Protection against SMB protocol-based attacks on Windows machines

This exercise is based on SMB-based attacks on Windows machines. The EternalBlue exploit officially named MS17-010 by Microsoft affects only Windows operating systems, anything that uses the SMBv1 (Server Message Block version 1) is especially valuable to attacks, as a maliciously crafted packet allows for remote code execution. Any infected device joining the network can spread the infection to vulnerable devices on the same network.

Affected machines with this vulnerability:

Server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016

In this exercise, you will learn about the SMBv1-based vulnerability, and its exploitation resulting in remote code execution and using Eternal Scanner to assist in automating the process of scanning for more vulnerable devices in a network. Additionally, this exercise will explain how an attacker gets memory/admin privileges of the target machine and what he can perform on the target machine remotely, 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:

CDAC NOIDA

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 SMBv1-based vulnerability

Use vulnerability scanners for determining the vulnerability of the host to CVE ms17_010.

```
       =[ metasploit v4.16.48-dev                         ]
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.52.144
RHOSTS => 192.168.52.144
msf auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.52.144:445    - Host is likely VULNERABLE to MS17-010! - Windows 7
ltimate 7601 Service Pack 1 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) >
```

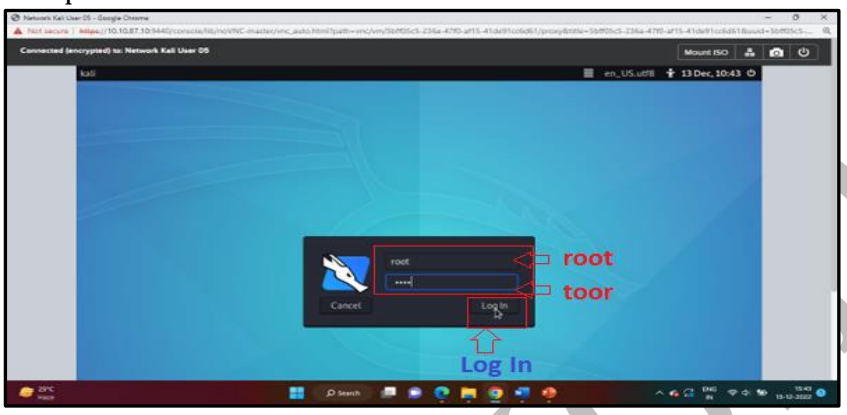
DAC NOIDA

Detection of SMB-based attack (Indicators of Attack):

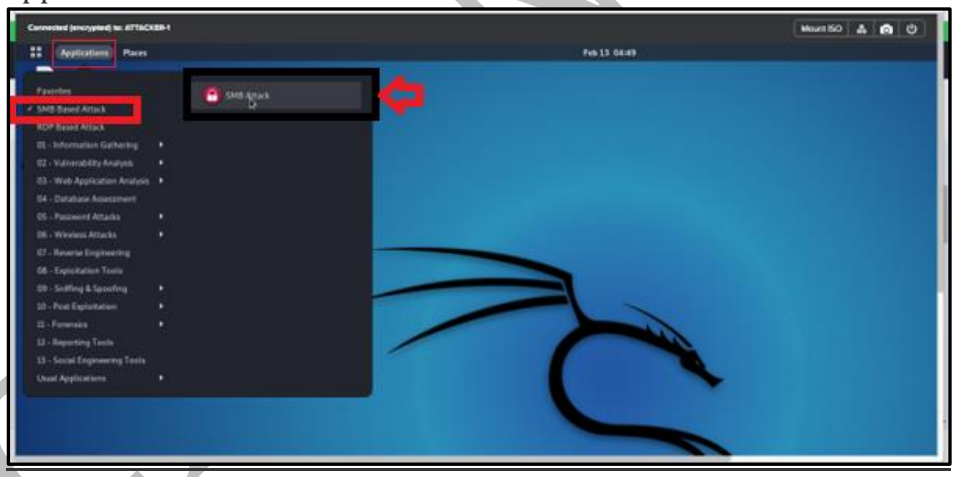
A. Performing an Attack on the Windows machine in your user account

To detect the IoA on your machine for an SMBv1 based attack, you have to first attack the machine through the following steps.

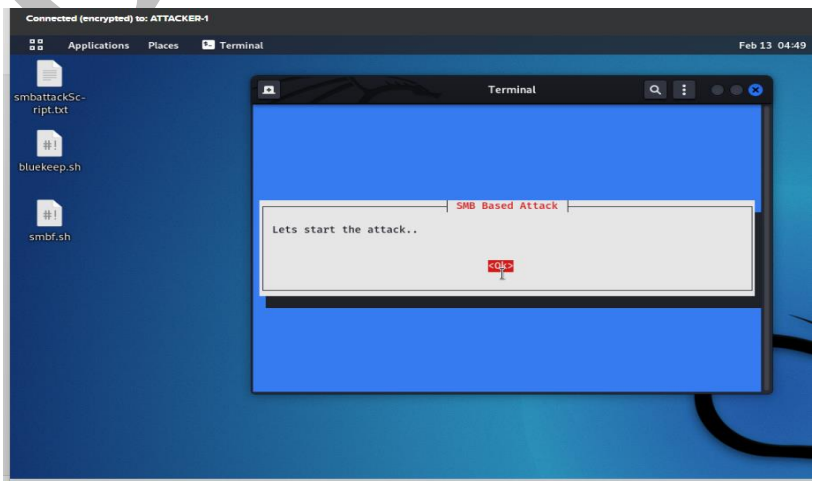
1. Connect to the kali Linux machine, created by you, using the RDP protocol. Kali Linux machine is being used as Attacker's machine.
2. When prompted for the username and password, enter cdac as username and cdac as password. The root is the administrator user of the machine.



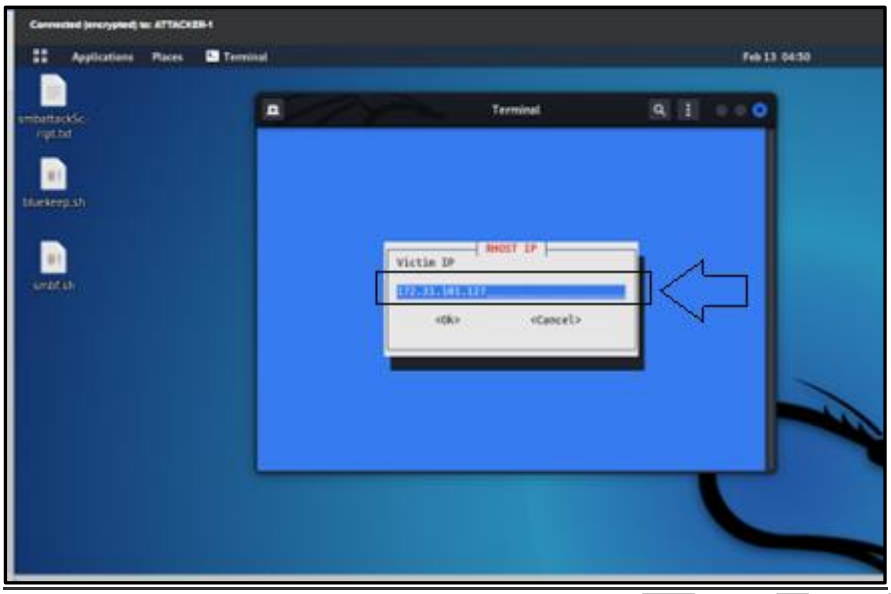
3. First, click on the application tab. The next step is to browse the category you want to explore here click on the category "SMB Based Attack". After that, click on the application "SMB Attack" to start.



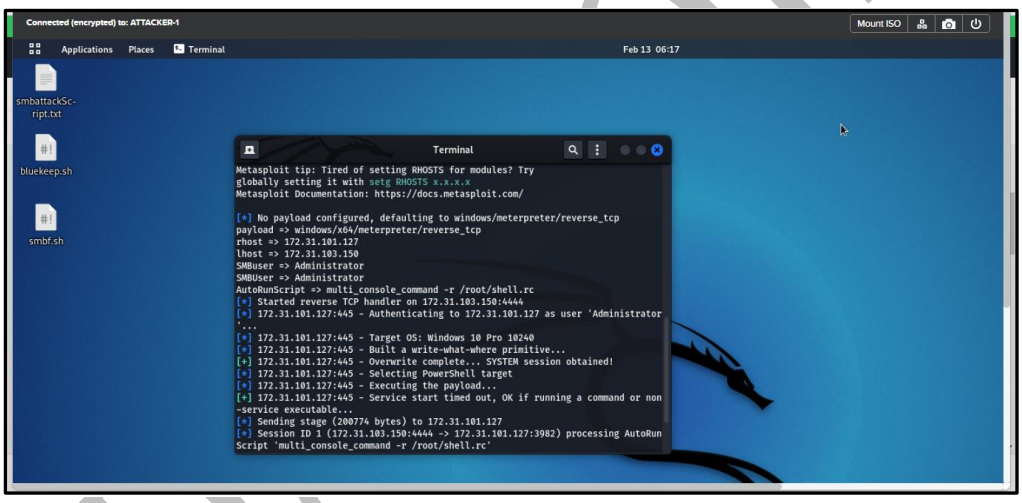
4. Click ok to start the attack.



Enter the Victim IP (Network Windows 10 IP).



You can see that your exploit was executed successfully.



B. Detection of SMB-based attack

Method 1: Detection using Wireshark.

