Attacking Windows using RDP Blue Keep exploit and learning defence

Bluekeep is a critical Remote Code Execution vulnerability in Microsoft's RDP service running on TCP port 3389. It could allow an attacker to execute remote code on a vulnerable machine that's running Remote Desktop Protocol (RDP). As the vulnerability is wormable, it spread rapidly. By sending a specially crafted packet a memory corruption bug is created in the target machine. The attacker crashes the kernel which causes a blue screen of death on the victim machine resulting in a Denial of Service (DoS) attack. Due to RDP vulnerability on versions earlier than windows 8.1. an attacker can also execute remote code execution and by placing a backdoor on the victim machine, it gets compromised.

Affected machines with this vulnerability:

Windows 7, Windows Server 2008, Windows Vista, and Windows Server 2004 machines with RDP enabled.

In this exercise, you will learn about the blue keep vulnerability, and its exploitation resulting in a Denial of Service attack, indicators of compromise, mode of Detection, mitigation, and prevention technique for this attack.

Indicator of Attack (IOA)

Indicators of attack(IOAs) are some events that could reveal an active attack before indicators of compromise become visible. It is not always possible to detect Indicators of attack, as the attackers generally target your machines when you are not available with them.
IOAs disclose the motivations of the attacker and the specific tools used in each process.

Examples of Indicators of Attacks(IOA)

I. Excessive SMTP traffic. Could be evidence of a compromised system being used to launch DDoS attacks.
II. Malware reinfection within a few minutes of removal. This could be indicative of an Advanced Persistent Threat.
III. Multiple user logins from different regions. This could be indicative of stolen user credentials.
IV. Network scans by internal hosts communicating with multiple hosts in a short time frame, which could reveal an attacker moving laterally within the network.

Indicators of Compromise (IOCs)

Indicators of Compromise (IOC) are pieces of forensic data, such as data found in host-based log entries or files, that identify potentially malicious activity on a system or network. An IOC is an indication that can be used to indicate an intrusion or compromise of a host in a network. Examples of an IOC include unusual network traffic, unusual privileged user account activity, login anomalies, increases in database read volume, suspicious registry or system file changes, etc.

IOC can reveal:

A. Tactics, Techniques, and Procedures (TTP) used during a cyberattack.
B. Severity of the event. Event severity is calculated based on the severity weight given in vulnerabilities.
C. Where to focus incident response and mitigation

Incident response is an approach to handling security breaches. The aim of incident response is to identify an attack, contain the damage, and know the root cause of the incident.

D. Who are the threat actors?

A threat actor also called a malicious actor is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact the security of an organization.

IOCs are a key source for:

1. Identification of an Advanced Persistent Threat (APT)
2. Indicating something is wrong with the network
3. Forensic identification of crime or attack
4. Understanding how a compromise occurred
5. Testing your system or network for vulnerabilities
6. Watch the Authentication Activity

Example: Anomalies in privileged account activity

Check the number of users created with administrator privilege

Guided Exercise

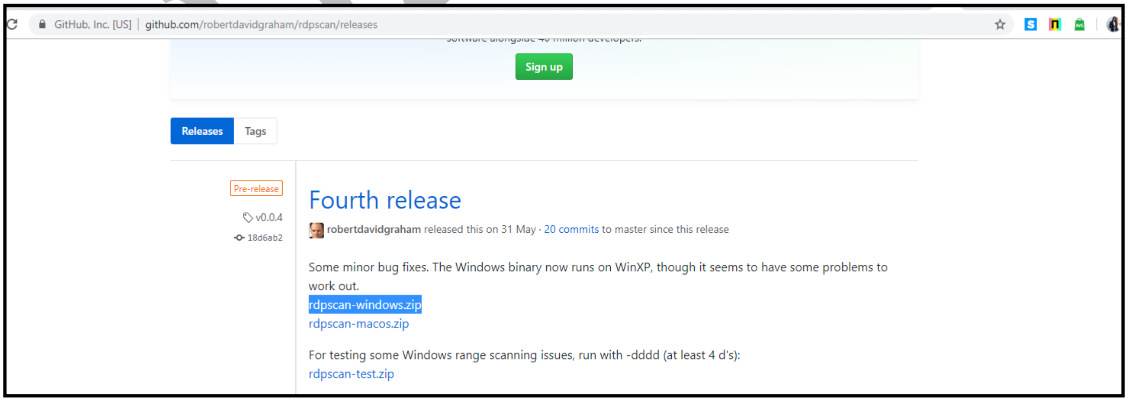
Checking the Vulnerability of the Windows machine for Bluekeep vulnerability

You can check your machine for RDP protocol related vulnerabilities using the RDP scan tool.

Testing your machine for Bluekeep vulnerability using RDPScan:

RDPScan is a free tool available to check this vulnerability.

Step1. Download the latest version from the below link
https://github.com/robertdavidgraham/rdpscan/releases


GitHub, Inc. [US] | github.com/robertdavidgraham/rdpscan/releases
Sign up
Releases
Tags
Pre-release
v0.0.4
18d6ab2

Fourth release

robertdavidgraham released this on 31 May · 20 commits to master since this release

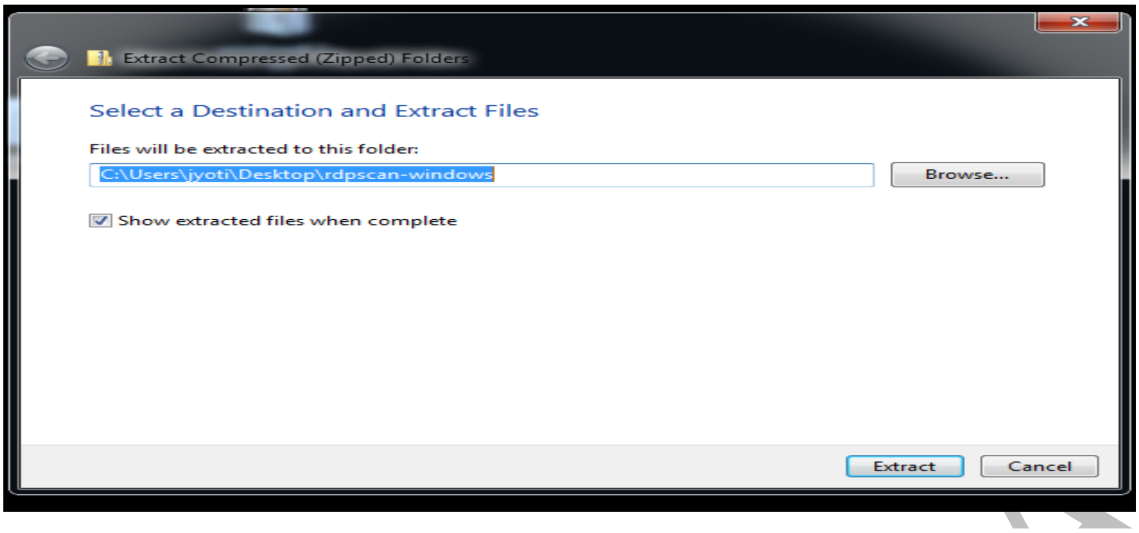
Some minor bug fixes. The Windows binary now runs on WinXP, though it seems to have some problems to work out.

rdpscan-windows.zip
rdpscan-macos.zip

For testing some Windows range scanning issues, run with -dddd (at least 4 d's):

rdpscan-test.zip

Extract the file of rdpscan-windows in the default location.



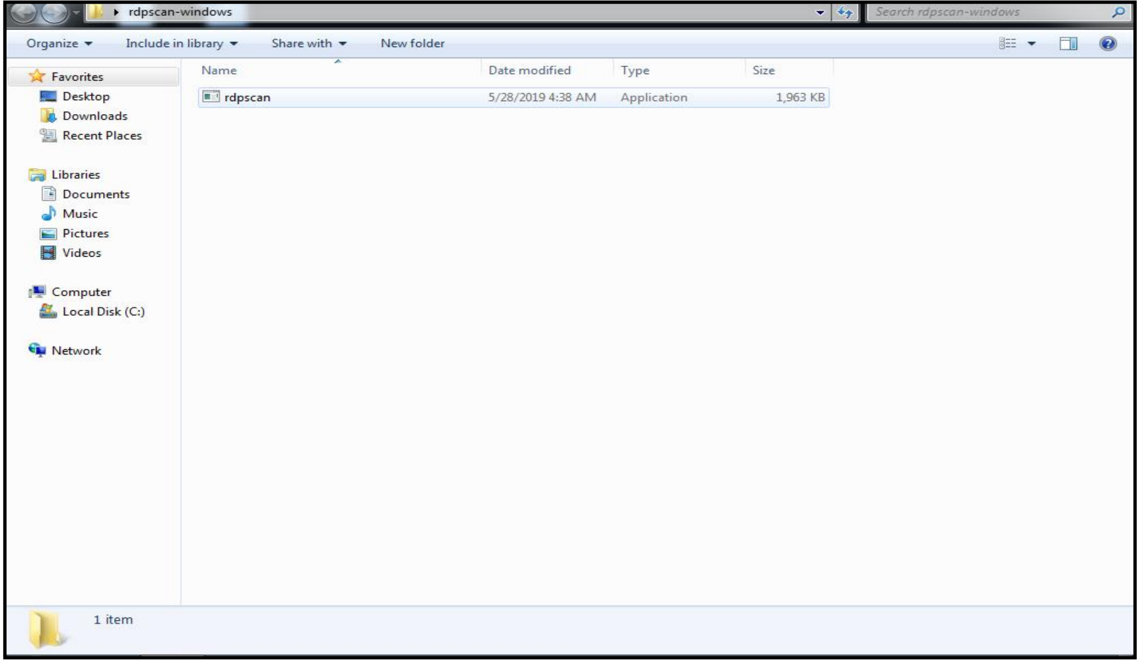
Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

C:\Users\jyoti\Desktop\rdpscan-windows

☑ Show extracted files when complete



rdpscan-windows

Name	Date modified	Type	Size
rdpscan	5/28/2019 4:38 AM	Application	1,963 KB

1 item

Run the program from the command line using the following commands:

Scan a single host:

```
rdpscan [ip_address]
rdpscan 192.168.153.138
```

Scan a range of IP addresses:

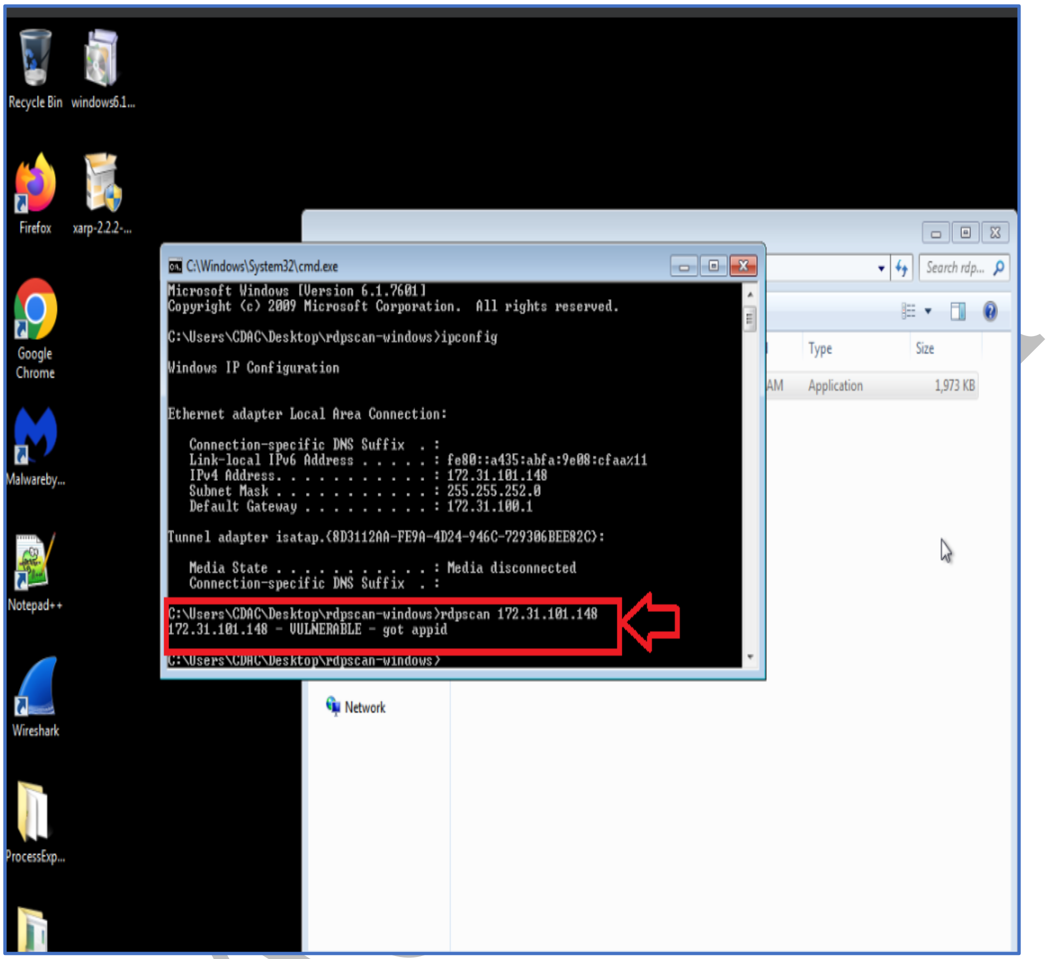
```
rdpscan [start_ip_address]-[end_ip_address]
```

Scan a network with CIDR notation:

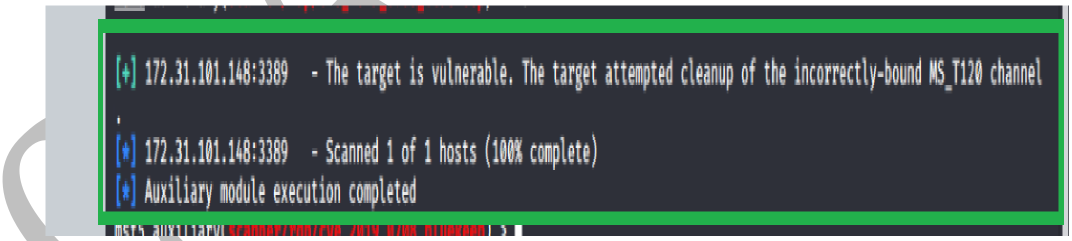
```
rdpscan [network]/[cidr_notation]
rdpscan 192.168.153.0/24
```

This command will scan each of the IP addresses to find out if port 3389 is open and vulnerable.

If a windows machine is vulnerable to blue keep RDP vulnerability, the rdpscan tool will show status as vulnerable.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\CDAC\Desktop\rdpscan-windows>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a435:abfa:9e08:cfaa%11
   IPv4 Address. . . . . . . . . . . : 172.31.101.148
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 172.31.100.1

Tunnel adapter isatap.{8D3112AA-FE9A-4D24-946C-729306BEE82C}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\CDAC\Desktop\rdpscan-windows>rdpscan 172.31.101.148
172.31.101.148 - VULNERABLE - got appid

C:\Users\CDAC\Desktop\rdpscan-windows>
```



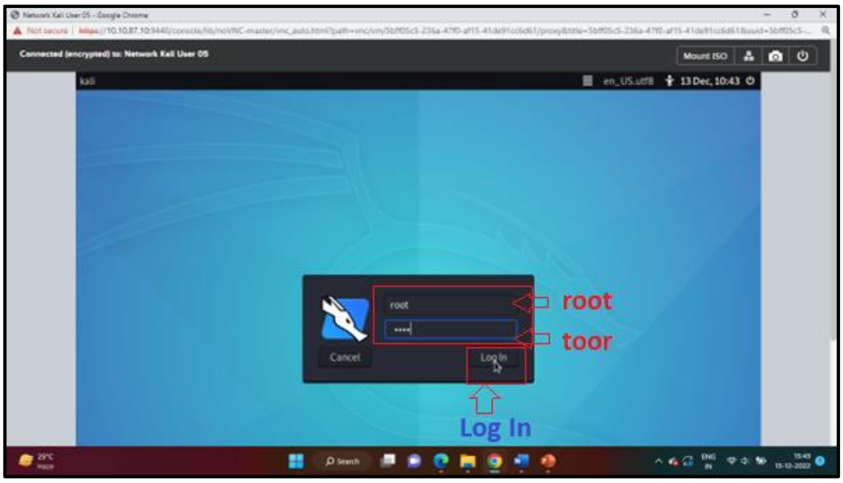
```
[+] 172.31.101.148:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel
.
[*] 172.31.101.148:3389   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Detection of Bluekeep RDP attack (Indicators of Attack):

A. Performing Bluekeep RDP Attack on the Windows machine in your user account

To detect the IoA on your machine for a Bluekeep vulnerability-based attack, you have to first attack the machine through the following steps.

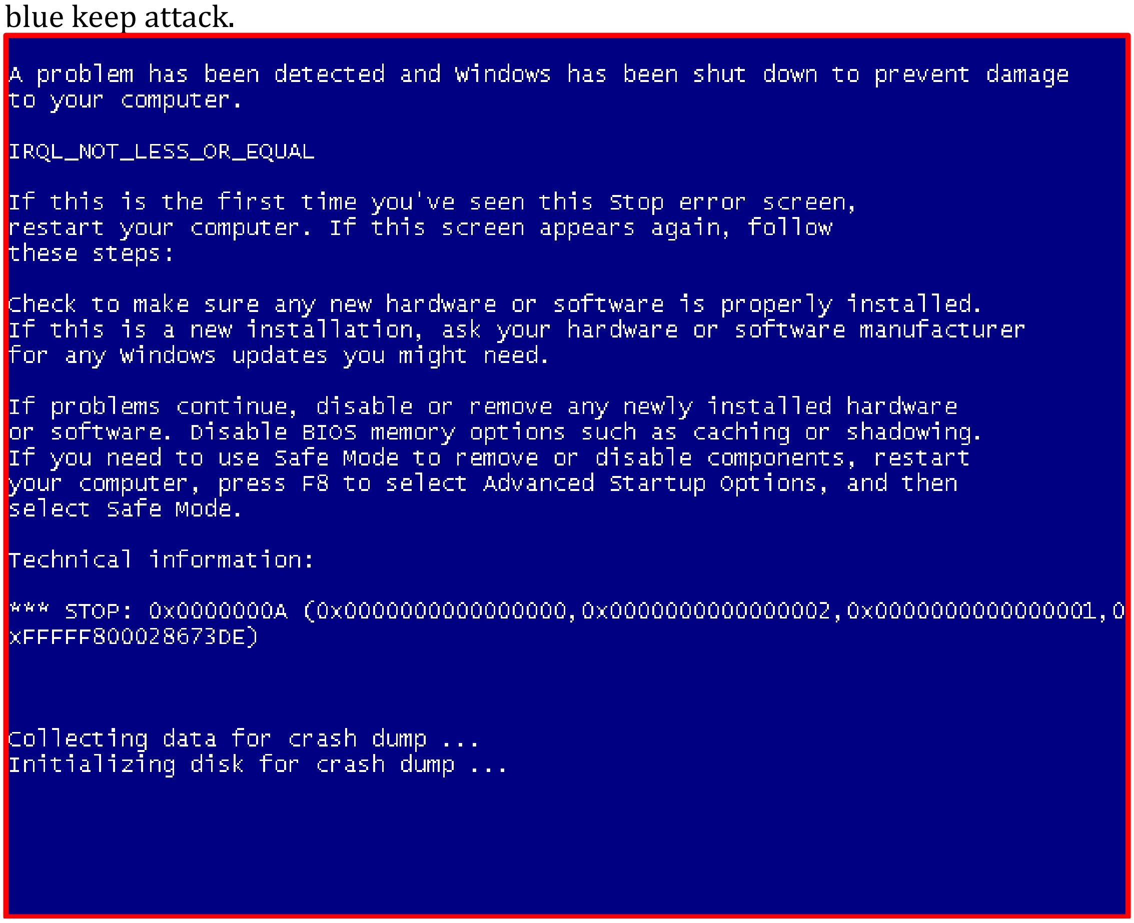
1. Connect to the kali Linux machine, created by you, using the RDP protocol. Kali Linux machine is being used as Attacker's machine.
2. When prompted for the username and password, enter root as username and toor as password. The root is the administrator user of the machine.



