Sniper - Automatic Exploiter Report

✔ **45.63.119.125**

Target successfully exploited!

Exploitation summary

At least one service running on the target system was found vulnerable and it was successfully exploited.

The successful exploits were:

- 443 Microsoft Exchange - Remote Code Execution (ProxyLogon - CVE-2021-26855, CVE-2021-27065)
- 443 Microsoft Exchange - Remote Code Execution (ProxyShell - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)

Sniper managed to obtain remote code execution as user `nt authority\system`.

Current working directory: `c:\windows\system32\inetsrv`.

Computer:	VULTR-GUEST
IP address:	45.63.119.125
OS:	Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393
Architecture:	x64-based PC
Domain:	pttresearch.local
Language:	en-us;English (United States)

The following TCP ports have been fingerprinted on the target machine:

OPEN PORT	SERVICE NAME	SERVICE VERSION	WEB FINGERPRINT		EXPLOIT STATUS
443	https	HTTPS Microsoft IIS httpd 10.0	**App title:** **Technology:** **Server:**	Outlook ASP.NET 4.0.30319 Microsoft-IIS 10.0	SUCCESSFULLY EXPLOITED • Microsoft Exchange - Remote Code Execution (ProxyLogon - CVE-2021-26855, CVE-2021-27065) • Microsoft Exchange - Remote Code Execution (ProxyShell - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)

System

Local users

This is the list of local users defined at the operating system level. They have privileges on this machine according to the Groups they are part of.
By cracking their password hashes, one can obtain remote access to this machine or to others in the network.

Username:	Administrator
Full name:	Administrator
Description:	Built-in account for administering the computer/domain
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:1324538437d25793cb92ba3893e8a139`
Groups:	Administrators, Schema Admins, Organization Manageme, Group Policy Creator, Domain Admins, Domain Users, Enterprise Admins

Username:	HealthMailbox84f1a64
Full name:	HealthMailbox-vultr-guest-Mailbox-Database-1159205079
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:adebcfe83974282b63d1f43edb7290ce`
Groups:	Domain Users

Username:	HealthMailbox502b450
Full name:	HealthMailbox-vultr-guest-001
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:647fbc6c34ffa1afa3c0635b3bd2ecf0`
Groups:	Domain Users

Username:	HealthMailboxb5d3706
Full name:	HealthMailbox-vultr-guest-002
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:1e6d70d821ac36aa9c1b4a58610a04f1`
Groups:	Domain Users

Username:	HealthMailbox7014eae
Full name:	HealthMailbox-vultr-guest-003
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:fc8d2ddc0f0fffb3d8aec1c4084fc178`
Groups:	Domain Users

Username:	HealthMailbox57897bf
Full name:	HealthMailbox-vultr-guest-004
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:1bba032a5dc1332cecbcd3b41c219c97`
Groups:	Domain Users

Username:	HealthMailbox7ac526f
Full name:	HealthMailbox-vultr-guest-005
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:dc4040d346a72308be562580b226cf97`
Groups:	Domain Users

Username:	HealthMailboxae9aaca
Full name:	HealthMailbox-vultr-guest-006
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:1fc358e81df4c1310dd2c6f938d1ef98`
Groups:	Domain Users

Username:	HealthMailbox3fad29d
Full name:	HealthMailbox-vultr-guest-007
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:10c2072a3844961fdc65fbd749c90e7a`
Groups:	Domain Users

Username:	HealthMailbox248b1a7
Full name:	HealthMailbox-vultr-guest-008
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:f4d34f692bec9c58b71ad57c1bb18942`
Groups:	Domain Users

Username:	HealthMailboxcdb820c
Full name:	HealthMailbox-vultr-guest-009
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:b629b2871650b4f08e426bfeab142d79`
Groups:	Domain Users

Username:	HealthMailbox033519b
Full name:	HealthMailbox-vultr-guest-010
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:fcf6ec36ad89380a271b5e7e1af16320`
Groups:	Domain Users

Username:	john.reaver
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:5132b70546185113327d27726be29cba`
Groups:	Users, Domain Users

Username:	suzanna.miles
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:7689f61ec2a4e2ec0c788217207e0a37`
Groups:	Domain Users

Username:	danny.scott
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:220036d802fb3f08f8b86c870ce8451f`
Groups:	Domain Users

Processes

This list contains all the processes running on the target OS. Notice the owner of each process, any antivirus solution or the full path of each executable.