1. **Download and install Wireshark on your machine.**
   Download link:https://www.wireshark.org/download.html

Perform the following steps after starting Wireshark:

1. Set the display filter to SMB. The following packets may be seen in the data stream.
   a. Negotiate Protocol Request and Negotiate Protocol Response
   b. NT Trans request.
   c. Trans2 Requests (in a large number)
   d. Trans2 Responses

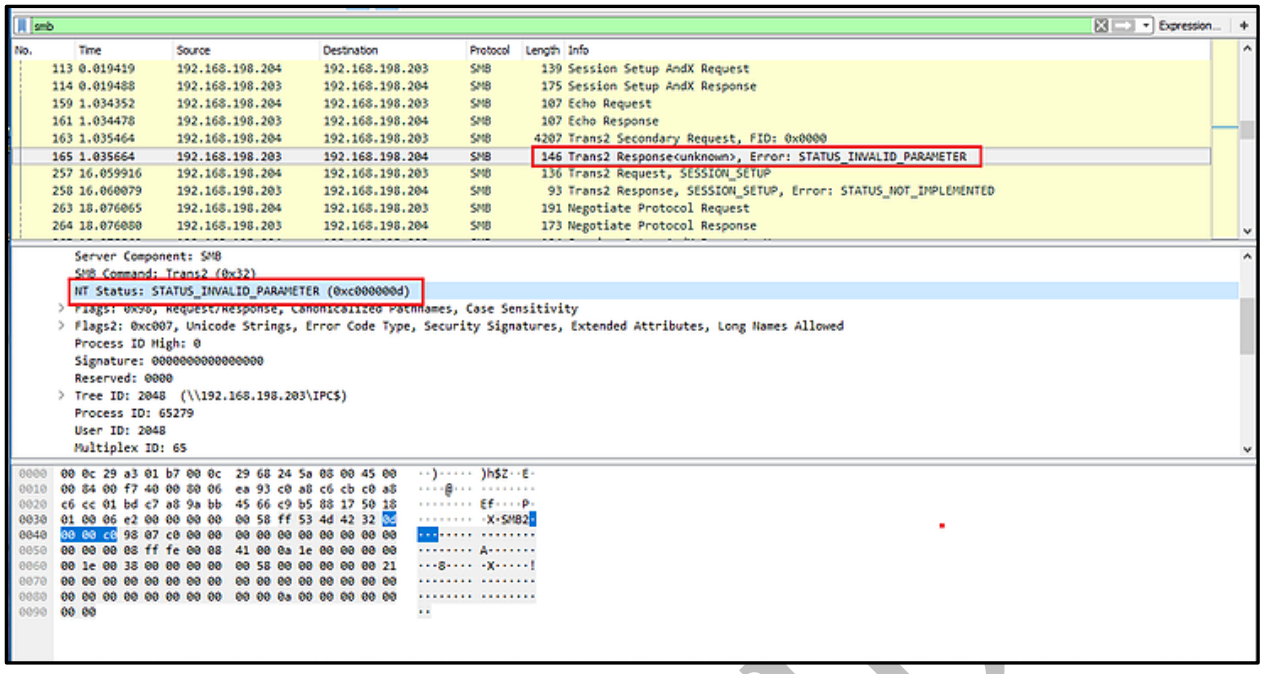
These packets are used by the Exploit to setup SMB session and download malware on the machine.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.198.204	192.168.198.203	TCP	66	51112 → microsoft-ds(445) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000275	Vmware_68:24:5a	Broadcast	ARP	60	Who has 192.168.198.204? Tell 192.168.198.203
3	0.000417	Vmware_a3:01:b7	Vmware_68:24:5a	ARP	60	192.168.198.204 is at 00:0c:29:a3:01:b7
4	0.000452	192.168.198.203	192.168.198.204	TCP	66	microsoft-ds(445) → 51112 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.000580	192.168.198.204	192.168.198.203	TCP	60	51112 → microsoft-ds(445) [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.000617	192.168.198.204	192.168.198.203	SMB	191	Negotiate Protocol Request
7	0.002461	192.168.198.203	192.168.198.204	SMB	173	Negotiate Protocol Response
8	0.002463	192.168.198.204	192.168.198.203	SMB	194	Session Setup AndX Request, User: anonymous
9	0.002639	192.168.198.203	192.168.198.204	SMB	251	Session Setup AndX Response
10	0.002651	192.168.198.204	192.168.198.203	SMB	154	Tree Connect AndX Request, Path: \\192.168.198.203\IPC$
11	0.002652	192.168.198.203	192.168.198.204	SMB	114	Tree Connect AndX Response
12	0.002653	192.168.198.204	192.168.198.203	SMB	136	Trans2 Request, SESSION_SETUP
13	0.002654	192.168.198.203	192.168.198.204	SMB	93	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
14	0.004962	192.168.198.204	192.168.198.203	SMB	1138	NT Trans Request, <unknown>
15	0.005044	192.168.198.203	192.168.198.204	SMB	93	NT Trans Response, <unknown (0)>
16	0.005204	192.168.198.204	192.168.198.203	SMB	4207	Trans2 Secondary Request, FID: 0x0000
17	0.005339	192.168.198.203	192.168.198.204	TCP	60	microsoft-ds(445) → 51112 [ACK] Seq=455 Ack=5697 Win=65536 Len=0
18	0.005346	192.168.198.203	192.168.198.204	TCP	60	[TCP ACKed unseen segment] microsoft-ds(445) → 51112 [ACK] Seq=455 Ack=8617 Win=65536 Len=0

```
> Frame 10: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
> Ethernet II, Src: Vmware_a3:01:b7 (00:0c:29:a3:01:b7), Dst: Vmware_68:24:5a (00:0c:29:68:24:5a)
> Internet Protocol Version 4, Src: 192.168.198.204 (192.168.198.204), Dst: 192.168.198.203 (192.168.198.203)
> Transmission Control Protocol, Src Port: 51112 (51112), Dst Port: microsoft-ds (445), Seq: 278, Ack: 317, Len: 100
> NetBIOS Session Service
v SMB (Server Message Block Protocol)
  > SMB Header
  > Tree Connect AndX Request (0x75)

0000  00 0c 29 68 24 5a 00 0c  29 a3 01 b7 08 00 45 00   ··)h$Z·· )·····E·
0010  00 8c 12 00 00 00 80 06  19 83 c0 a8 c6 cc c0 a8   ........ ........
0020  c6 cb c7 a8 01 bd c9 b4  7f 2b 9a bb 44 72 50 18   ........ ·+··DrP·
0030  00 ff d1 15 00 00 00 00  00 60 ff 53 4d 42 75 00   ........ ·`·SMBu·
0040  00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 ff fe 00 08  40 00 04 ff 00 60 00 08   ........ @·····`·
0060  00 01 00 35 00 00 5c 00  5c 00 31 00 39 00 32 00   ···5··\· \·1·9·2·
0070  2e 00 31 00 36 00 38 00  2e 00 31 00 39 00 38 00   .·1·6·8· .·1·9·8·
0080  2e 00 32 00 30 00 33 00  5c 00 49 00 50 00 43 00   .·2·0·3· \·I·P·C·
0090  24 00 00 00 3f 3f 3f 3f  3f 00                      $···???? ?·
```

```
smb                                                                  Expression...

No.  Time      Source          Destination     Protocol Length Info