B. Detection of Bluekeep RDP attack

If the attack happens on your machine, the following may be the indicators of the attack:

1. Blue screen of death: the following screen will be the first visible sign of an RDP blue keep attack.



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000000A (0x0000000000000000,0x0000000000000002,0x0000000000000001,0
xFFFFF800028673DE)



Collecting data for crash dump ...
Initializing disk for crash dump ...
```

2. Using Event Log Viewer

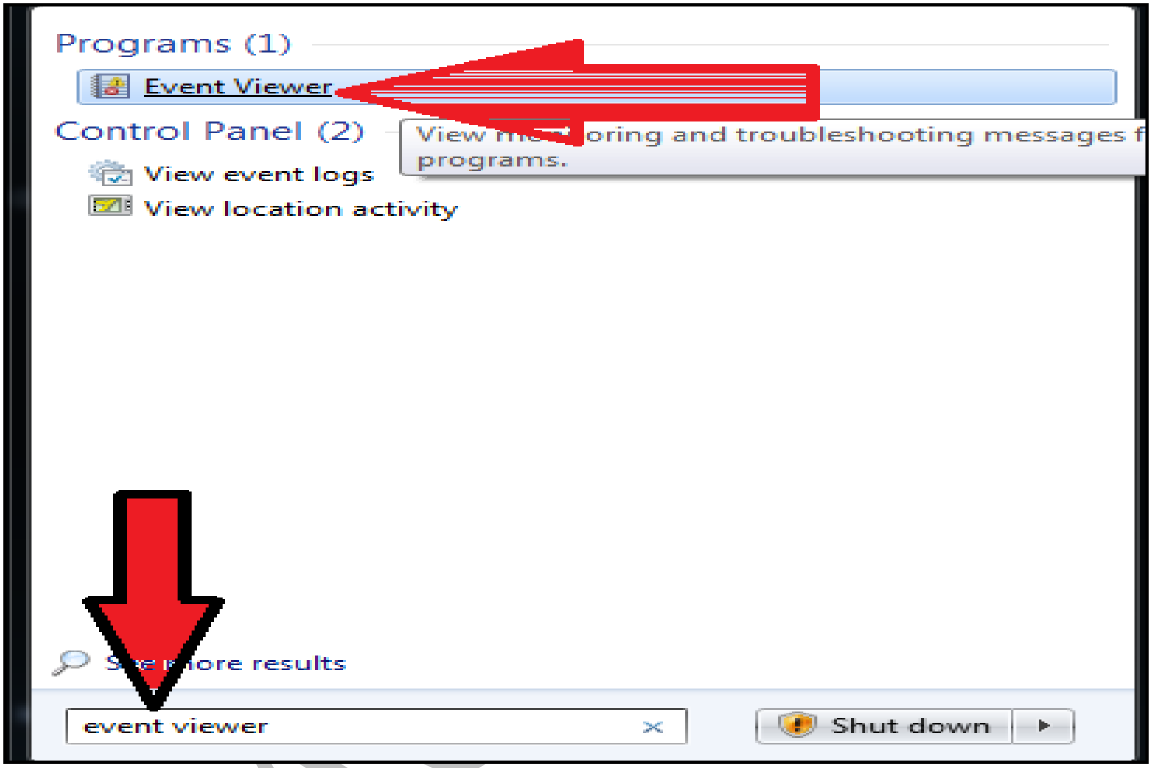
   The Windows Event Viewer shows logs of applications and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems.

https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/

If the blue screen appears several times in the user machine, the user must check Event Viewer logs because when the attacker runs the exploit script for Bluekeep vulnerability, it will send the authentication packet, which generates the events “TerminalServices-**RemoteConnectionManager**”.

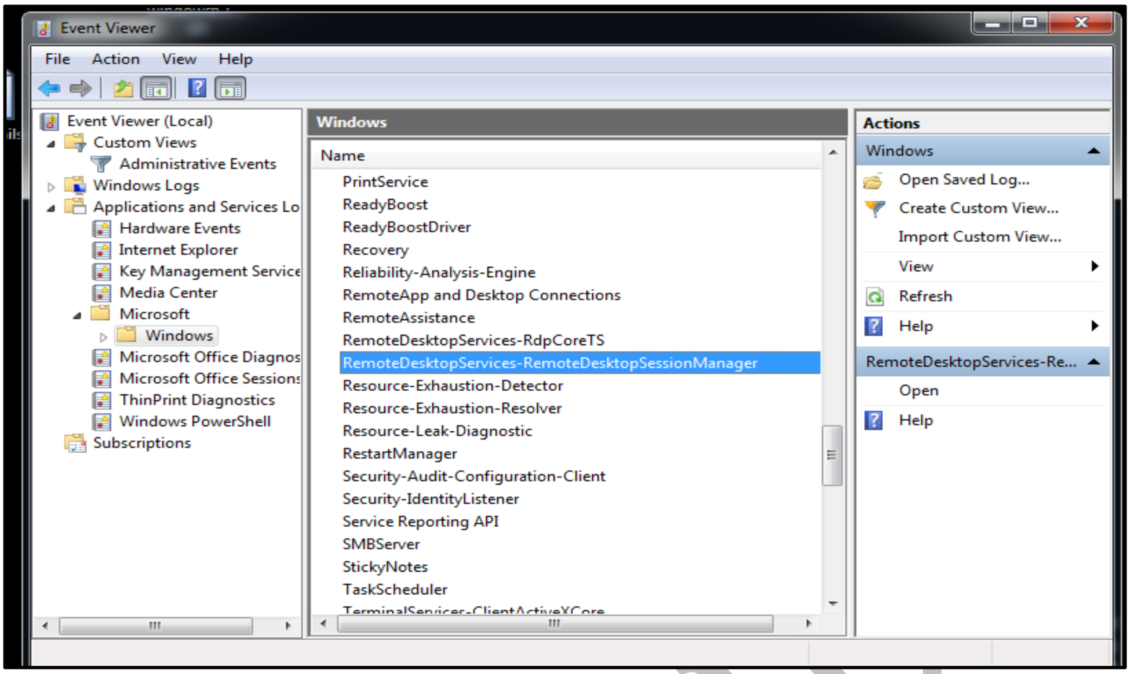
The following steps must be performed to check Event Viewer Logs.

1. Type Event Viewer in the Windows search box.

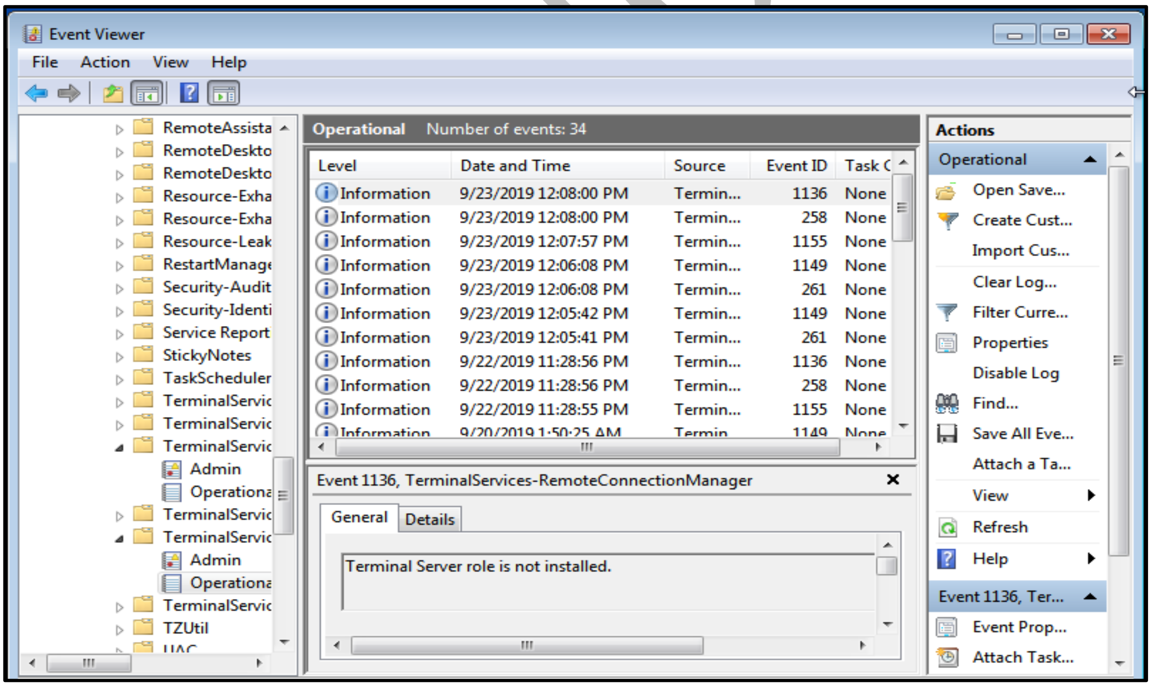


event viewer

2. Click on Applications and **Services Logs>Microsoft>Windows>RemoteDesktopServices-RemoteDesktopSessionManager**



3. Click on**TerminalServices-RemoteConnectionManager.** Expand it and **Click on Operational** to find events TerminalServices **-RemoteConnectionManager.** The presence of these events ensures the RDP-related attack.



Operational Number of events: 34

Level	Date and Time	Source	Event ID	Task C
Information	9/23/2019 12:08:00 PM	Termin...	1136	None
Information	9/23/2019 12:08:00 PM	Termin...	258	None
Information	9/23/2019 12:07:57 PM	Termin...	1155	None
Information	9/23/2019 12:06:08 PM	Termin...	1149	None
Information	9/23/2019 12:06:08 PM	Termin...	261	None
Information	9/23/2019 12:05:42 PM	Termin...	1149	None
Information	9/23/2019 12:05:41 PM	Termin...	261	None