BINARY	COMMAND	USER	PID	WINDOW TITLE
System Idle Process		NT AUTHORITY\SYSTEM	0	N/A

Process				
System		NT AUTHORITY\SYSTEM	4	N/A
smss.exe		NT AUTHORITY\SYSTEM	304	N/A
csrss.exe		N/A	404	N/A
wininit.exe		NT AUTHORITY\SYSTEM	480	N/A
winlogon.exe	`winlogon.exe`	NT AUTHORITY\SYSTEM	564	N/A
services.exe		NT AUTHORITY\SYSTEM	616	N/A
lsass.exe	`C:\Windows\system32\lsass.exe`	NT AUTHORITY\SYSTEM	624	N/A
svchost.exe		NT AUTHORITY\SYSTEM	808	N/A
dwm.exe	`dwm.exe`	Window Manager\DWM-1	740	N/A
dfsrs.exe		NT AUTHORITY\SYSTEM	2516	N/A
Microsoft.ActiveDirectory.WebServices.exe		NT AUTHORITY\SYSTEM	2580	N/A
hostcontrollerservice.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\hostcontrollerservice.exe`	NT AUTHORITY\SYSTEM	2588	N/A
ismserv.exe		NT AUTHORITY\SYSTEM	2600	N/A
SMSvcHost.exe		NT AUTHORITY\LOCAL SERVICE	2608	N/A
dns.exe		NT AUTHORITY\SYSTEM	2692	N/A
MSExchangeHMRecovery.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMRecovery.exe`	NT AUTHORITY\SYSTEM	2700	N/A
MSExchangeHMHost.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMHost.exe`	NT AUTHORITY\SYSTEM	2712	N/A
fms.exe	`C:\Program Files\Microsoft\Exchange Server\V15\FIP-FS\Bin\FMS.exe`	NT AUTHORITY\SYSTEM	2728	N/A
mqsvc.exe		NT AUTHORITY\NETWORK SERVICE	2752	N/A
sftracing.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\Diagnostics\TraceService\sftracing.exe`	NT AUTHORITY\SYSTEM	2872	N/A
inetinfo.exe	`C:\Windows\system32\inetsrv\inetinfo.exe`	NT AUTHORITY\SYSTEM	2904	N/A
dfssvc.exe		NT AUTHORITY\SYSTEM	2912	N/A
WMSvc.exe		NT AUTHORITY\LOCAL SERVICE	2936	N/A
Microsoft.Exchange.Directory.TopologyService.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.Directory.TopologyService.exe`	NT AUTHORITY\SYSTEM	3776	N/A

vds.exe		NT AUTHORITY\SYSTEM	3888	N/A
WmiPrvSE.exe	`C:\Windows\system32\wbem\wmiprvse.exe`	NT AUTHORITY\SYSTEM	2324	N/A
noderunner.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\Runtime\1.0\NodeRunner.exe --noderoot "C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\Data\Nodes\Fsis\AdminNode1" --addfrom "C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\Data\Nodes\Fsis\AdminNode1\Configuration\Local\Node.ini" --tracelog "C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\Data\Nodes\Fsis\AdminNode1\Logs\NodeRunner.log"`	NT AUTHORITY\SYSTEM	4408	N/A
MSExchangeMailboxAssistants.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMailboxAssistants.exe`	NT AUTHORITY\SYSTEM	4524	N/A
MSExchangeDagMgmt.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeDagMgmt.exe`	NT AUTHORITY\SYSTEM	2216	N/A
MSExchangeFrontendTransport.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe`	NT AUTHORITY\SYSTEM	4900	N/A
Microsoft.Exchange.RpcClientAccess.Service.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.RpcClientAccess.Service.exe`	NT AUTHORITY\SYSTEM	4620	N/A
MSExchangeCompliance.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeCompliance.exe`	NT AUTHORITY\SYSTEM	4608	N/A
msexchangerepl.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\msexchangerepl.exe`	NT AUTHORITY\SYSTEM	4604	N/A
ComplianceAuditService.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\ComplianceAuditService.exe`	NT AUTHORITY\SYSTEM	4588	N/A
MSExchangeMailboxReplication.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMailboxReplication.exe`	NT AUTHORITY\SYSTEM	4624	N/A
MSExchangeTransportLogSearch.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeTransportLogSearch.exe`	NT AUTHORITY\SYSTEM	4520	N/A
Microsoft.Exchange.Search.Service.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Search.Service.exe`	NT AUTHORITY\SYSTEM	4148	N/A
MSExchangeSubmission.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeSubmission.exe`	NT AUTHORITY\SYSTEM	4720	N/A
Microsoft.Exchange.UM.CallRouter.exe	`C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\CallRouter\Microsoft.Exchange.UM.CallRouter.exe`	NT AUTHORITY\SYSTEM	3848	N/A
umservice.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\umservice.exe`	NT AUTHORITY\SYSTEM	3712	N/A