  7  0.002461  192.168.198.203  192.168.198.204  SMB      173  Negotiate Protocol Response
  8  0.002463  192.168.198.204  192.168.198.203  SMB      194  Session Setup AndX Request, User: anonymous
  9  0.002639  192.168.198.203  192.168.198.204  SMB      251  Session Setup AndX Response
 10  0.002651  192.168.198.204  192.168.198.203  SMB      154  Tree Connect AndX Request, Path: \\192.168.198.203\IPC$
 11  0.002652  192.168.198.203  192.168.198.204  SMB      114  Tree Connect AndX Response
 12  0.002653  192.168.198.204  192.168.198.203  SMB      136  Trans2 Request, SESSION_SETUP
 13  0.002654  192.168.198.203  192.168.198.204  SMB       93  Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
 14  0.004962  192.168.198.204  192.168.198.203  SMB     1138  NT Trans Request, <unknown>
 15  0.005044  192.168.198.203  192.168.198.204  SMB       93  NT Trans Response, <unknown (0)>
 16  0.005204  192.168.198.204  192.168.198.203  SMB     4207  Trans2 Secondary Request, FID: 0x0000

    Process ID High: 0
    Signature: 0000000000000000
    Reserved: 0000
  > Tree ID: 2048  (\\192.168.198.203\IPC$)
    Process ID: 65279
    User ID: 2048
    Multiplex ID: 65
  v NT Trans Request (0xa0)
    Word Count (WCT): 28
    Max Setup Count: 1
    Reserved: 0000
    Total Parameter Count: 30

0050  00 00 00 08 ff fe 00 08  41 00 14 01 00 00 1e 00   ........ A·......
0060  00 00 d0 03 01 00 1e 00  00 00 00 00 00 00 1e 00   ........ ........
0070  00 00 4b 00 00 00 d0 03  00 00 68 00 00 00 01 00   ··K····· ··h·····
0080  00 00 00 cc 03 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 01 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

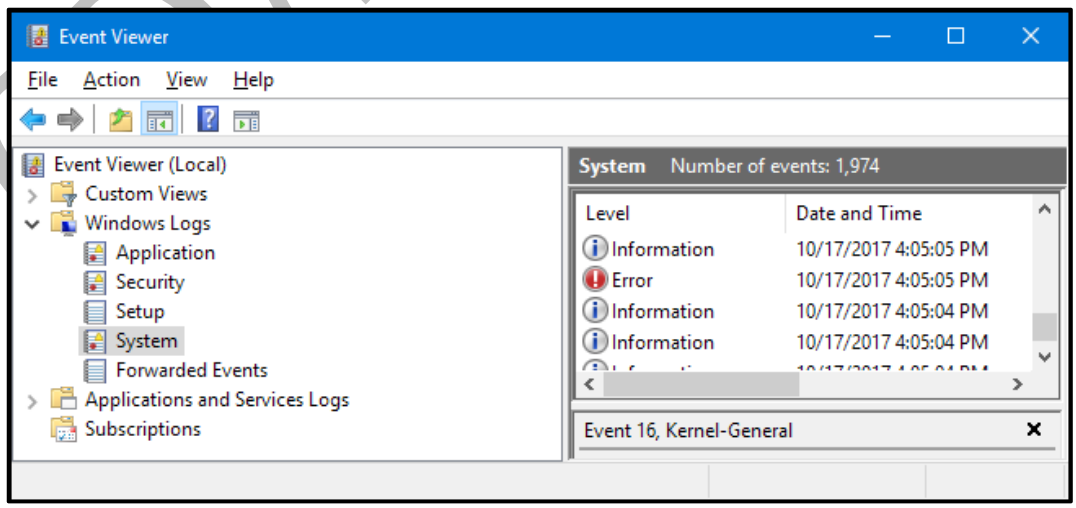
NT Trans Request Header



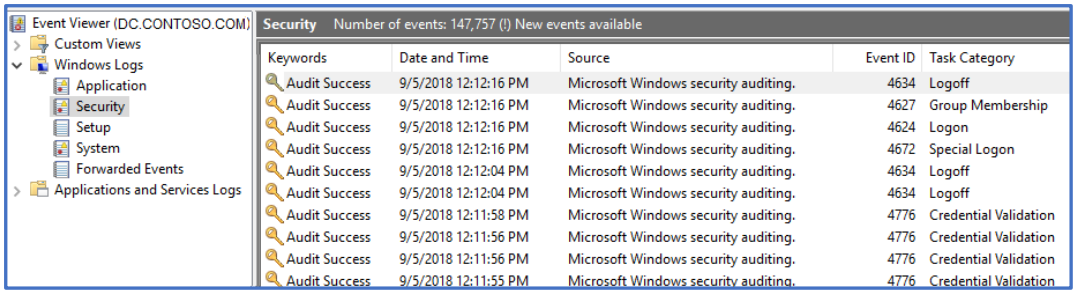
This method only works if traffic is monitored continuously.

Method2: Detection using Windows Event Log Viewer

- The Windows Event Viewer app collects, manages and shows log related to application and system messages.
- It also shows errors, information messages, and warnings.
- It's a useful tool for troubleshooting all kinds of different Windows problems.
- In case of SMB attack, the attacker gets a remote session on the victim machine and tries to access the important files, creates new admin accounts, delete the created accounts etc.
- These events can easily be detected using Windows Event Log viewer.



Selecting Security option to view the logs



Few possibly dangerous events to monitor in Event Viewer

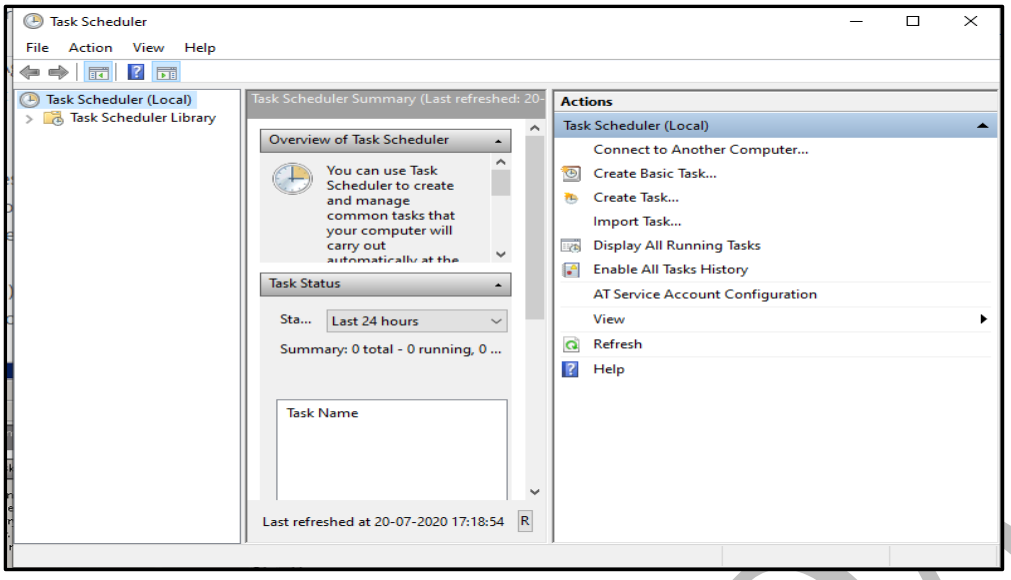
- EVENT 4663 – This one is generated when you have a high number of files being deleted. Chances are it's innocent. It can also be someone who is dumping crucial information and wants to make life difficult for you and/or the company.
- EVENT 4724 – Password reset. Again, probably innocent enough. But then it depends on the account having the password reset. Resetting service account passwords is a nice way for an upset sysadmin to spread havoc through the infrastructure.
- EVENT 4704 & 4717 – Changes to user rights assignments.

  If someone is planning something sneaky, there's a really good chance they won't follow protocol to do it. An event like this will often tell you what rights were assigned to a user or account, but it probably won't tell you who did it. This is one to watch for because a hacker on the inside might try to elevate a service account or an ordinary user account with permissions that will give them access to the system and help them cover their tracks doing it.
- EVENT 4719 & 4739 – If you see these, start thinking someone has altered the Audit and Account policies in the system. Often a good prelude to an internal hack.