Information	9/22/2019 11:28:56 PM	Termin...	1136	None
Information	9/22/2019 11:28:56 PM	Termin...	258	None
Information	9/22/2019 11:28:55 PM	Termin...	1155	None
Information	9/20/2019 1:50:25 AM	Termin	1149	None

Event 1136, TerminalServices-RemoteConnectionManager

Terminal Server role is not installed.

Prevention from the attack:

You can prevent your machines from Blue Keep vulnerability-based attacks using the following steps.

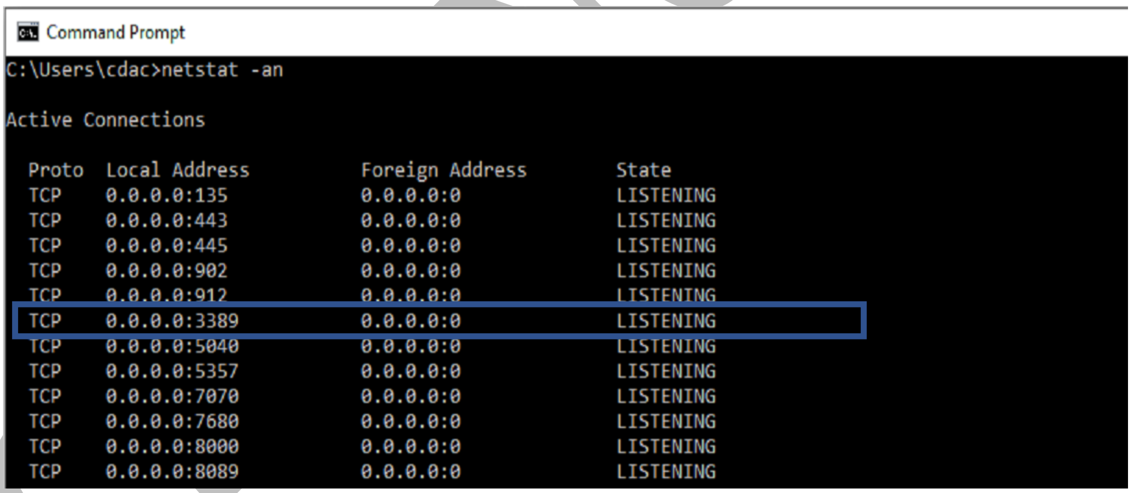
1. **Patch insecure computers.**

2. **Block vulnerable ports:** Users can also prevent the BlueKeep vulnerability by blocking port 3389 at firewalls, which is used by the RDP. This port should especially be blocked if devices and the firewall are facing the external Internet.
3. **Disable unnecessary services:** Any services that are not required, such as remote desktop services, should be blocked to prevent potential security gaps that attackers could exploit.
4. **Enable network control:** Organizations can enable Network Level Authentication (NLA), which gives them control of users that connect to their systems and prevent unauthorized access to their data and resources. This also helps them block unauthorized users looking to exploit the BlueKeep vulnerability to attack the business.
5. **Educate users:** In addition to patching systems, installing the latest software, and protecting networks, it is also important to be aware of the latest risks. Users need to ensure they understand the risks they face and can identify the signs of a potential cyberattack.

Let's understand these steps in detail.

Step1: If RDP service is not required on the system, disable it as a security best practice

Check the open ports on your windows machine. if port no 3389 is found open, disable it. This port is used for running RDP (Remote desktop service). you can check it using the netstat command (run on command prompt), as follows.

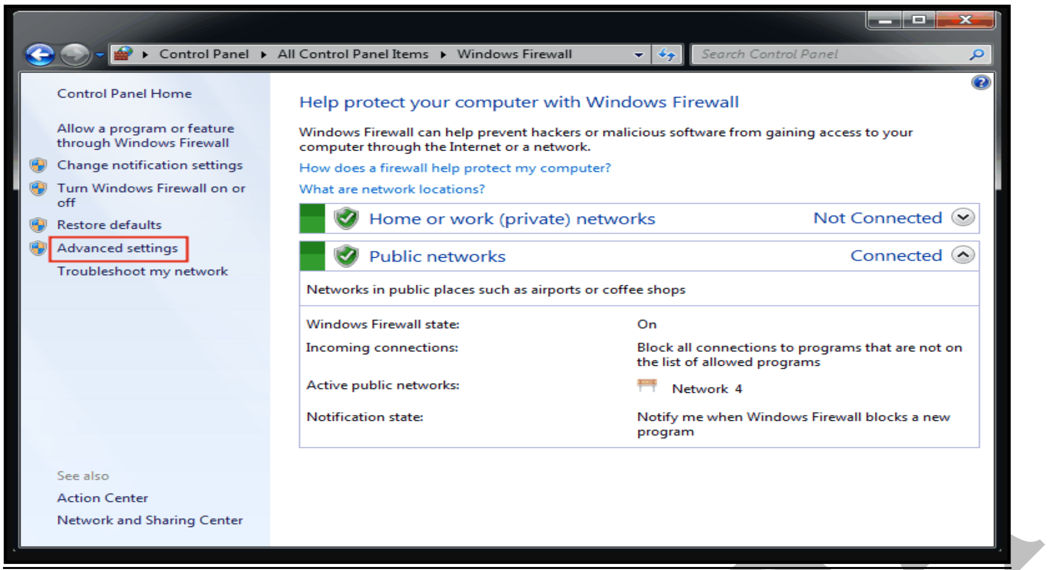