Microsoft.Exchange.ServiceHost.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.ServiceHost.exe`	NT AUTHORITY\SYSTEM	3852	N/A
Microsoft.Exchange.EdgeSyncSvc.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.EdgeSyncSvc.exe`	NT AUTHORITY\SYSTEM	3660	N/A
Microsoft.Exchange.Store.Service.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Store.Service.exe`	NT AUTHORITY\SYSTEM	496	N/A
MSExchangeDelivery.exe		NT AUTHORITY\NETWORK SERVICE	4488	N/A
Microsoft.Exchange.AntispamUpdateSvc.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.AntispamUpdateSvc.exe`	NT AUTHORITY\SYSTEM	828	N/A
MSExchangeThrottling.exe		NT AUTHORITY\NETWORK SERVICE	5112	N/A
updateservice.exe		N/A	7752	N/A
w3wp.exe	`c:\windows\system32\inetsrv\w3wp.exe -ap "MSExchangeServicesAppPool" -v "v4.0" -c "C:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipm66907648-9520-4317-9f09-f220a8009ca3 -h "C:\inetpub\temp\apppools\MSExchangeServicesAppPool\MSExchangeServicesAppPool.config" -w "" -m 0`	NT AUTHORITY\SYSTEM	8392	N/A
Microsoft.Exchange.Store.Worker.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Store.Worker.exe -id:096536dd-5aa9-42f0-a372-d5a2b16db062 -dag:60f54fd2-704a-4abd-9195-357acb21dbe3 -pipe:3420 -readykey:Global\WorkerReadyKey-1af71805-a83a-45c9-9be4-c47c9d284ad7`	NT AUTHORITY\SYSTEM	8864	N/A
ForefrontActiveDirectoryConnector.exe		N/A	4512	N/A
scanningprocess.exe		N/A	8624	N/A
MSExchangeTransport.exe		NT AUTHORITY\NETWORK SERVICE	9924	N/A
EdgeTransport.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\edgetransport.exe -pipe:2536 -stopkey:Global\ExchangeStopKey-ea3c038b-f020-44e4-8c8b-383c82cb4c49 -resetkey:Global\ExchangeResetKey-ac7d9785-8549-45a5-972b-0da770976821 -readykey:Global\ExchangeReadyKey-a6a0d23a-0c9e-4aef-90bd-4414d4b0d459 -hangkey:Global\ExchangeHangKey-18be9d9f-fccd-4360-96ed-37186d0479ad -startUpProgressKey:Global\ExchangeProgressKey-97204def-3249-4b71-8ed8-9978a48658e8`	NT AUTHORITY\NETWORK SERVICE	10072	N/A

	-workerListening			
conhost.exe	\??\C:\Windows\system32\conhost.exe 0x4	NT AUTHORITY\NETWORK SERVICE	10084	N/A
msdtc.exe		NT AUTHORITY\NETWORK SERVICE	2156	N/A
Microsoft.Exchange.Diagnostics.Service.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.Diagnostics.Service.exe	NT AUTHORITY\SYSTEM	9392	N/A
SearchIndexer.exe		NT AUTHORITY\SYSTEM	2124	N/A
rundll32.exe	NT AUTHORITY\SYSTEM	6288	N/A	
RuntimeBroker.exe		N/A	10308	N/A
sihost.exe	sihost.exe	PTTRESEARCH\Administrator	10360	N/A
taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}	PTTRESEARCH\Administrator	10416	N/A
ServerManager.exe	C:\Windows\system32\ServerManager.exe	PTTRESEARCH\Administrator	2440	N/A
ApplicationFrameHost.exe		N/A	5024	N/A
cmd.exe	C:\Windows\system32\cmd.exe	PTTRESEARCH\Administrator	12752	N/A
puttygen.exe	C:\Program Files\PuTTY\puttygen.exe	PTTRESEARCH\Administrator	13472	N/A
brave.exe	C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe	PTTRESEARCH\Administrator	13868	N/A
MsMpEng.exe		NT AUTHORITY\SYSTEM	10196	N/A
MSExchangeHMWorker.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMWorker.exe -pipe:5556 -stopkey:Global\ExchangeStopKey-3124c830-aa15-47fa-a4f7-c14acf1ca44a -resetkey:Global\ExchangeResetKey-2614b25a-9ace-4bcf-a6b6-8c984c027885 -readykey:Global\ExchangeReadyKey-6e786174-c1b8-4ddf-a133-df8eee97ebcb -hangkey:Global\ExchangeHangKey-3c40d463-c52b-469b-a4dc-f07cf19d6f0a -startUpProgressKey:Global\ExchangeProgressKey-96c4b482-8c2a-450d-9bce-640a7a5dff3b -passive -workerListening	NT AUTHORITY\SYSTEM	19628	N/A
UMWorkerProcess.exe	C:\Program Files\Microsoft\Exchange Server\V15\bin\UMworkerprocess.exe -port:16001 -stopkey:Global\ExchangeUMStopKey-6abaf08b-ea47-4e2c-adee-cff30cc34e9c -resetkey:Global\ExchangeUMResetKey-9fac0cd3-1f7d-4a7c-b3b3-34814b08e116 -fatalkey:Global\ExchangeUMFatalKey-101b577c-45ee-453e-ae84-374cc6350188 -readykey:Global\ExchangeUMReadyKey-0ae26f27-c8aa-4582-bbeb-4950ff8877de -	NT AUTHORITY\SYSTEM	11032	N/A