- EVENT 1102 – This is often a worth monitoring event. This means that someone has just cleared the security log. Again, this can be innocent, but it can also mean someone is trying to cover his tracks. This is a good hint that could easily mean that an attack on the network is coming, or it's already winding down.
- EVENT 4720 -When a user account is created in Active Directory, event ID 4720 is logged.
- EVENT 4663: An attempt was made to access an object. Finding who opened a file in the Windows audit is straightforward. Simply look for event ID 4663.
- EVENT 4616 -The system time was changed.

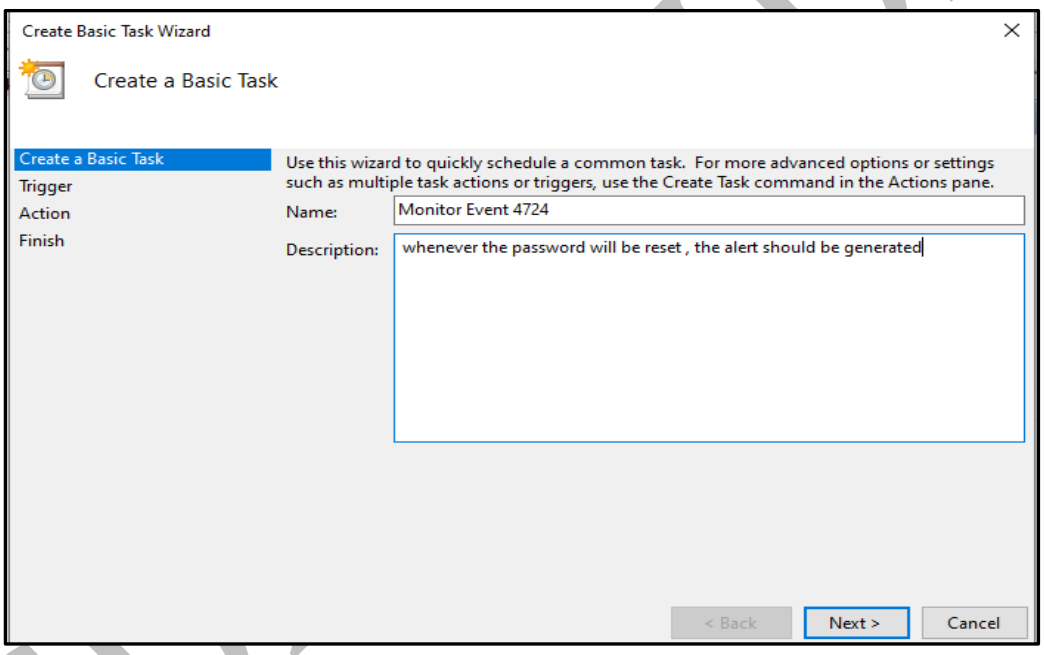
  Creating alerts for suspicious events

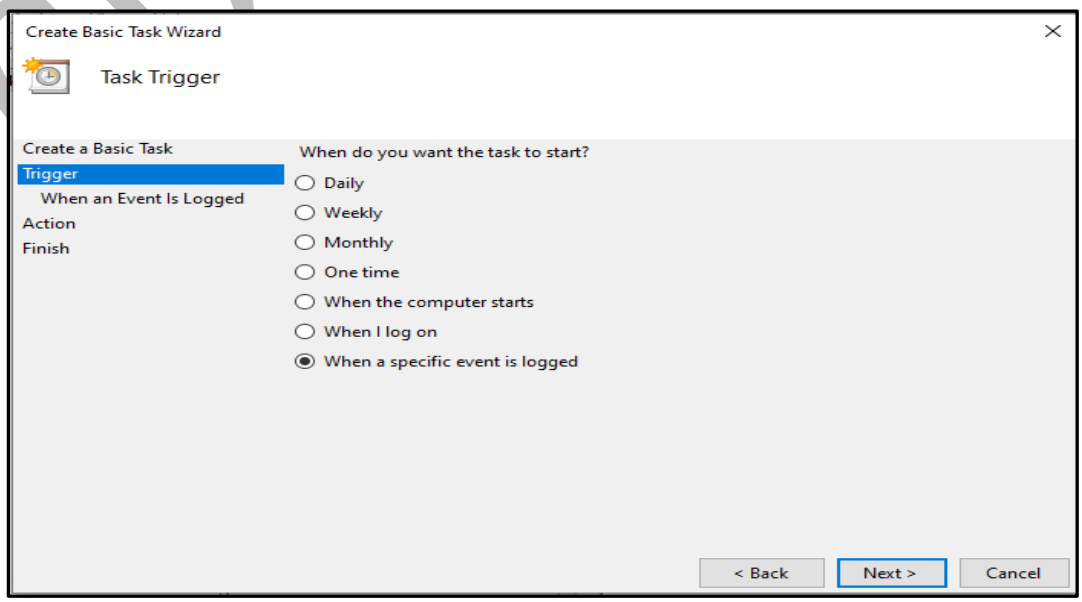
- Windows 8 and later operating systems come equipped with its own built in means of alerting of certain events. It provides a task scheduler for the same. Search for task scheduler in windows search box.

CDAC NOIDA

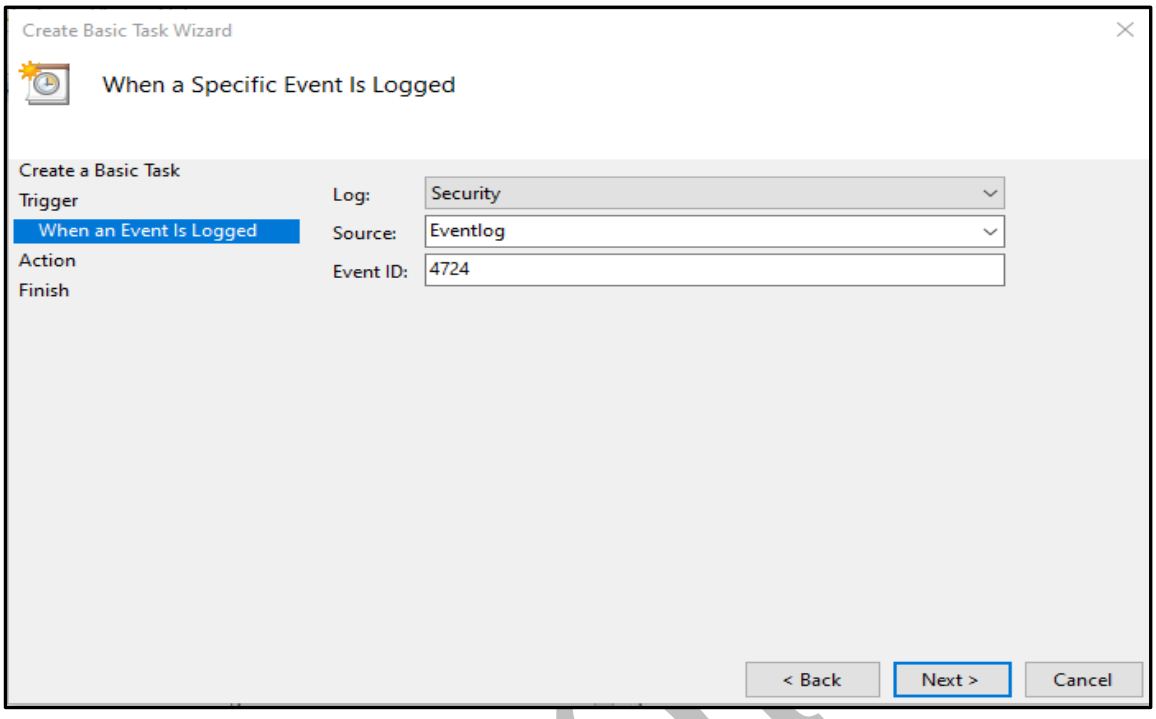


Click on “Create a Basic task”. Provide command with event id.Click on Next button

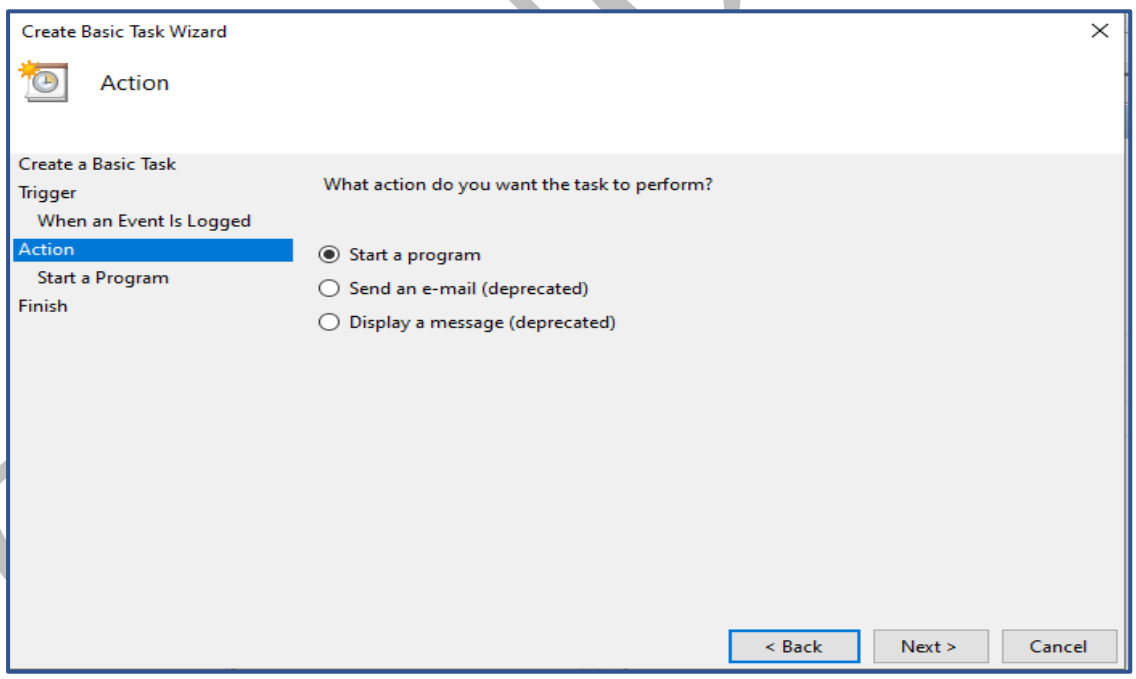




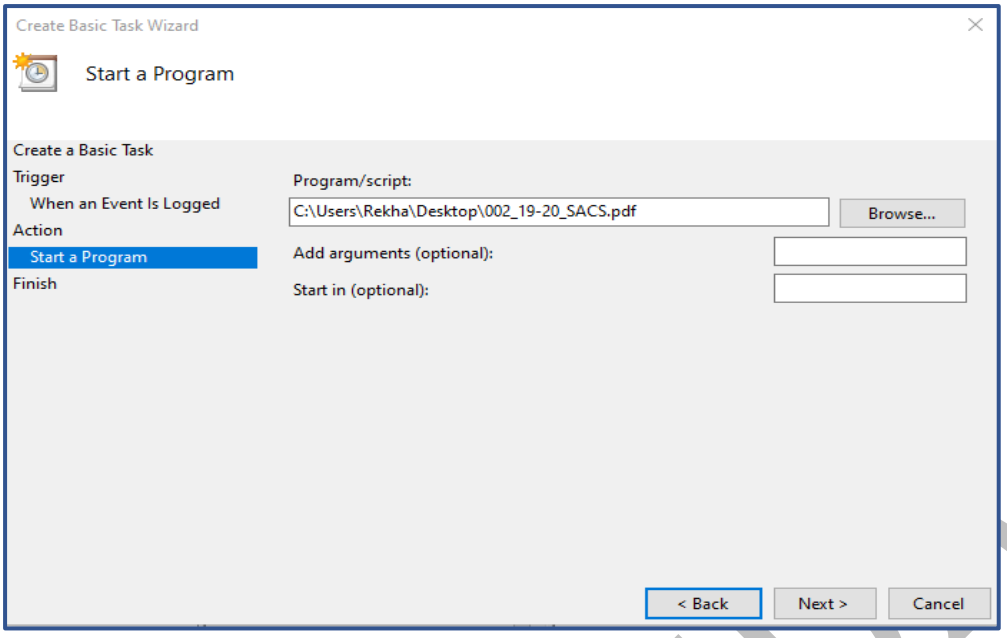
- Make following changes and click on Next button.



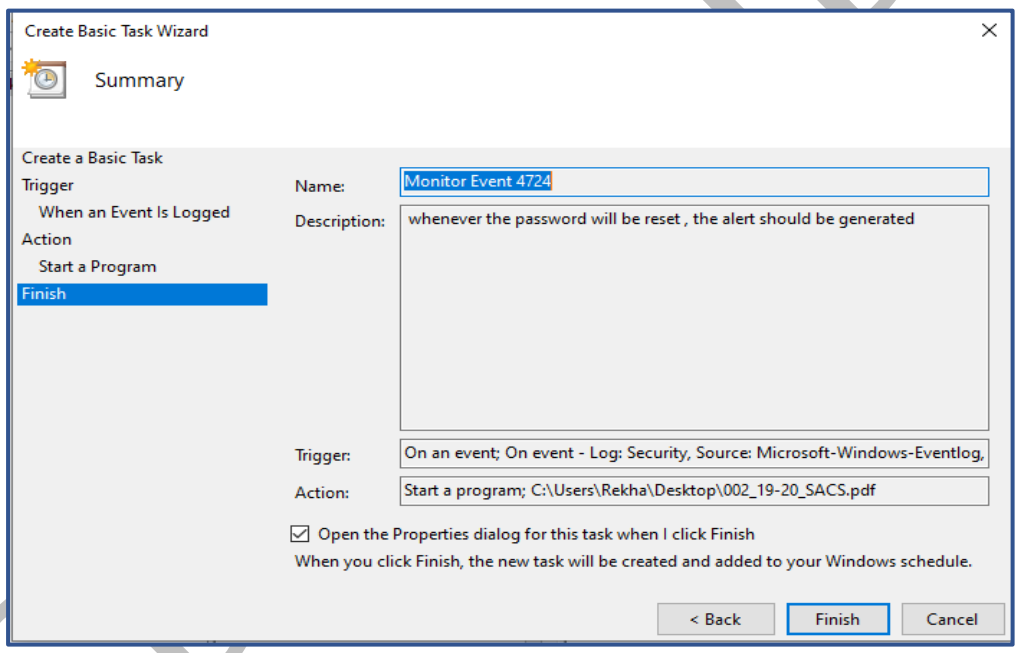
- Click on start a program

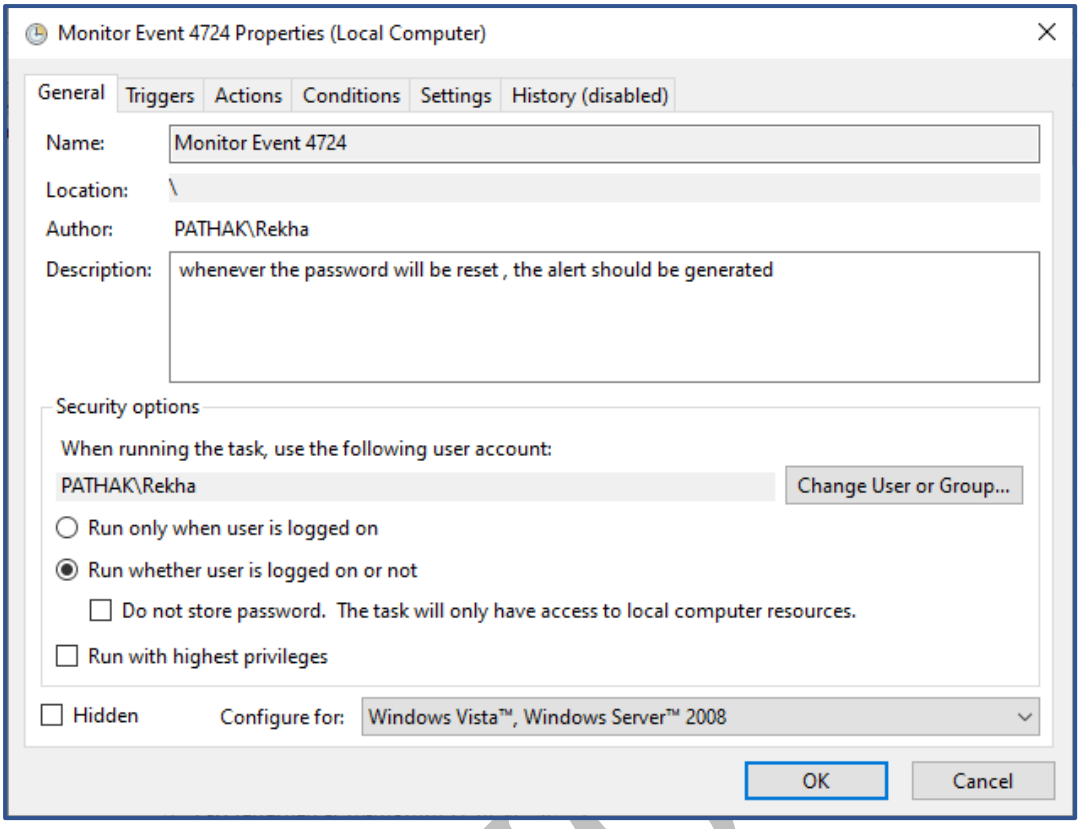


- select a programme to run and click on Next.



Click on Finish button.





- After clicking on finish a prompt will ask for the admin password.

  Provide the password and the task has been created.

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 SMBv1 vulnerability by blocking port 445 at firewalls, which is used by the SMB. This port should especially be blocked if devices and the firewall are facing the external Internet.
3. **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.

IMMEDIATE RESPONSE TO THE SMB ATTACK, IF DETECTED/IDENTIFIED:

Method: Blocking SMB port 445 using Windows Firewall:

Blocking the SMB Port immediately, allows any ongoing session from the attacker to be blocked.

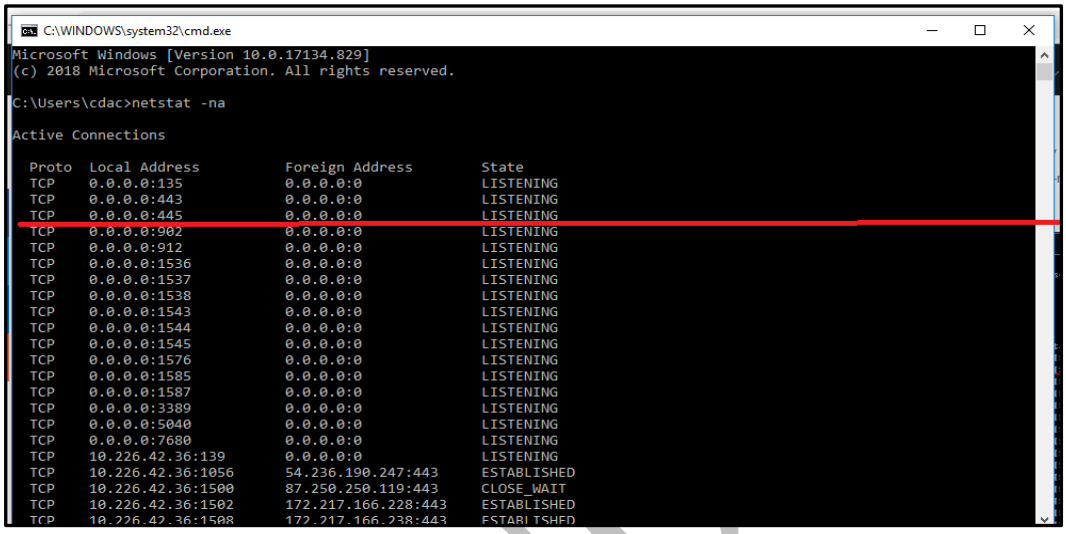
This is a temporary solution for isolating the system from the attacker. The protective measures are required to be imposed for preventing any such incident in future.

a. Check if Port 445 is Enabled.

(i) Press Windows + R key combo to start Run box.
(ii) Input "cmd" to start Command Prompt.
(iii) Type: "netstat –na" and press Enter.

"netstat –na" command shows connected ports.

Port no 445 must be visible here.

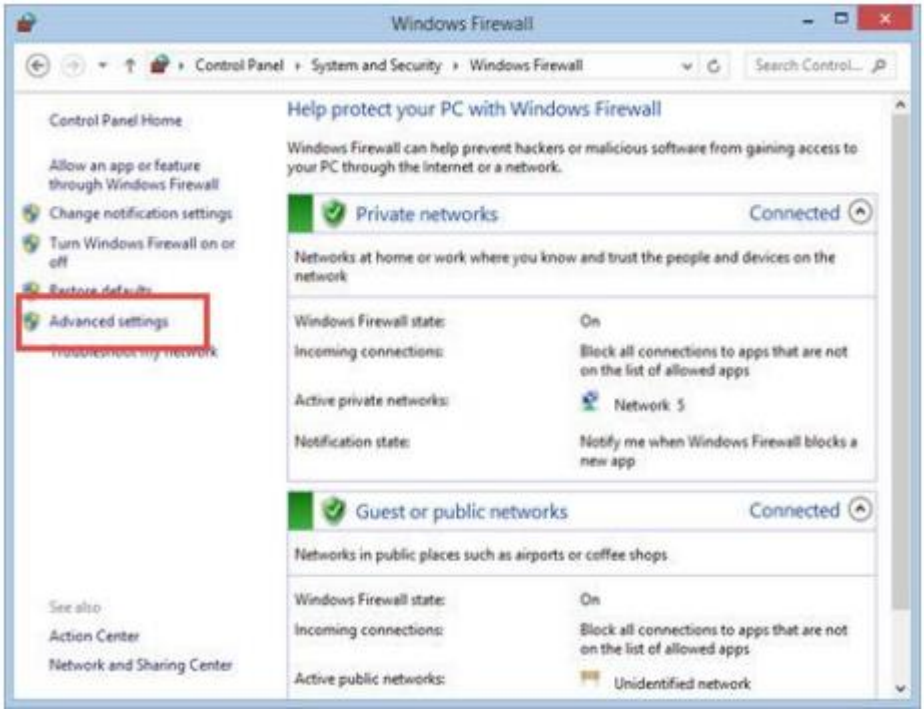


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.829]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\cdac>netstat -na

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    0.0.0.0:1536           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1537           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1538           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1543           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1544           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1545           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1576           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1585           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1587           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    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    10.226.42.36:139       0.0.0.0:0              LISTENING
  TCP    10.226.42.36:1056      54.236.190.247:443     ESTABLISHED
  TCP    10.226.42.36:1500      87.250.250.119:443     CLOSE_WAIT
  TCP    10.226.42.36:1502      172.217.166.228:443    ESTABLISHED
  TCP    10.226.42.36:1508      172.217.166.238:443    ESTABLISHED
```