```
C:\Users\cdac>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7070           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8089           0.0.0.0:0              LISTENING
```

Disabling unused and unneeded services helps reduce exposure to security vulnerabilities.

Blocking port, No 3389 in Windows Firewall:

a. Go to Start > Control Panel > Windows Firewall and find Advanced settings on the left side.



Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

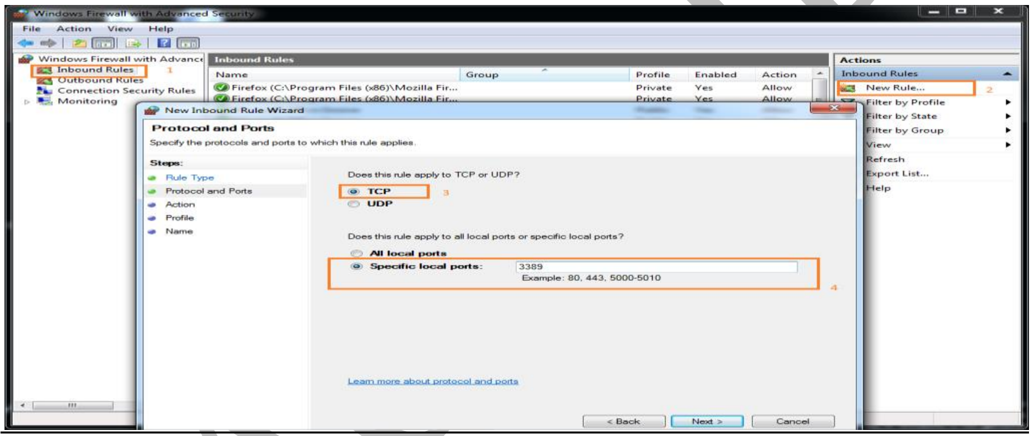
Home or work (private) networks — Not Connected

Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	Network 4
Notification state:	Notify me when Windows Firewall blocks a new program

b. Click on Inbound Rules > New rule. Then in the pop-up window, choose Port > Next >TCP > Specific local ports and type 3389 and go to Next



Inbound Rules

Name	Group	Profile	Enabled	Action
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Allow
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Allow

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

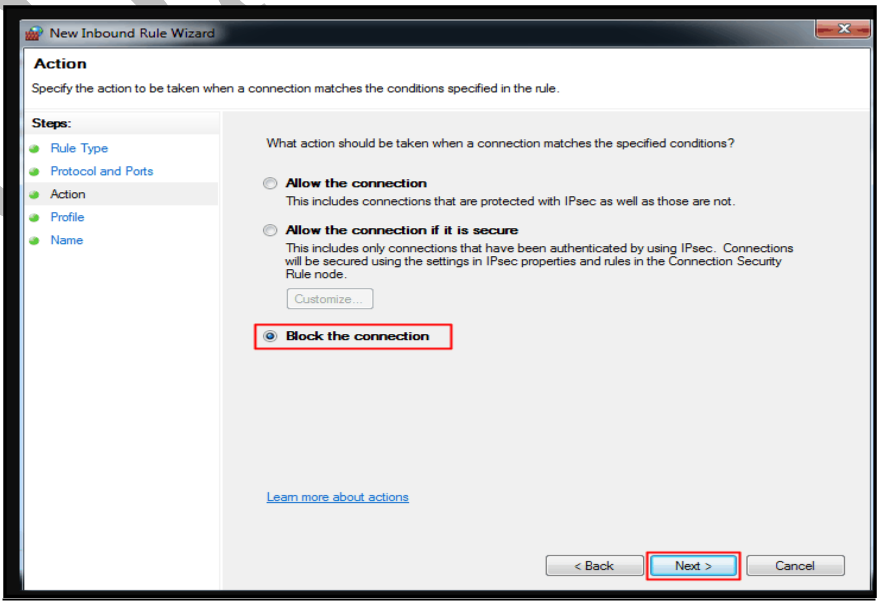
Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 3389
Example: 80, 443, 5000-5010

c. Choose Block the connection > Next. Tick the three checkboxes and click Next. Specify the name and description and click Finish.



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

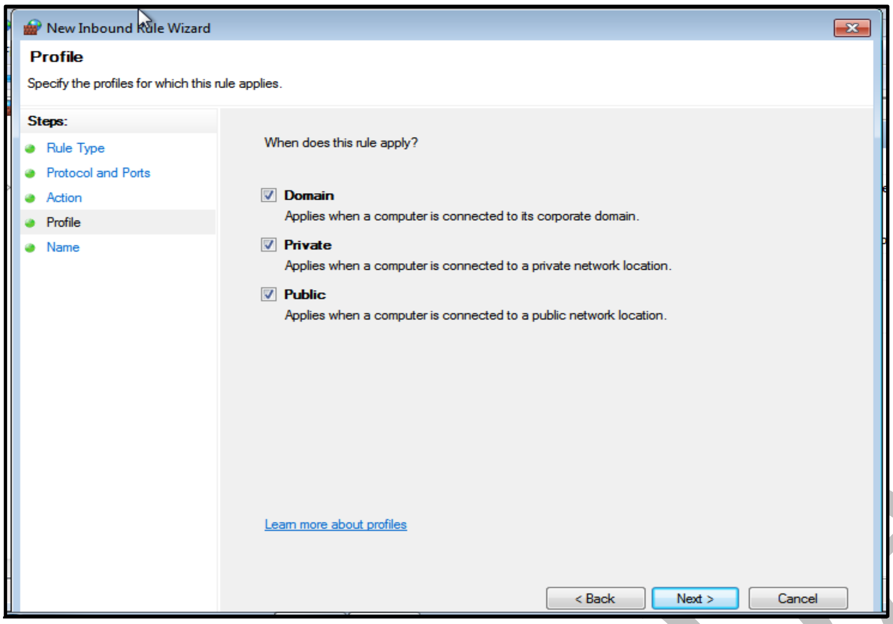
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

○ Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● Block the connection


New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

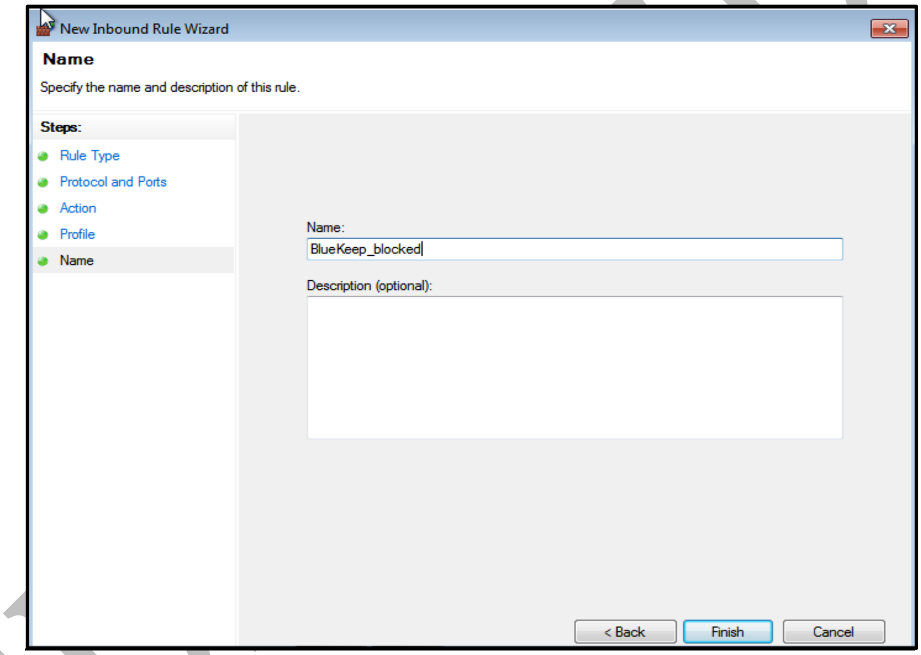
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.


New Inbound Rule Wizard

Name

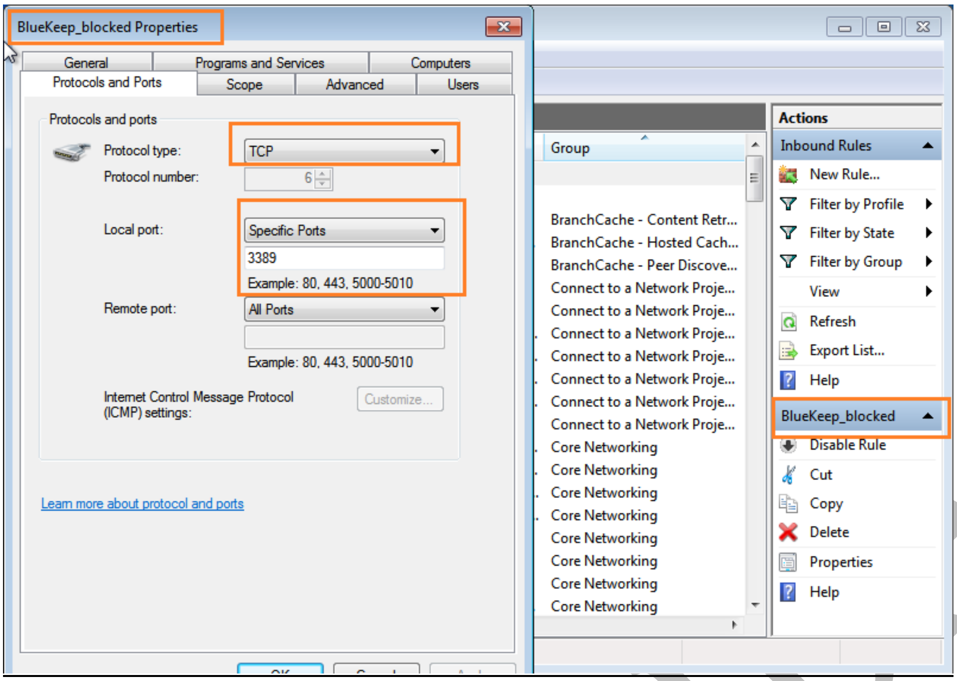
Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:
BlueKeep_blocked

Description (optional):

d. Check if rule is created by Properties > Protocols and Ports > Local Port.



BlueKeep_blocked Properties

Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: Specific Ports

3389

Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

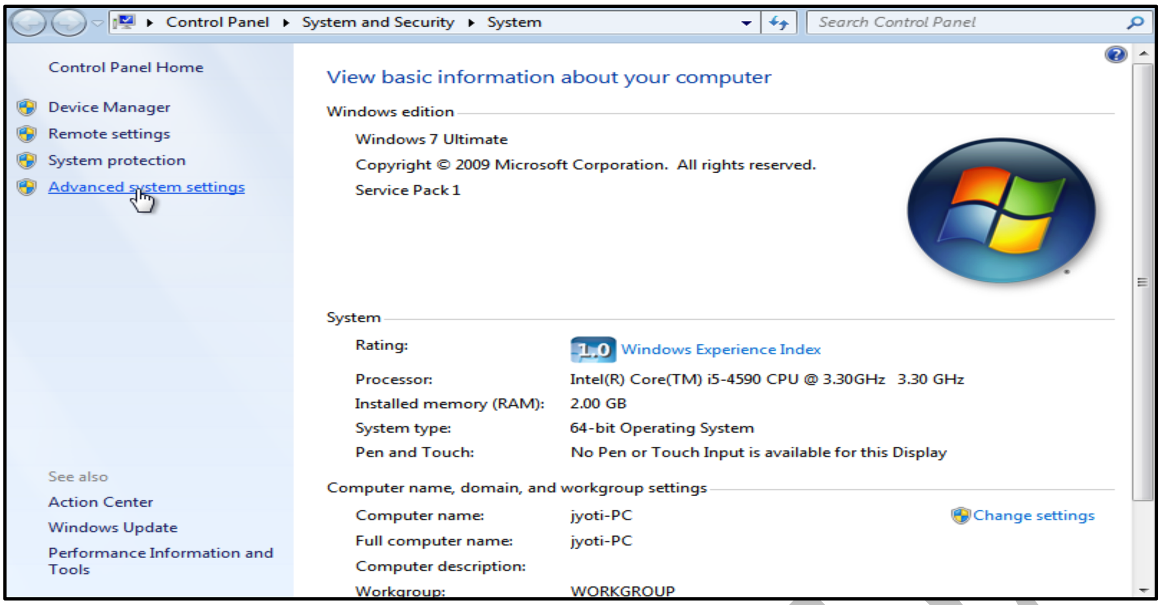
Internet Control Message Protocol (ICMP) settings: Customize...

Learn more about protocol and ports

