (least privilege).

Remove unnecessary Shares and Harden Configuration

1. Audit Windows shares to ensure only required and secured shares exist with least privilege access rights.

REFERENCES		
MITRE ID	**TECHNIQUE NAME**	**DESCRIPTION**
T1190	Exploit Public Facing Application	This technique involves adversaries exploiting known or unknown vulnerabilities in internet-exposed applications, such as web servers or SMB services, to gain initial access to a network or system. By leveraging bugs, misconfigurations, or weaknesses in these services, attackers bypass normal authentication and enter target environments.
T1210	Exploitation of Remote Services	Adversaries target vulnerabilities or improper configurations in remote services (like SMB) with specifically crafted network traffic, allowing them to execute code or commands on remote systems from any accessible network location. Successful exploitation results in unauthorized control, often escalating privileges or spreading laterally across the network.
T1059	Command and Scripting Interpreter	Attackers leverage local or remote command-line interfaces and scripting environments (such as PowerShell, bash, or Windows Command Prompt) to execute arbitrary commands or scripts on a target machine. This enables automation of payloads, execution of further attack steps, and control over compromised systems through scriptable interfaces
MITRE ID	**MITIGATION NAME**	**DESCRIPTION**
M1054	Software Update	Regularly update and patch software, operating systems, and applications to address known vulnerabilities and minimize the window of opportunity for attackers to exploit unpatched flaws.
M1042	Disable or Remove Feature of Program	Turn off or uninstall unused, unsafe, or legacy software or protocols—such as SMBv1—to reduce the attack surface and eliminate avenues for exploitation

M1053	Software Configuration	Adjust and harden configuration settings of systems and applications to minimize security risks, including disabling insecure functionalities and enforcing secure defaults
M1030	Network Segmentation	Divide networks into trusted zones and restrict connections between them to limit an attacker's ability to move laterally and access sensitive resources.
M1022	Restrict File and Directory Permissions	Set stringent access controls and permissions on critical files and directories to ensure only authorized users and processes can modify or access them, reducing exploitation risk
TECHNICAL ARTICLES	https://attack.mitre.org/techniques/T1190/ https://attack.mitre.org/techniques/T1210/ https://attack.mitre.org/techniques/T1059/ https://www.cve.org/CVERecord?id=CVE-2017-0143 https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 https://www.juniper.net/us/en/threatlabs/ips-signatures/detail.SMB:CVE-2017-0143-MC.html https://cloud.google.com/blog/topics/threat-intelligence/smb-exploited-wannacry-use-of-eternalblue/ https://research.checkpoint.com/2017/eternalblue-everything-know/ https://www.crowdstrike.com/en-us/blog/badrabbit-ms17-010-exploitation-part-one-leak-and-control/	