b. Start & Use the Windows Firewall with Advanced Security

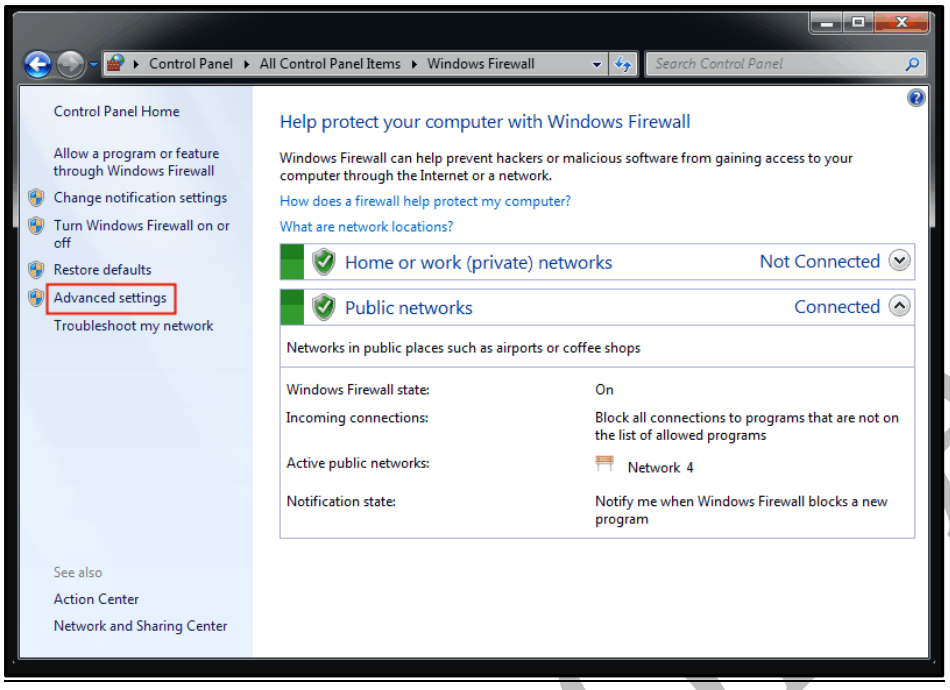
The Windows Firewall with Advanced Security is a tool which provides detailed control over the rules that are applied by the Windows Firewall. It allows to view the rules used by the Windows Firewall, change their properties, create new rules or disable existing ones.