Note: RDP service (Port no 3389) must be disabled, only if you do not need it. If you close port 3389, you will not be able to get access to a remote desktop, either on the same network or another network. The best solution for this problem is enabling Network Level Authentication and installing security updates for RDP as mentioned below.

Step2: Next step to prevent the Blue keep RDP attack is to configure Network Level Authentication on the machine which offers extra authentication measure and enhance security so the attacker doesn't log in easily. To enable Network Level Authentication, perform the following steps.

a. Go to properties>Advanced system setting



View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

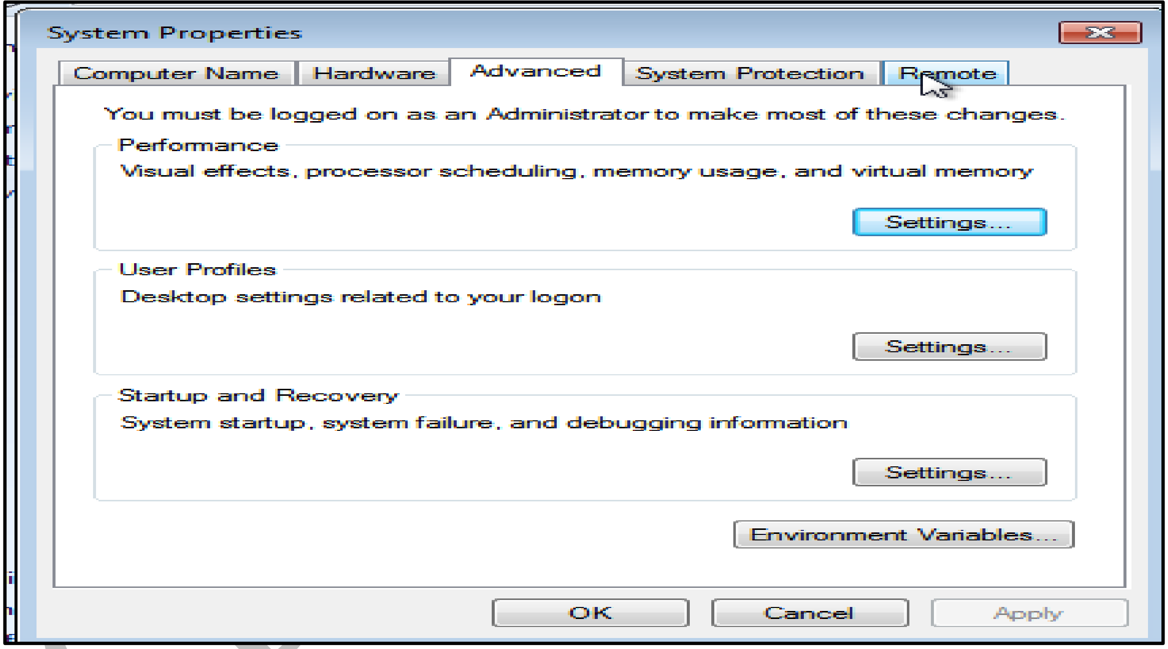
System

Rating:	1.0 Windows Experience Index
Processor:	Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 3.30 GHz
Installed memory (RAM):	2.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	jyoti-PC
Full computer name:	jyoti-PC
Computer description:	
Workgroup:	WORKGROUP

b. On the Remote tab in the System Properties dialog box on an RD Session Host server.



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

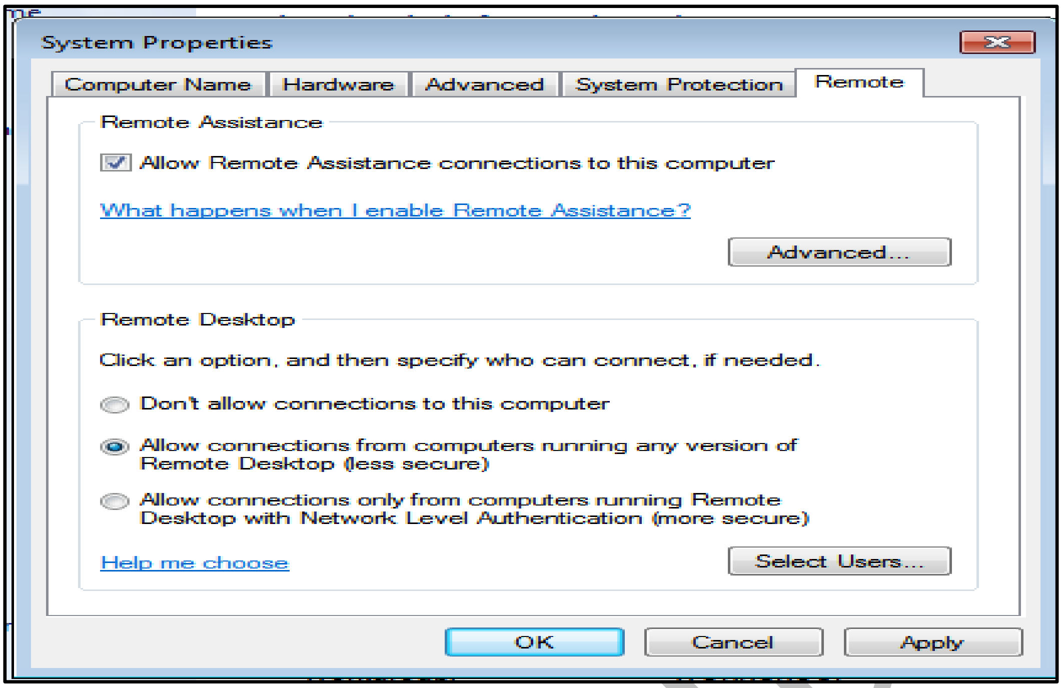
User Profiles

Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information

- Choose the option **Allow the connection only from computers running Remote Desktop with Network Level Authentication (more secure).**



Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

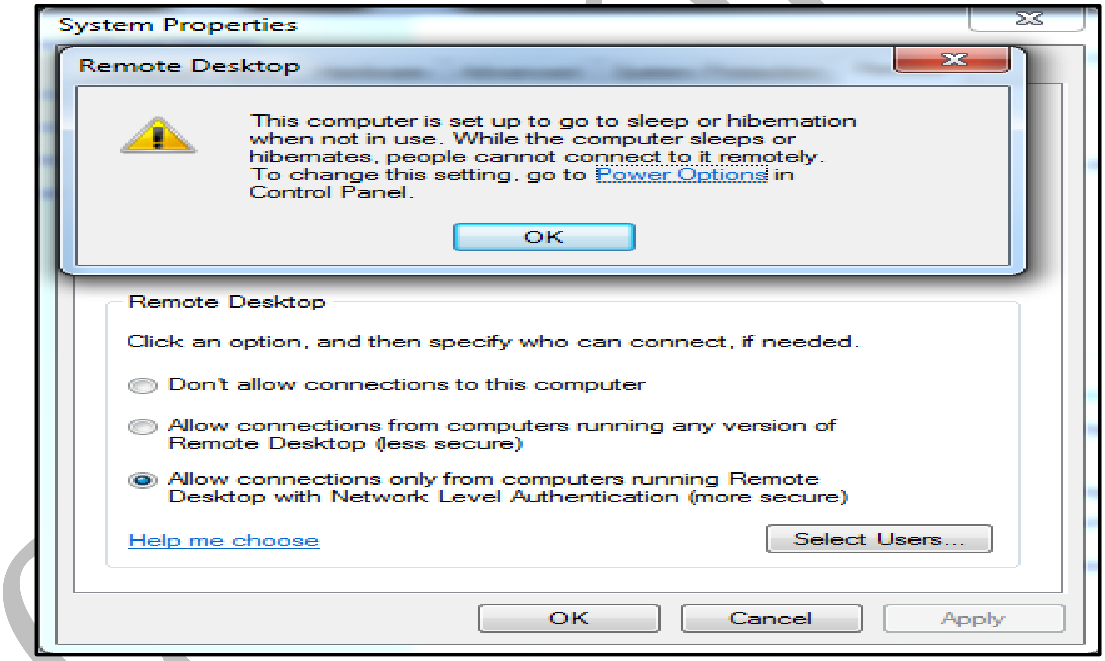
Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

● Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose



This computer is set up to go to sleep or hibernation when not in use. While the computer sleeps or hibernates, people cannot connect to it remotely. To change this setting, go to Power Options in Control Panel.

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

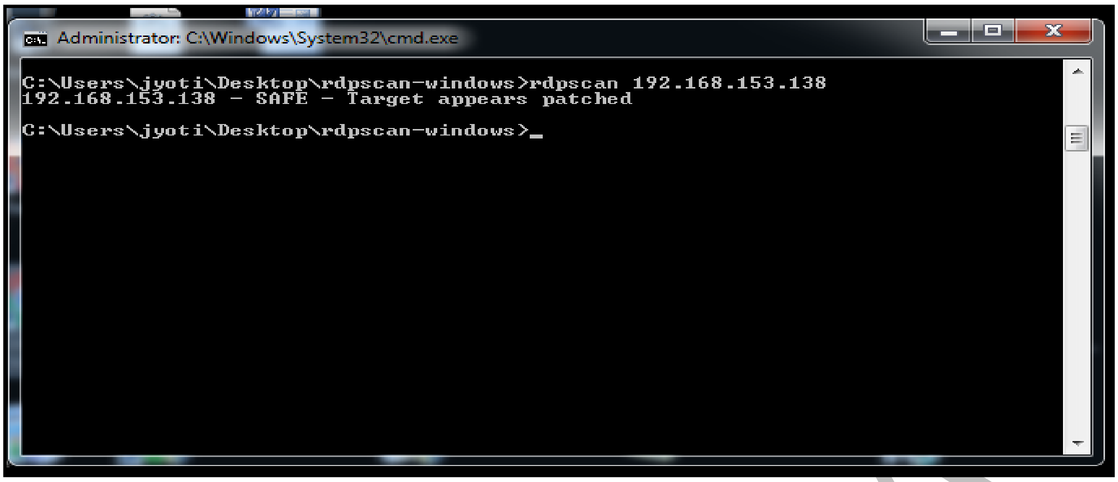
○ Allow connections from computers running any version of Remote Desktop (less secure)

● Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

After scanning for the vulnerability, the output may be Safe**, Vulnerable, or Unknown.**

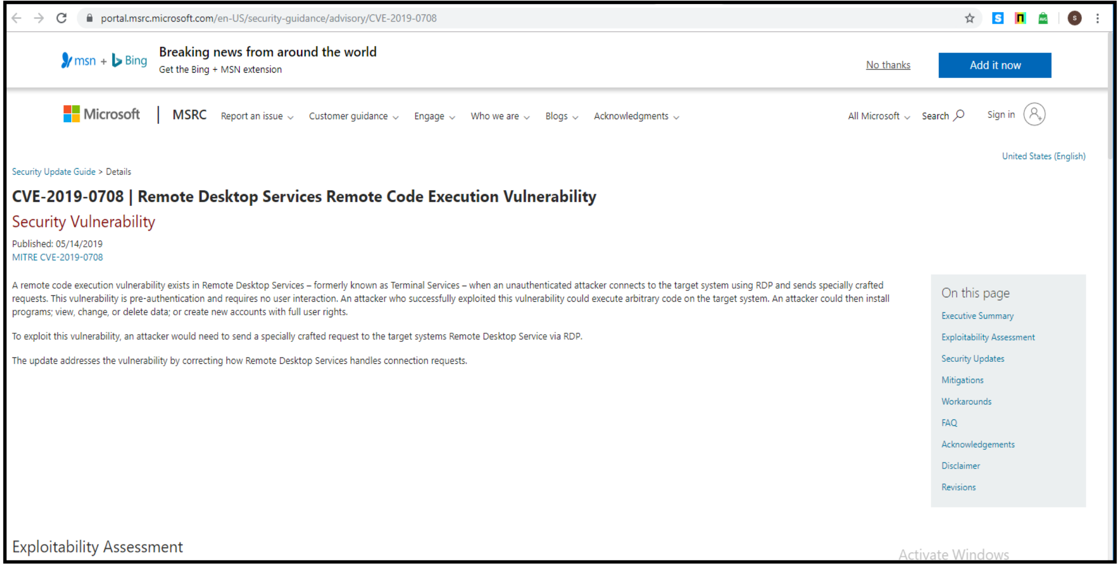
Here in this case, it reflects the status as **safe.**