	`tempdir:temp\UMTempFiles -sipport:5067 -perfenabled:1 -startupMode:TCP -passive`			
explorer.exe	`C:\Windows\explorer.exe /NOUACCHECK`	PTTRESEARCH\Administrator	17176	N/A
ShellExperienceHost.exe	`C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca`	PTTRESEARCH\Administrator	12160	N/A
SearchUI.exe	`C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca`	PTTRESEARCH\Administrator	16932	N/A
winrshost.exe		N/A	20240	N/A
MpCmdRun.exe	`C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2203.5-0\MpCmdRun.exe SpyNetService -RestrictPrivileges -AccessKey 4976425D-D96E-A0CE-BDE1-D69D8DC9F217 -Reinvoke`	NT AUTHORITY\NETWORK SERVICE	21344	N/A
LogonUI.exe	`LogonUI.exe /flags:0x0 /state0:0xa0aa5855 /state1:0x41c64e6d`	NT AUTHORITY\SYSTEM	14348	N/A
LockAppHost.exe		N/A	29436	N/A
tasklist.exe	NT AUTHORITY\SYSTEM	19024	N/A	
TrustedInstaller.exe		NT AUTHORITY\SYSTEM	22784	N/A
TiWorker.exe	`C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.14393.3926_none_7ec739a4221e2b99\TiWorker.exe -Embedding`	NT AUTHORITY\SYSTEM	19568	N/A
NETSTAT.EXE	NT AUTHORITY\SYSTEM	26856	N/A	
WMIC.exe	NT AUTHORITY\SYSTEM	10812	N/A	
systeminfo.exe	NT AUTHORITY\SYSTEM	29272	N/A	
net.exe	NT AUTHORITY\SYSTEM	15020	N/A	

Disk drives

Sniper has skimmed the filesystem and extracted some interesting files as proof of concept.

Drive C:\

Path:	C:\EXCHAN~1\Install-AdminToolsRole-20210422-114100039612600255599.ps1
Name:	Install-AdminToolsRole-20210422-114100039612600255599.ps1
Size:	7,903 KB
Modified:	04/22/2021 11:41 AM

Content:

```
# Default Install steps for AdminToolsRole.
# Programmatically generated on 4/22/2021 11:41:00 AM.

#
# Variable Declarations
#
$RoleAllRoles = 'BridgeheadRole,GatewayRole,ClientAccessRole,MailboxRole,UnifiedMessag
ingRole,FrontendTransportRole,AdminToolsRole,MonitoringRole,CentralAdminRole,CentralAd
minDatabaseRole,CentralAdminFrontEndRole,LanguagePacksRole,CafeRole,FfoWebServiceRole,
OSPRole'
$RoleBinPath = 'C:\Program Files\Microsoft\Exchange Server\V15\Bin'
$RoleDatacenterPath = 'C:\Program Files\Microsoft\Exchange Server\V15\Datacenter'
$RoleDatacenterServiceEndpointABCHContactService = '<ServiceEndpoint><Url>http://pvt-c
ontacts.msn.com/abservice/abservice.asmx</Url></ServiceEndpoint>'
$RoleDatacenterServiceEndpointDomainPartnerManageDelegation = '<ServiceEndpoint><Url>h
ttps://domains.live.com/service/managedelegation.asmx</Url></ServiceEndpoint>'
$RoleDatacenterServiceEndpointDomainPartnerManageDelegation2 = '<ServiceEndpoint><Url>
https://domains.live.com/service/managedelegation2.asmx</Url></ServiceEndpoint>'
$RoleDatacenterServiceEndpointLiveFederationMetadata = '<ServiceEndpoint><Url>https://
nexus.passport.com/FederationMetadata/2006-12/FederationMetadata.xml</Url></ServiceEnd
point>'
$RoleDatacenterServiceEndpointLiveGetUserRealm = '<ServiceEndpoint><Url>https://login.
live.com/GetUserRealm.srf</Url></ServiceEndpoint>'
$RoleDatacenterServiceEndpointLiveServiceLogin2 = '<ServiceEndpoint><Url>https://login
.live.com/RST2.srf</Url></ServiceEndpoint>'
$RoleDatacenterServiceEndpointMsoFederationMetadata = '<ServiceEndpoint><Url>https://n
exus.microsoftonline-p.com/FederationMetadata/2006-12/FederationMetadata.xml</Url></Se
rviceEndpoint>'
$RoleDomainController = 'vultr-guest.pttresearch.local'
$RoleFqdnOrName = 'vultr-guest.pttresearch.local'
$RoleInstallationMode = 'Install'
$RoleInstallPath = 'C:\Program Files\Microsoft\Exchange Server\V15\'
$RoleInvocationID = '20210422-114100039612600255599'
$RoleIsDatacenter = $False
$RoleIsDatacenterDedicated = $False
$RoleIsFfo = $False
$RoleIsPartnerHosted = $False
$RoleLanguagePacksPath = 'E:\\'
$RoleLoggedOnUser = 'PTTRESEARCH\administrator'
$RoleLoggingPath = 'C:\Program Files\Microsoft\Exchange Server\V15\Logging'
$RoleNetBIOSName = 'VULTR-GUEST'
$RolePreviousVersion = $null
$RoleProductPlatform = 'amd64'
$RoleRoleName = 'AdminToolsRole'
$RoleSetupLoggingPath = 'C:\ExchangeSetupLogs'
$RoleTargetVersion = '15.01.1591.010'
$RoleUpdatesDir = $null

#
# Component tasks
#

# Tasks for 'All Roles Common First - Run Once' component
# [ID = AllRolesCommonFirst_RunOnce___b30cefaa0d2a486086e9b6517e52add7, Wt = 1, isFata
l = True] "Configuring the server."
4/22/2021 11:41:00 AM:
```

```
"ddurb"="?"
"burb"="?"
"gguob"="?"
"nyopb"="?"
"tub"="?"
"opb"="?"
"jjutb"="?"
"zotb"="?"
"pytb"="?"
"hmob"="?"
"yitb"="?"
"vurb"="?"
"shyb"="?"
"vepb"="?"
"ryrb"="?"
"zab"="?"
"job"="?"
"nzupb"="?"
"jjyb"="?"
"gotb"="?"
"jjieb"="?"
"wob"="?"
"dub"="?"
"shurb"="?"
"lieb"="?"
"cyb"="?"
"cuopb"="?"
"cipb"="?"
"hxopb"="?"
"shatb"="?"
"zurb"="?"
"shopb"="?"
"cheb"="?"
"zzietb"="?"
"nbieb"="?"
"keb"="?"
```