Click on **Control Panel ->System and Security ->Windows Firewall**

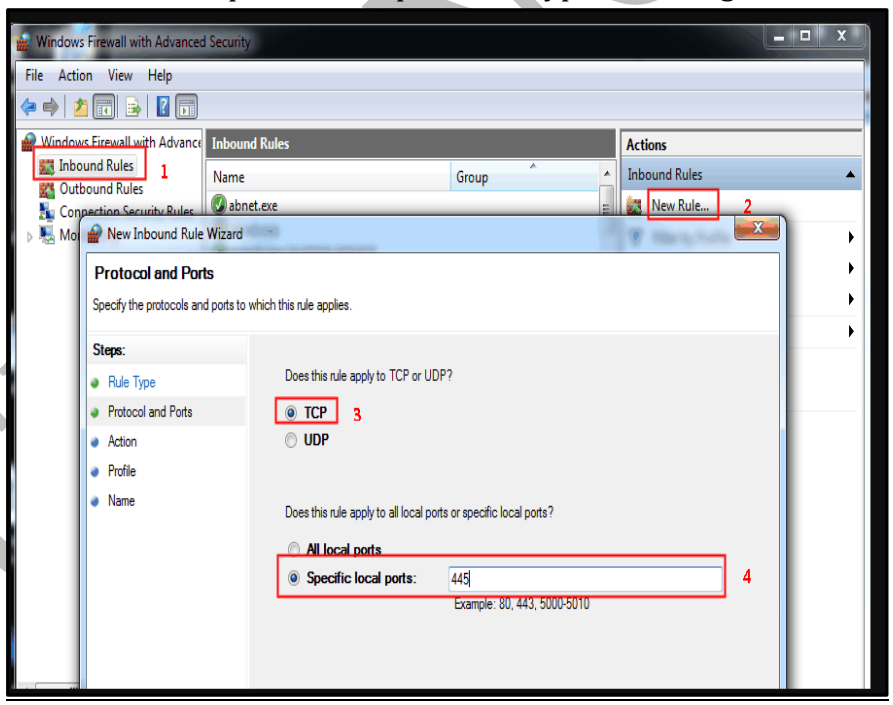


c. Block Port 445 in Windows Firewall

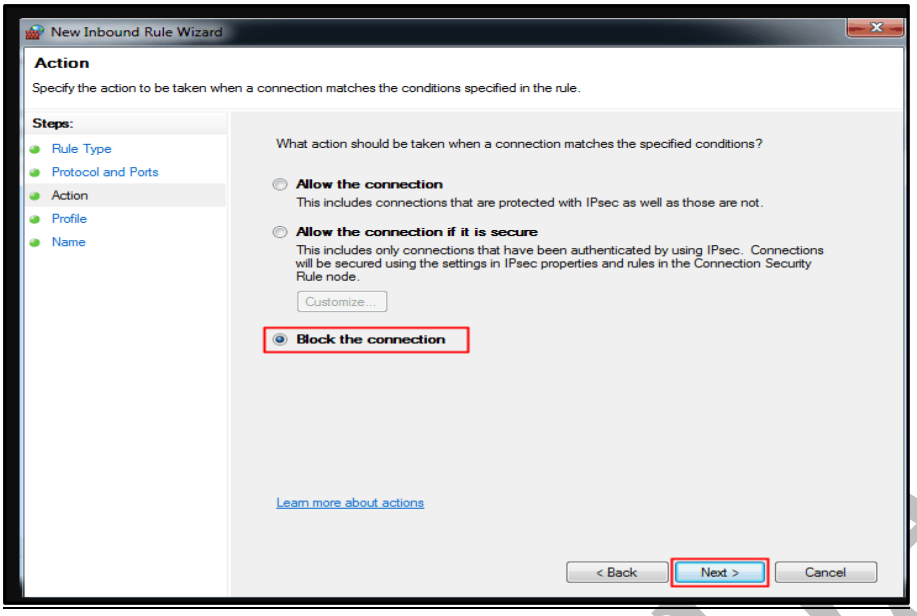
(i) Click on Advanced Settings



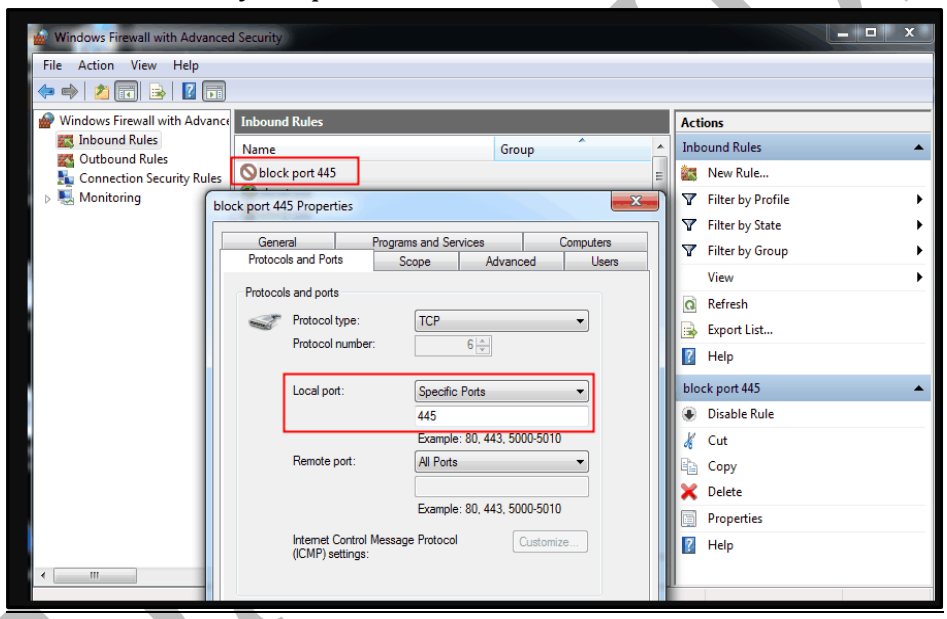
(ii) Click on Inbound Rules > New rule. Then in the pop-up window, choose Port > Next >TCP > Specific local ports and type 445 and go Next



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



(iv) Check the rule by Properties > Protocols and Ports > Local Port.



Please Note that If port 445 is blocked, it is not possible to copy any file system data to or from the path where port 445 is closed. In terms of domain host, this will definitely break group policy. The machine will lose browsing capabilities to networks past the intranet network as well.

PREVENTING THE POSSIBLE SMB BASED ATTACKS:

The prevention of SMB vulnerability-based attacks is only possible by patching your Windows machine with the required patches. these patches are released by Microsoft periodically for known vulnerabilities.

To help you , install the patch on your machine, the patch setup file has already been downloaded and kept on the desktop of your windows machine..

You can install it using one click installation.

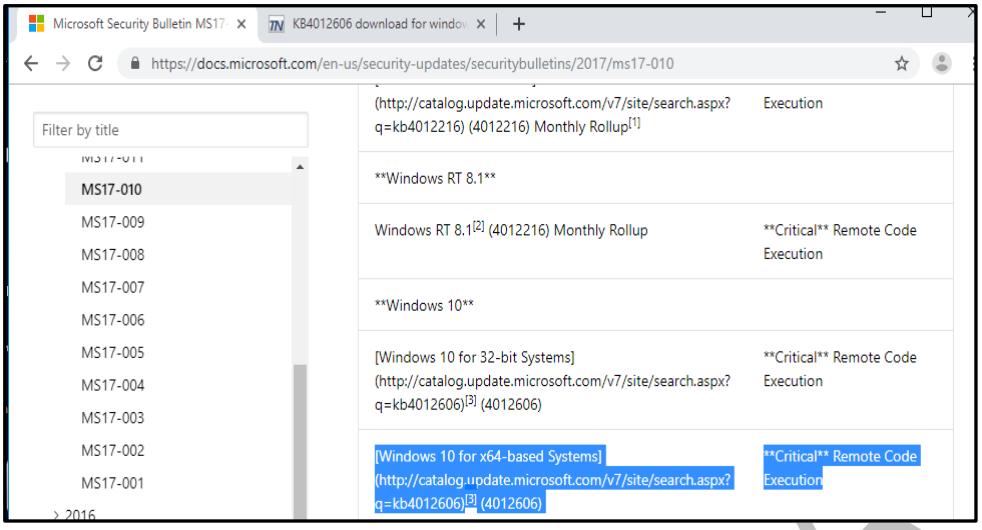
However, if you want to install a patch for your host machine follow the below given steps.

Step1: Installing Security Update for Microsoft Windows SMB Server (4013389)

a. Go to the Microsoft Security bulletin where the links are available for the security update packages.