```
C:\Users\jyoti\Desktop\rdpscan-windows>rdpscan 192.168.153.138
192.168.153.138 - SAFE - Target appears patched

C:\Users\jyoti\Desktop\rdpscan-windows>_
```

Step 3: **CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability security update**

a. Go to https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708where the links are available for the security update packages.



portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
msn + Bing
Breaking news from around the world
Get the Bing + MSN extension
No thanks
Add it now
Microsoft
MSRC
Report an issue
Customer guidance
Engage
Who we are
Blogs
Acknowledgments
All Microsoft
Search
Sign in
United States (English)
Security Update Guide > Details

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

Security Vulnerability

Published: 05/14/2019

MITRE CVE-2019-0708

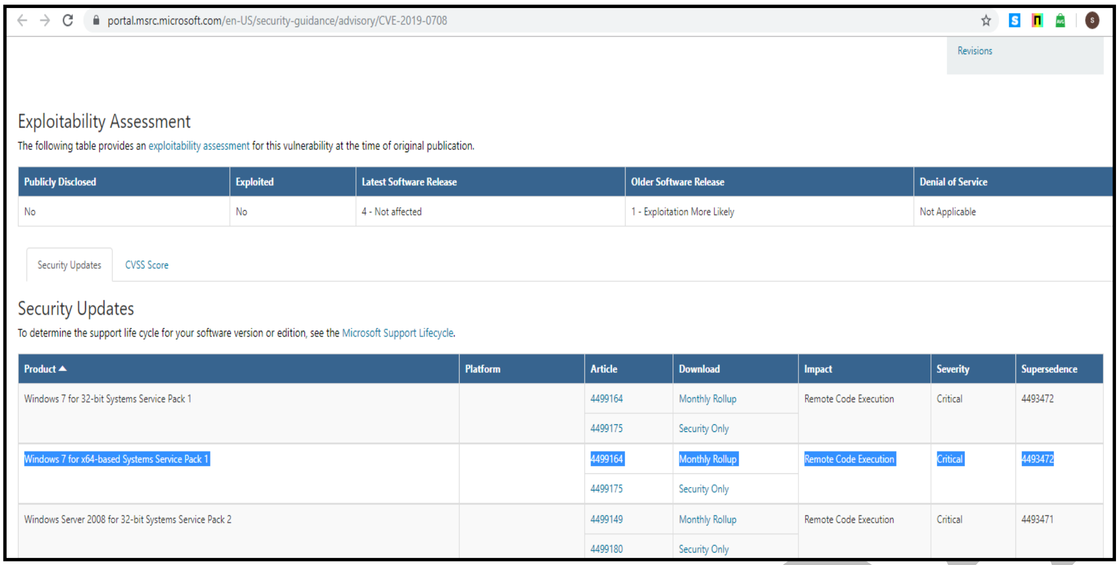
A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

Exploitability Assessment

b. Scroll down to the operating system that is in use. In this example, it was Windows 7 64bits.



portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
Revisions

Exploitability Assessment

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	4 - Not affected	1 - Exploitation More Likely	Not Applicable

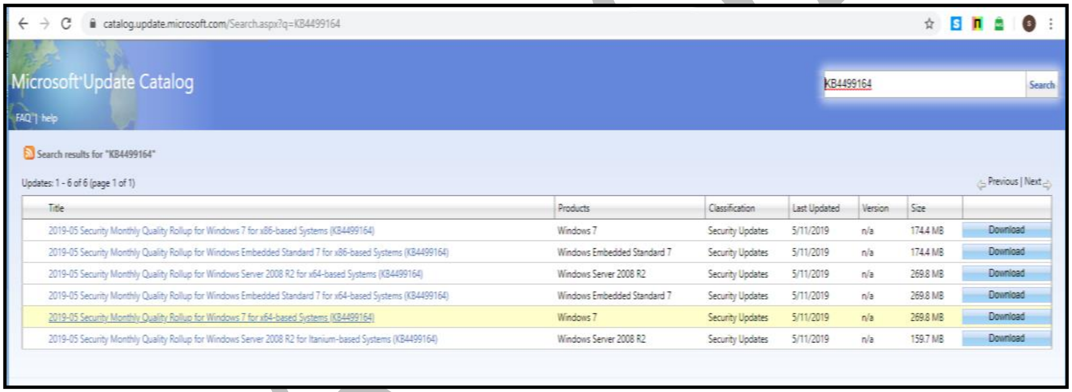
Security Updates
CVSS Score

Security Updates

To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.

Product ▲	Platform	Article	Download	Impact	Severity	Supersedence
Windows 7 for 32-bit Systems Service Pack 1		4499164	Monthly Rollup	Remote Code Execution	Critical	4493472
		4499175	Security Only			
Windows 7 for x64-based Systems Service Pack 1		4499164	Monthly Rollup	Remote Code Execution	Critical	4493472
		4499175	Security Only			
Windows Server 2008 for 32-bit Systems Service Pack 2		4499149	Monthly Rollup	Remote Code Execution	Critical	4493471
		4499180	Security Only			

c. Click on the desired package. In this example, the package used is Windows 7 for x64-based Systems Service Pack 1 (KB4499164) Monthly Rollup. Make sure it’s the Monthly Rollup link that is chosen!

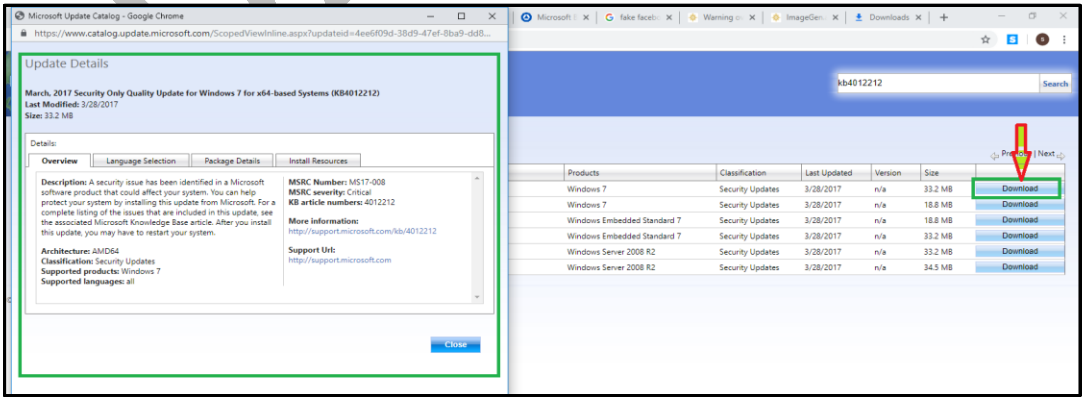


Search results for "KB4499164"

Updates: 1 - 6 of 6 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	
2019-05 Security Monthly Quality Rollup for Windows 7 for x86-based Systems (KB4499164)	Windows 7	Security Updates	5/11/2019	n/a	174.4 MB	Download
2019-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB4499164)	Windows Embedded Standard 7	Security Updates	5/11/2019	n/a	174.4 MB	Download
2019-05 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4499164)	Windows Server 2008 R2	Security Updates	5/11/2019	n/a	269.8 MB	Download
2019-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems (KB4499164)	Windows Embedded Standard 7	Security Updates	5/11/2019	n/a	269.8 MB	Download
2019-05 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4499164)	Windows 7	Security Updates	5/11/2019	n/a	269.8 MB	Download
2019-05 Security Monthly Quality Rollup for Windows Server 2008 R2 for Itanium-based Systems (KB4499164)	Windows Server 2008 R2	Security Updates	5/11/2019	n/a	159.7 MB	Download

d. A new window will open. Select the update for the windows version that window 7 have and press Download.



Microsoft Update Catalog - Google Chrome
https://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=4ee6f09d-38d9-47ef-8ba9-dd8...
Microsoft
fake facebo
Warning o
ImageGen
Downloads
kb4012212
Search
Previous | Next
Overview
Language Selection
Package Details
Install Resources
Close

Update Details

March, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4012212)
Last Modified: 3/28/2017
Size: 33.2 MB

Details:

Description: A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.

Architecture: AMD64
Classification: Security Updates
Supported products: Windows 7
Supported languages: all

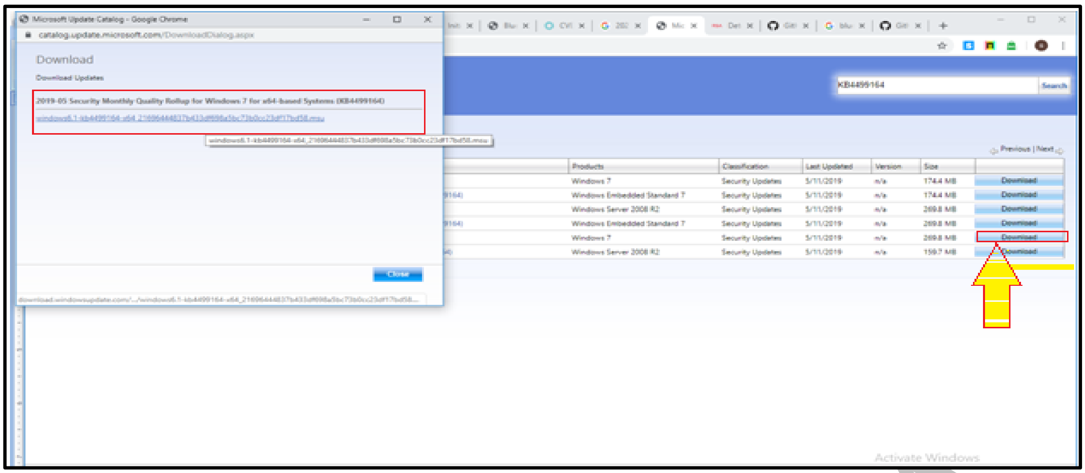
MSRC Number: MS17-008
MSRC severity: Critical
KB article numbers: 4012212

More information:
http://support.microsoft.com/kb/4012212

Support Url:
http://support.microsoft.com

Products	Classification	Last Updated	Version	Size	