Path:	C:\Users\ADMINI~1\Desktop\configure.bat
Name:	configure.bat
Size:	386 KB
Modified:	11/04/2021 03:54 PM

Content:	`PowerShell.exe -PSConsoleFile "\\ServerName\c$\Program Files\Microsoft\Exchange Server\Bin\ExShell.Psc1" -Command ". '\\Server Name\c$\Users\User\Desktop\testps1.ps1'"`
	
	`PowerShell.exe -noexit -command ". 'C:\Program Files\Microsoft\Exchange Server\V15\bin\RemoteExchange.ps1'; Connect-ExchangeServer -auto; 'C:\Program Files\Microsoft\Exchange Server\V15\bin\enablesentforshared.ps1'"`

Path:	C:\Users\ADMINI~1\Desktop\Server-SHA512.crt
Name:	Server-SHA512.crt
Size:	2,152 KB
Modified:	11/04/2021 03:58 PM

Content:	-----BEGIN CERTIFICATE----- MIIF7zCCBNegAwIBAgIRANdVj9r18RBbshMoK3B3KaMwDQYJKoZIhvcNAQEFBQAw gZcxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJVVDEXMBUGA1UEBxMOU2FsdCBMYWtl IENpdHkxHjAcBgNVBAoTFVRoZSBVU0VSVFJVU1QgTmV0d29yazEhMB8GA1UECxMY aHR0cDovL3d3dy51c2VydHJ1c3QuY29tMR8wHQYDVQQDExZVVE4tVVNFUkZpcnN0 LUhhcmR3YXJlMB4XDTExMDMxNTAwMDAwMFoXDTE0MDMxNDIzNTk1OVowgd8xCzAJ BgNVBAYTAlVTMQ4wDAYDVQQREwUzODQ3NzEQMA4GA1UECBMHRmxvcmlkYTEQMA4G A1UEBxMHRW5nbGlzaDEXMBUGA1UECRMOU2VhIFZpbGxhZ2UgMTAxFDASBgNVBAoT C0dvb2dsZSBMdGQuMRMwEQYDVQQLEwpUZWNoIERlcHQuMSgwJgYDVQQLEx9Ib3N0 ZWQgYnkgR1RJIEdyb3VwIENvcnBvcmF0aW9uMRQwEgYDVQQLEwtQbGF0aw51bVNT TDEYMBYGA1UEAxMPbG9naW4ueWFob28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAoaQFPe2FRZOKGE3GAwBX4kB38Bzr0BnfIl0If9EHPEGJRhej Cfr8+KkE0ZaPq9dPPPmtGKl0gcRXCjomFs5iPrw/bCHuk43LDaAfmpbQj631k5OC 7nIMoXUVo3uEVrit/1IRcYS8QjALfpio4ag/N1LQ8XxvkNhFCqw5cmph1bvDjPnC zN/9OnG5r7zcOtwMtrHS0Ym7Qbby3lfVFd78/eIxxd/KwdiPLL/wDltx4DRxw8VN fXrU+u0wSy/qti6ekzziOvhCohru3N/ND6n2eYQajmwCtoblv1FqZvjznNNZDHul mXjNfJn6xpZH2DLUdHYOd0sgdKS3iXWSSrRbVQIDAQABo4IB6jCCAeYwHwYDVR0j BBgwFoAUoXJfJhsomEOVXQc31YWWnUvSw0UwHQYDVR0OBBYEFIZJRfwzGTPUBO0n Ye7oAckMfy9+MA4GA1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAAMB0GA1UdJQQW MBQGCCsGAQUFBwMBBggrBgEFBQcDAjBGBgNVHSAEPzA9MDsGDCsGAQQBsjEBAgED BDArMCkGCCsGAQUFBwIBFh1odHRwczovL3NlY3VyZS5jb21vZG8uY29tL0NQUzB7 BgNVHR8EdDByMDigNqA0hjJodHRwOi8vY3JsLmNvbW9kb2NhLmNvbS9VVE4tVVNF UkZpcnN0LUhhcmR3YXJlLmNybDA2oDSgMoYwaHR0cDovL2NybC5jb21vZG8ubmV0 L1VUTi1VU0VSRmlyc3QtSGFyZHdhcmUuY3JsMHEGCCsGAQUFBwEBBGUwYzA7Bggr BgEFBQcwAoYvaHR0cDovL2NydC5jb21vZG9jYS5jb20vVVROQWRkVHJ1c3RTZXJ2 ZXJDQS5jcnQwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmNvbW9kb2NhLmNvbTAv BgNVHREEKDAmgg9sb2dpbi55YWhvby5jb22CE3d3dy5sb2dpbi55YWhvby5jb20w DQYJKoZIhvcNAQEFBQADggEBAD1XyUgkXO5kgfWuvlUpFv8qL4Tt2fijA8gwZrvI 1IEtIfcI96yWQppBdXg6XRAjy5JCYfgK2m1lNBnlqdYtE3jXgUSSqW6AYxXL/jUf AtGKFLCozJQgO6ga8F02UNsNrulk5PaNaX0wyBQXAErlpjX7fQ0inXl2Uiy8lwaI mhX0c+bx9ZilzQdEkbinaGdF0nIRYOJxt1BV4oqpDdaS7gQqizCgogVGNG2Sxjuq TaDQqwEZCjK36OPP8dKXSXuspJf38FeuY3eaf5baTf2+3Ac24yW9iXmOKRITi4gH +2vbpM2zLSfp1Mpg14VT+3TGXDWMcB/5sreSJyDHlNVnFDA= -----END CERTIFICATE-----