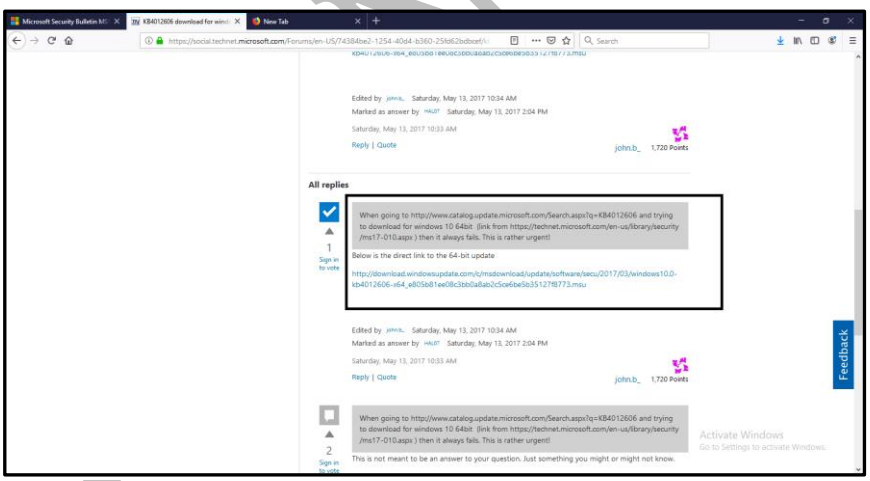
1. Scroll down to the operating system that is in use. In this example, it is Windows 10 64bits.

CEC NOIDA



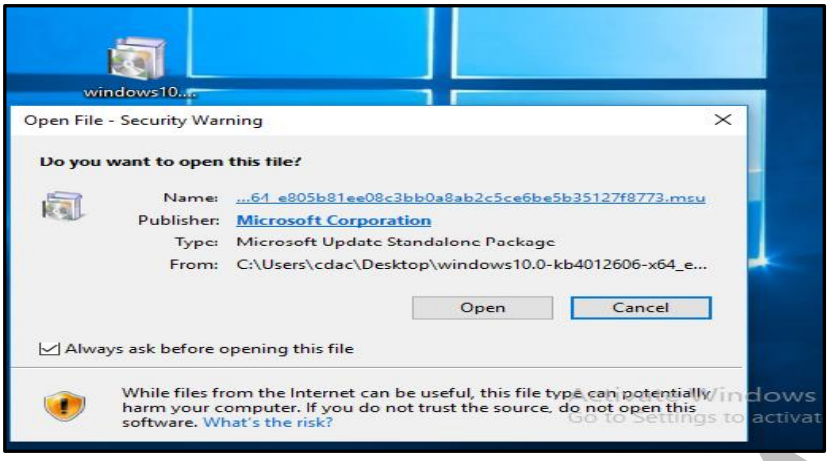
2. Click on the desired package. In this example, the package used is Windows 10 for x64-based Systems (kb4012606) update.

3. Download the package Windows 10 for x64-based Systems (kb4012606). As given in the below image

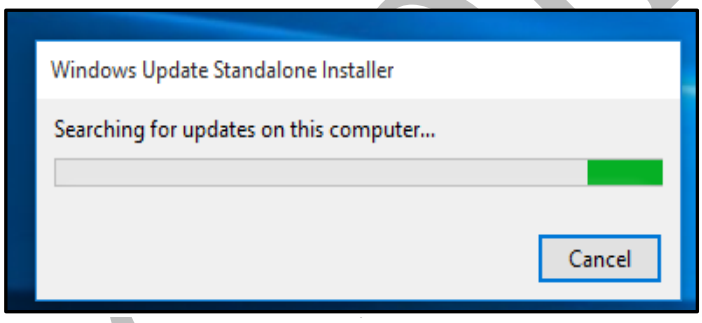


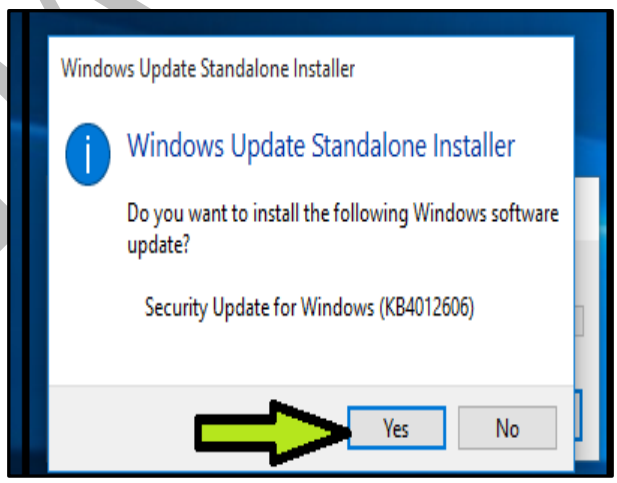
4. .

5. After the download is complete, install the update by right-clicking the file and clicking on Run command.

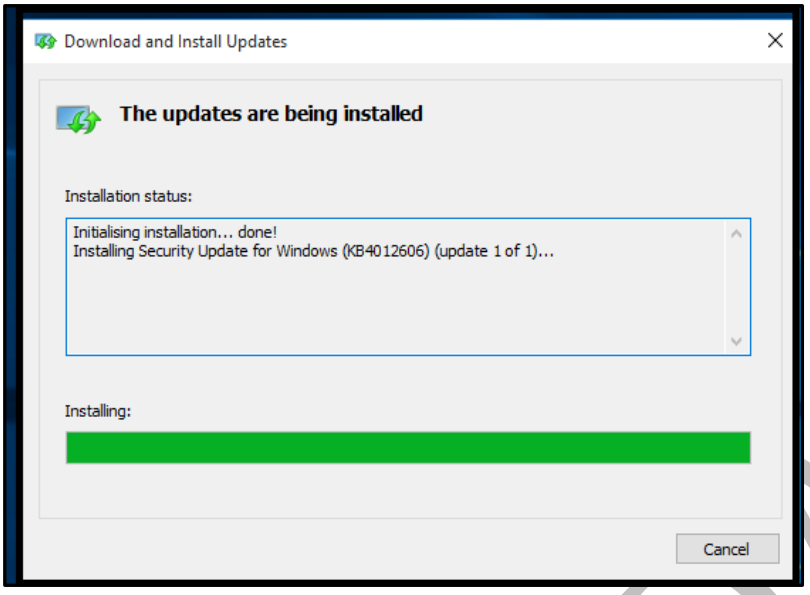


6. Window Prompt appears with the message "Do you want to install the following Windows software update". Press Yes and this will initialize the installation setup:

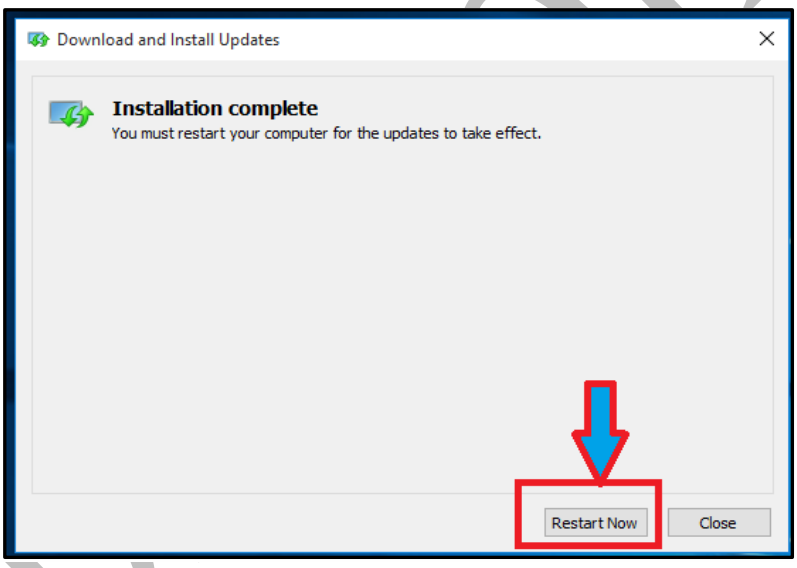




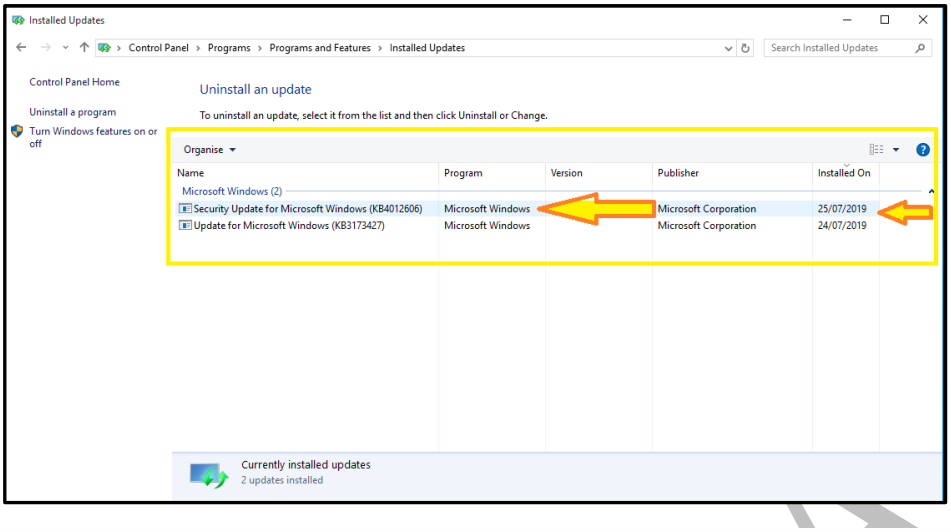
CDAC NOIDA



7. At the end of the installation, it will require to restart the computer. Restart it.

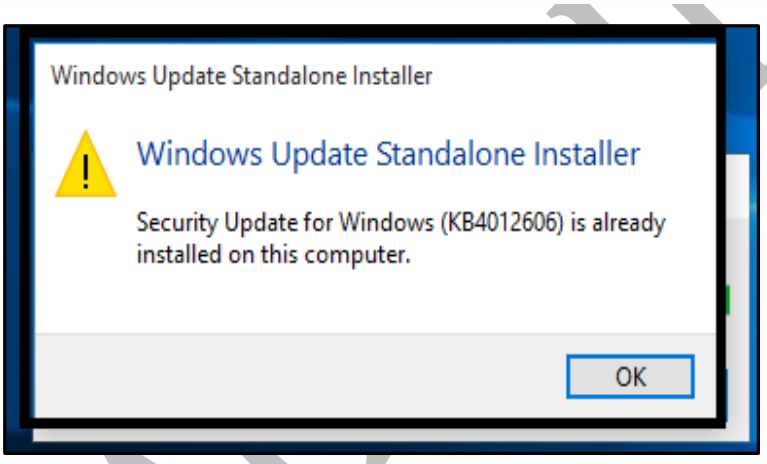


8. To check if the installation was successful, just go to Control Panel > Windows Updates > View update History (on the left side) and see if the Security Update for Windows is installed. It should have the current date in the Date Installed column.