Windows 7	Security Updates	3/28/2017	n/a	33.2 MB	Download
Windows 7	Security Updates	3/28/2017	n/a	18.8 MB	Download
Windows Embedded Standard 7	Security Updates	3/28/2017	n/a	18.8 MB	Download
Windows Embedded Standard 7	Security Updates	3/28/2017	n/a	33.2 MB	Download
Windows Server 2008 R2	Security Updates	3/28/2017	n/a	33.2 MB	Download
Windows Server 2008 R2	Security Updates	3/28/2017	n/a	34.5 MB	Download

e. Click on the link that will appear after pressing the Download button:



Microsoft Update Catalog - Google Chrome

catalog.update.microsoft.com/DownloadDialog.aspx

Download

Download Updates

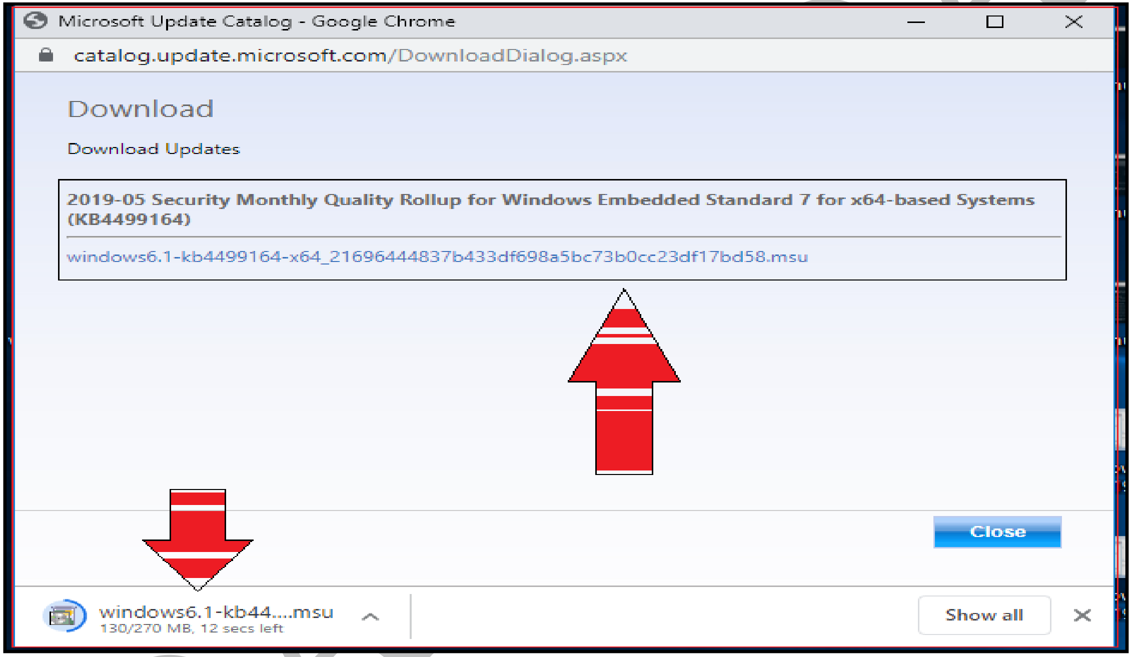
2019-05 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4499164)

windows6.1-kb4499164-x64_21696444837b433df698a5bc73b0cc23df17bd58.msu

KB4499164

Products	Classification	Last Updated	Version	Size	
Windows 7	Security Updates	5/11/2019	n/a	174.4 MB	Download
Windows Embedded Standard 7	Security Updates	5/11/2019	n/a	174.4 MB	Download
Windows Server 2008 R2	Security Updates	5/11/2019	n/a	269.8 MB	Download
Windows Embedded Standard 7	Security Updates	5/11/2019	n/a	269.8 MB	Download
Windows 7	Security Updates	5/11/2019	n/a	269.8 MB	Download
Windows Server 2008 R2	Security Updates	5/11/2019	n/a	159.7 MB	Download

f. After the download is complete, run it as would run any other setup.



Microsoft Update Catalog - Google Chrome

catalog.update.microsoft.com/DownloadDialog.aspx

Download

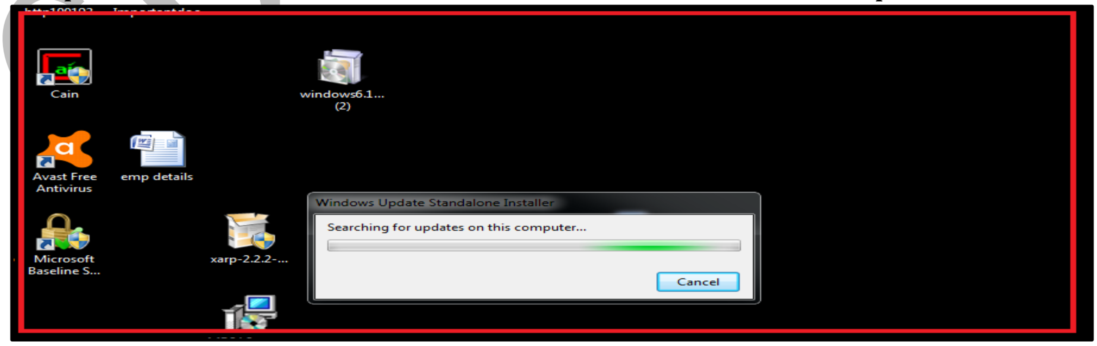
Download Updates

2019-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems (KB4499164)

windows6.1-kb4499164-x64_21696444837b433df698a5bc73b0cc23df17bd58.msu

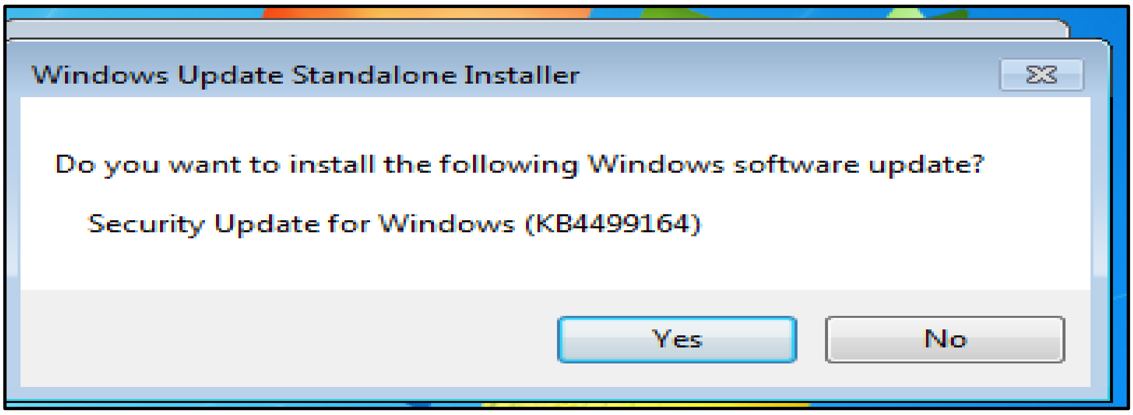
windows6.1-kb44....msu
130/270 MB, 12 secs left

g. Windows appears "Do you want to install the following Windows software update". Press Yes and this will initialize the installation setup:



Windows Update Standalone Installer

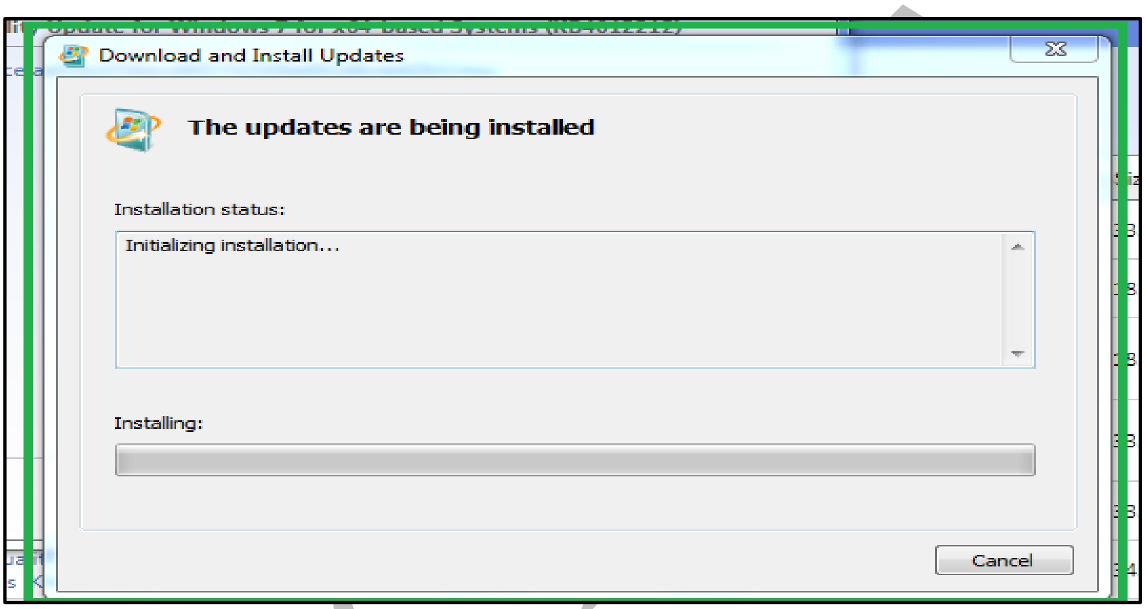
Searching for updates on this computer...



Windows Update Standalone Installer

Do you want to install the following Windows software update?

Security Update for Windows (KB4499164)



Download and Install Updates

The updates are being installed

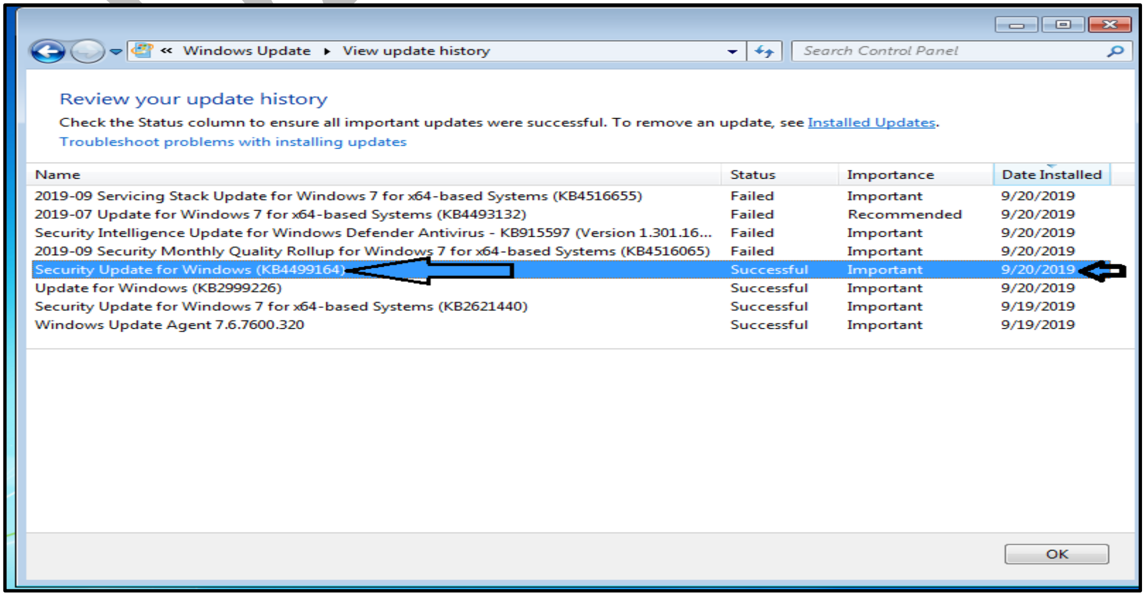
Installation status:

Initializing installation...

Installing:

h. At the end of the installation, it will ask to restart the computer, so restart it.

i. After rebooting, to check if the installation was successful, just go to Control Panel > Windows Updates > View update History (on the left side) and see if the Security Update for Windows is installed. It should have the current date in the Date Installed column.



Review your update history

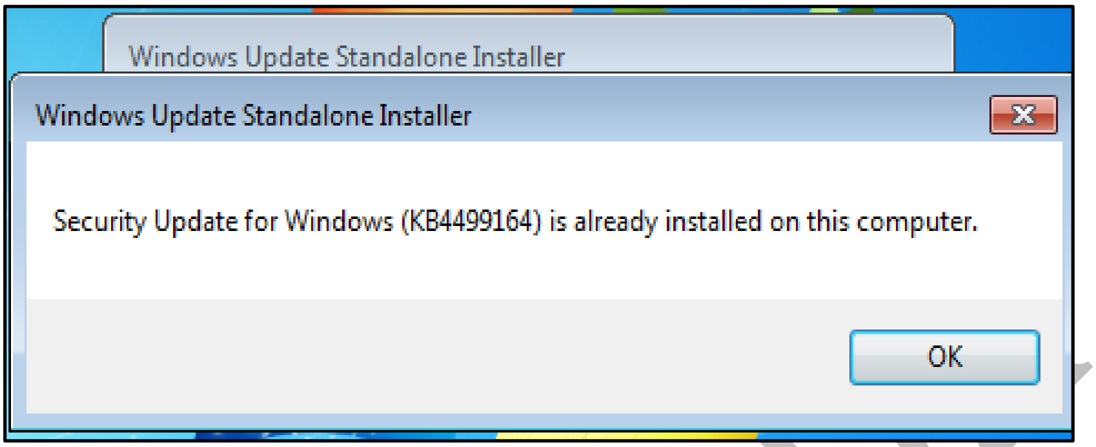
Check the Status column to ensure all important updates were successful. To remove an update, see Installed Updates.

Troubleshoot problems with installing updates

Name	Status	Importance	Date Installed
2019-09 Servicing Stack Update for Windows 7 for x64-based Systems (KB4516655)	Failed	Important	9/20/2019
2019-07 Update for Windows 7 for x64-based Systems (KB4493132)	Failed	Recommended	9/20/2019
Security Intelligence Update for Windows Defender Antivirus - KB915597 (Version 1.301.16...	Failed	Important	9/20/2019
2019-09 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516065)	Failed	Important	9/20/2019
Security Update for Windows (KB4499164)	Successful	Important	9/20/2019
Update for Windows (KB2999226)	Successful	Important	9/20/2019
Security Update for Windows 7 for x64-based Systems (KB2621440)	Successful	Important	9/19/2019
Windows Update Agent 7.6.7600.320	Successful	Important	9/19/2019

IMPORTANT!

If the update has been already applied or installed, then windows appear on the screen informing about it.



Windows Update Standalone Installer

Security Update for Windows (KB4499164) is already installed on this computer.

Note: To check the hardening of your machine for Blue Keep-based attacks, again perform the attack on your machine and check for the Indicators of the Attack. if an attack happens, re-read the manual again and take the steps for hardening the machine against this attack.