Path:	C:\Users\danny.scott\.ssh\authorized_keys
Name:	authorized_keys
Size:	3 KB
Modified:	05/23/2022 07:58 AM
Content:	abc

Path:	C:\Users\danny.scott\.ssh\id_rsa.ppk
Name:	id_rsa.ppk
Size:	1,458 KB
Modified:	05/23/2022 07:57 AM

Content:	PuTTY-User-Key-File-3: ssh-rsa Encryption: none Comment: rsa-key-20220523 Public-Lines: 6 AAAAB3NzaC1yc2EAAAADAQABAAABAQC3eSiFFi+ctvzwHo4RWFhkilCZ8vfH7usV VA8lpuUxqUm+udAZ4D4VTLAi865R7AHF7TmEoFHXbbW8p2KpMUBCngR2sdPJAJni Vd7tYlajTIXTjz7jKxvV9KxRRbqBCqOPauqtT6y3+gQ8KrqImejBB+BD4HS9D7Ja rGQxZck9uiWzQh9U4eaWVKjMuK/fUp3rPl5fbGXenfm868FqdY/dh2SJbgdYUAvL n+z2sYP9ZxTGBAPu1cfFFRInsGOYSvNH+IS3bB+5sAIkbrieheSid4aN/1yfmYdY nHRK4poNH2+CL+ydYm2672JrywE8uKmcUsp0Tjjm+eskaGrU+ggd Private-Lines: 14 AAABAFKrmyBsoMOCiHJBsk4KernCwRK9Mfy6oN6ZY8HZc8huuTXhT+1450B9r5fw KQnsx9fBTnt+KaJiYtNAsQn/sS7TOLug4Pze8nfTrYFVICiwoFR1ZSbDE+XSO5rb SnA+tPg4esng7rhvRV0++5H1l7TysZCKILXXzsughfzkGktfQ6cXp3coVDpme9CQ mEUEk3sg97RDdCg184M0RLh5trMHMFWSJWHmajRgVXFiHhHl75Jm3ZqFpco5zSJS CA2Hd3qRWFZRZD6qZARjZrOEkHb2JfvHvI6MoOMN4kBoFYYB9mA41SgVBCWHImQg 3mdeLguZjl1/Ct+rMt+zzTuuCUEAAACBAN1w1X+0ZF+TM2ohxjRp2+kN2wOUXQrD M6wkPylC6NgGVP1kPiJXi3XMzVhXJs8efZjEGVh79RB4aFrCsgQNLV+155fCSeXs m1E5k2fXS86wO5C9AtE6IgeUE4tvE9gUhGBSHha6i71vBZPwmESokcSEYK+lLe3d C/aUFFQrmP1VAAAAgQDUG2tNDg2G/RKXkckoaWf/0iG0YwmYjpNGojrAcTdgW/LU MlNKhLJhOmRukW6oa/WFk0b2IU69/kHQYMAk2iOVh41NgAh9qac2DSya+mp6IYuN Wo0Oa15uy9hKVP/cQVO1elGypZBGnWjYUYX5I6xexpAtpY3VUqm942hiMRefqQAA AIEAuCIXaoT0NQE+UGOd2A+ITSvbfMLkfcdBLS0Dm1of44lZQcB9hPMgudEqAnek Md86d+jY9GRCZtiZ5/uXVuPb8C/xR/Irc5sO3MZlHJKTNucwuiS0nc15afJWTqA7 Ur+6mL9M82qOWQOrohaH4dokmK7XcF/XLYxugd58RRhfakQ= Private-MAC: e826d56b18a427040c6b2a5b6b4b02d064c8f96525d3e003b9a809ed03ae09dd