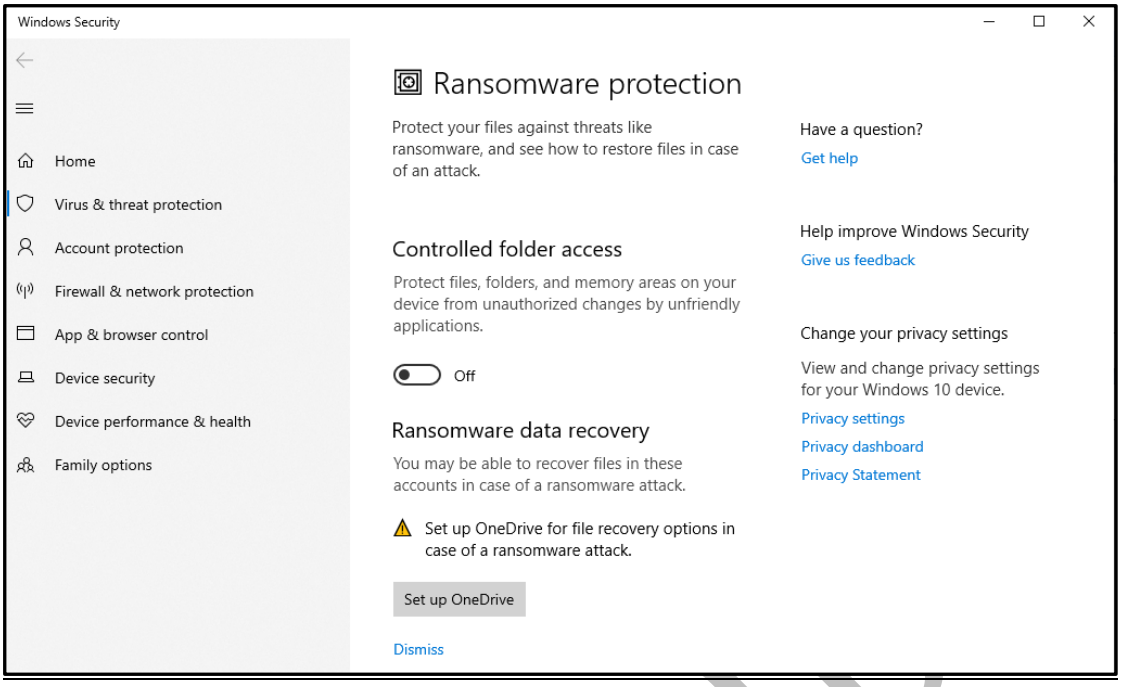
IMPORTANT!

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

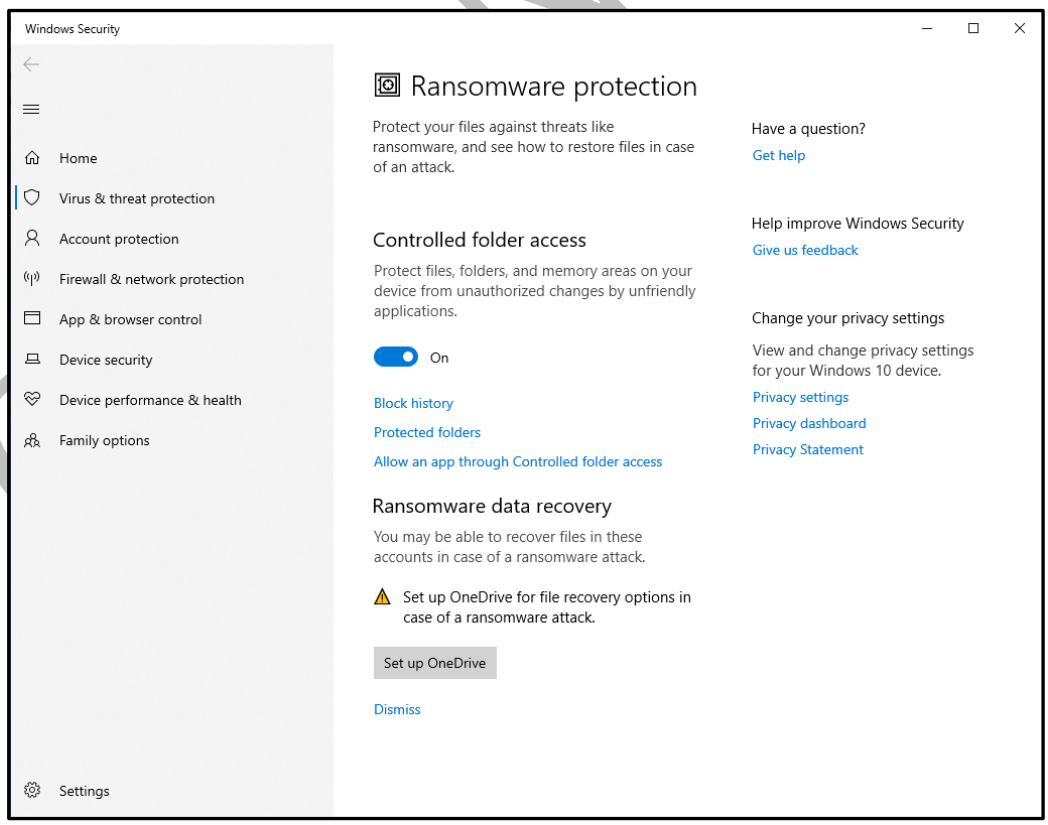


Step2: This method is applicable for windows 10 users. This method allows protecting against the ransom ware attack, which is possible using smb based exploits.

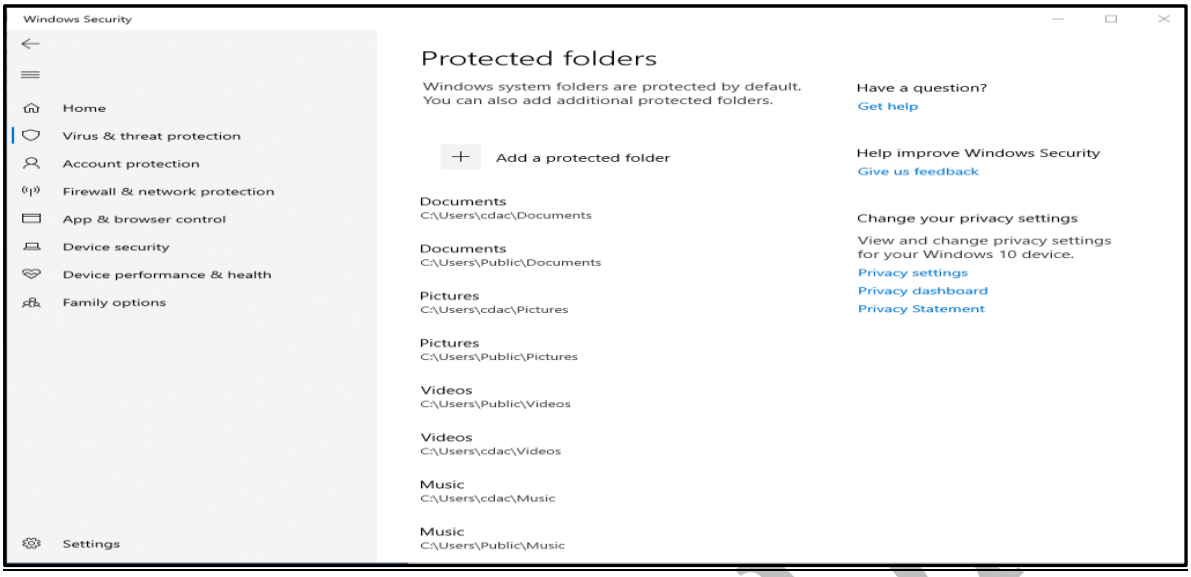
a. <u>Go to windows search bar and search for Ransom ware protection.</u>



b. Switch on the Controlled folder access. This setting blocks any unauthorized changes to the protected folders.



c. Click on Protected folder to view the folders, which are protected by this setting. This allows addition of new folders also.


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Protected folders
Windows system folders are protected by default.
You can also add additional protected folders.
Add a protected folder
Documents
C:\Users\cdac\Documents
Documents
C:\Users\Public\Documents
Pictures
C:\Users\cdac\Pictures
Pictures
C:\Users\Public\Pictures
Videos
C:\Users\Public\Videos
Videos
C:\Users\cdac\Videos
Music
C:\Users\cdac\Music
Music
C:\Users\Public\Music
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

CDAC NOIDA