Path:	C:\Users\danny.scott\.ssh\id_rsa.pub
Name:	id_rsa.pub
Size:	477 KB
Modified:	05/23/2022 07:57 AM
Content:	---- BEGIN SSH2 PUBLIC KEY ---- Comment: "rsa-key-20220523" AAAAB3NzaC1yc2EAAAADAQABAAABAQC3eSiFFi+ctvzwHo4RWFhkilCZ8vfH7usV VA8lpuUxqUm+udAZ4D4VTLAi865R7AHF7TmEoFHXbbW8p2KpMUBCngR2sdPJAJni Vd7tYlajTIXTjz7jKxvV9KxRRbqBCqOPauqtT6y3+gQ8KrqImejBB+BD4HS9D7Ja rGQxZck9uiWzQh9U4eaWVKjMuK/fUp3rPl5fbGXenfm868FqdY/dh2SJbgdYUAvL n+z2sYP9ZxTGBAPu1cfFFRInsGOYSvNH+IS3bB+5sAIkbrieheSid4aN/1yfmYdY nHRK4poNH2+CL+ydYm2672JrywE8uKmcUsp0Tjjm+eskaGrU+ggd ---- END SSH2 PUBLIC KEY ----

Path:	C:\Windows\DFSRAD~1.CON DfsrAdmin.exe.config
Name:	DFSRAD~1.CON DfsrAdmin.exe.config
Size:	1,315 KB
Modified:	02/03/2021 08:32 PM

Content:

```
ï»¿<configuration>
  <appSettings>
    <!-- Enable the DFS trace listener -->
    <add key="DfsTraceListenerEnabled" value="0" />
    <!-- Trace log file location -->
    <add key="TraceLogLocation" value="%windir%\Debug\DfsMgmt" />
    <!-- Max trace log file size in KB. The default is 10MB (10240KB)
         This value cannot exceed 256MB (262144KB) -->
    <add key="MaxTraceLogSize" value="10240" />
  </appSettings>


  <system.diagnostics>
        <switches>
          <!-- DFS tracing switches can accept the following values:
          0       - No tracing is enabled
          17024   - Trace Errors
          1024    - Trace Warnings
          18048   - Trace Errors and Warnings
          117     - Trace execution flow
          2071    - Trace data flow
          65535   - Trace all
          -->
            <!-- DFS Object Model tracing switch -->
            <add name="DfsFrsTracing" value="0" />
            <!-- DFS UI tracing switch -->
            <add name="DfsrAdminTracing" value="0" />
        </switches>
        <trace autoflush="true">
            <listeners>
              <add name="DfsListener" type="Microsoft.RemoteFileSystems.Management.Dfs
TraceListener" />
            </listeners>
        </trace>
    </system.diagnostics>
</configuration>
```

Network

Configuration

The network configuration of the target host.

Console

```

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5400:4ff:fe00:45ff%2
   IPv4 Address. . . . . . . . . . . : 45.63.119.125
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 45.63.119.1

 Tunnel adapter Local Area Connection* 3:

    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

 Tunnel adapter isatap.{22055F96-118B-4B4F-B6B0-D7E7DDC94B3C}:

    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

```

Neighbors

Some of the live hosts existing in the same local area network as the target host. The information is extracted from the ARP table.

Console

```

Interface: 45.63.119.125 --- 0x2
  Internet Address      Physical Address      Type
  45.63.119.1           fe-00-04-00-45-ff     dynamic
  45.63.119.255         ff-ff-ff-ff-ff-ff     static
  108.61.113.20         fe-00-04-00-45-ff     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
   255.255.255.255       ff-ff-ff-ff-ff-ff     static

```

Services

This list contains the network services of the target host which have open TCP ports.

Console

```

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

```

```
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:444            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:465            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:475            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:476            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:477            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:587            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:717            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:808            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:890            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2525           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3800           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3801           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3803           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3823           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3828           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3843           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3863           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3867           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3875           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:5060           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:5062           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:5067           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6001           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6015           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6062           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6064           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6074           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6075           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6231           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6290           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6334           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6383           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6390           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6400           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6401           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6402           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6403           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6405           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6406           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6409           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6413           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6432           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6434           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6457           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6466           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6516           0.0.0.0:0              LISTENING       InHost
```

```
TCP    0.0.0.0:65349          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:65692          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:7046           0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:7048           0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:8172           0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:9389           0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:9710           0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18779          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18788          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18792          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18793          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18799          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18802          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18803          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18818          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18824          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18825          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18829          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18830          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18832          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18834          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18841          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18844          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18846          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18907          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18916          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:18943          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:29303          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:30348          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:41794          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:45728          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:52377          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:64327          0.0.0.0:0              LISTENING       inmost
TCP    0.0.0.0:64337          0.0.0.0:0              LISTENING       inmost
TCP    45.63.119.127:53       0.0.0.0:0              LISTENING       inmost
TCP    45.63.119.127:81       45.63.119.127:28084    TIME_WAIT       inmost
TCP    45.63.119.127:139      0.0.0.0:0              LISTENING       inmost
TCP    45.63.119.127:443      88.80.189.6:50357      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50380      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50388      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50390      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50397      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50394      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50396      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50410      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50417      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50440      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50447      ESTABLISHED     inmost
TCP    45.63.119.127:443      88.80.189.6:50528      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50744      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50810      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50830      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:50934      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:51000      ESTABLISHED     inmost
TCP    45.63.119.127:443      88.80.189.6:51007      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:51004      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:51006      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:51008      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:51010      TIME_WAIT       inmost
TCP    45.63.119.127:443      88.80.189.6:51017      ESTABLISHED     inmost
TCP    45.63.119.127:443      88.80.189.6:51014      ESTABLISHED     inmost
TCP    45.63.119.127:443      88.80.189.6:51016      ESTABLISHED     inmost
TCP    45.63.119.127:443      88.80.189.6:51018      ESTABLISHED     inmost
TCP    45.63.119.127:443      88.80.189.6:51020      ESTABLISHED     inmost
```

```
  TCP    45.63.119.125:443      88.80.189.67:51046     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51048     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51050     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51052     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51054     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51056     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51058     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51060     ESTABLISHED     InHost
  TCP    45.63.119.125:443      88.80.189.67:51074     ESTABLISHED     InHost
  TCP    45.63.119.125:444      45.63.119.125:28070    TIME WAIT       InHost
  TCP    45.63.119.125:444      45.63.119.125:28074    ESTABLISHED     InHost
  TCP    45.63.119.125:28074    45.63.119.125:444      ESTABLISHED     InHost
  TCP    45.63.119.125:28080    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:28091    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:28111    8.241.9.126:80         ESTABLISHED     InHost
  TCP    45.63.119.125:28134    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:28136    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:28138    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:28140    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:28167    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:28169    45.63.119.125:444      TIME WAIT       InHost
  TCP    45.63.119.125:38847    20.199.120.85:443      ESTABLISHED     InHost
  TCP    45.63.119.125:38855    20.199.120.85:443      ESTABLISHED     InHost
  TCP    45.63.119.125:64327    45.63.119.125:28102    TIME WAIT       InHost
  TCP    127.0.0.1:53           0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:443          127.0.0.1:28079        TIME WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:28089        TIME WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:28097        TIME WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:28112        TIME WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:28154        TIME WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:28158        TIME WAIT       InHost
  TCP    127.0.0.1:444          127.0.0.1:28121        ESTABLISHED     InHost
  TCP    127.0.0.1:444          127.0.0.1:28170        TIME WAIT       InHost
  TCP    127.0.0.1:444          127.0.0.1:41815        ESTABLISHED     InHost
  TCP    127.0.0.1:445          127.0.0.1:28164        ESTABLISHED     InHost
  TCP    127.0.0.1:808          127.0.0.1:27879        ESTABLISHED     InHost
  TCP    127.0.0.1:5060         127.0.0.1:28066        ESTABLISHED     InHost
  TCP    127.0.0.1:5062         127.0.0.1:28099        ESTABLISHED     InHost
  TCP    127.0.0.1:6102         0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:16001        0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:16001        127.0.0.1:45727        ESTABLISHED     InHost
  TCP    127.0.0.1:27879        127.0.0.1:808          ESTABLISHED     InHost
  TCP    127.0.0.1:27916        127.0.0.1:5060         TIME WAIT       InHost
  TCP    127.0.0.1:27948        127.0.0.1:5062         TIME WAIT       InHost
  TCP    127.0.0.1:28066        127.0.0.1:5060         ESTABLISHED     InHost
  TCP    127.0.0.1:28099        127.0.0.1:5062         ESTABLISHED     InHost
  TCP    127.0.0.1:28121        127.0.0.1:444          ESTABLISHED     InHost
  TCP    127.0.0.1:28164        127.0.0.1:445          ESTABLISHED     InHost
  TCP    127.0.0.1:41815        127.0.0.1:444          ESTABLISHED     InHost
  TCP    127.0.0.1:45727        127.0.0.1:16001        ESTABLISHED     InHost

```

Scan parameters

Target:	45.63.119.125
Authenticated scan:	443

Scan information

Start time:	2022-05-31 11:49:00 UTC+03
Finish time:	2022-05-31 11:52:04 UTC+03
Scan duration:	3 min, 4 sec
Scan status:	Finished