

( ) ( )

<https://github.com/WinPEAS/WinPEAS> (<https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS/winPEASexe>) SharpUp (<https://github.com/GhostPack/SharpUp>) Seatbelt (<https://github.com/GhostPack/Seatbelt>)

## SharpUp

```
PS C:\Download> .\sharpup.exe
SharpUp.exe [audit] [check1] [check2]...

audit - Specifies whether or not to enable audit mode. If enabled, SharpUp will run vulenrability checks
regardless if the process is in high integrity or the user is in the local administrator's group.
If no checks are specified, audit will run all checks. Otherwise, each check following audit will
be ran.

check* - The individual vulnerability check to be ran. Must be one of the following:

- AlwaysInstallElevated
- CachedGPPPassword
- DomainGPPPassword
- HijackablePaths
- McAfeeSitelistFiles
- ModifiableServiceBinaries
- ModifiableServiceRegistryKeys
- ModifiableServices
- RegistryAutoLogons
- RegistryAutoruns
- TokenPrivileges
- UnattendedInstallFiles
- UnquotedServicePath
```

SharpUp                      CachedGPPPassword DomainGPPPassword

1           AlwaysInstalledElevated        Token

2           CachedGPPPassword DomainGPPPassword RegistryAutoLogons

## WinPEAS

System Information

Basic System info information

Use Watson to search for vulnerabilities

Enumerate Microsoft updates  
PS, Audit, WEF and LAPS Settings  
LSA protection  
Credential Guard  
WDigest  
Number of cached cred  
Environment Variables  
Internet Settings  
Current drives information  
AV  
Windows Defender  
UAC configuration  
NTLM Settings  
Local Group Policy  
Applocker Configuration & bypass suggestions  
Printers  
Named Pipes  
AMSI Providers  
SysMon  
.NET Versions

#### Users Information

Users information  
Current token privileges  
Clipboard text  
Current logged users  
RDP sessions  
Ever logged users  
Autologin credentials  
Home folders  
Password policies  
Local User details  
Logon Sessions

#### Processes Information

Interesting processes (non Microsoft)

#### Services Information

Interesting services (non Microsoft) information  
Modifiable services

Writable service registry binpath

PATH Dll Hijacking

#### Applications Information

Current Active Window

Installed software

AutoRuns

Scheduled tasks

Device drivers

#### Network Information

Current net shares

Mapped drives (WMI)

hosts file

Network Interfaces

Listening ports

Firewall rules

DNS Cache (limit 70)

Internet Settings

#### Windows Credentials

Windows Vault

Credential Manager

Saved RDP settings

Recently run commands

Default PS transcripts files

DPAPI Masterkeys

DPAPI Credential files

Remote Desktop Connection Manager credentials

Kerberos Tickets

Wifi

AppCmd.exe

SSClient.exe

SCCM

Security Package Credentials

AlwaysInstallElevated

WSUS

#### Browser Information

Firefox DBs

Credentials in firefox history  
Chrome DBs  
Credentials in chrome history  
Current IE tabs  
Credentials in IE history  
IE Favorites  
Extracting saved passwords for: Firefox, Chrome, Opera, Brave

#### Interesting Files and registry

Putty sessions  
Putty SSH host keys  
SuperPutty info  
Office365 endpoints synced by OneDrive  
SSH Keys inside registry  
Cloud credentials  
Check for unattended files  
Check for SAM & SYSTEM backups  
Check for cached GPP Passwords  
Check for and extract creds from McAfee SiteList.xml files  
Possible registries with credentials  
Possible credentials files in users homes  
Possible password files inside the Recycle bin  
Possible files containing credentials (this take some minutes)  
User documents (limit 100)  
Oracle SQL Developer config files check  
Slack files search  
Outlook downloads  
Machine and user certificate files  
Office most recent documents  
Hidden files and folders  
Executable files in non-default folders with write permissions  
WSL check

#### Events Information

Logon + Explicit Logon Events  
Process Creation Events  
PowerShell Events  
Power On/Off Events

#### Additional (slower) checks

LOLBAS search

run linpeas.sh in default WSL distribution

## WinPEAS

1

2

3

4

5

6 DNS

7 Windows DPAPI Wifi Kerberos

8

9 ( PuTTY)

10

## WinPEAS

## SeatBelt

Available commands (+ means remote usage is supported):

+ AMSIProviders	- Providers registered for AMSI
+ AntiVirus	- Registered antivirus (via WMI)
+ AppLocker	- AppLocker settings, if installed
ARPTable	- Lists the current ARP table and adapter information (equivalent to arp -a)
AuditPolicies	- Enumerates classic and advanced audit policy settings
+ AuditPolicyRegistry	- Audit settings via the registry
+ AutoRuns	- Auto run executables/scripts/programs
Certificates	- Finds user and machine personal certificate files
CertificateThumbprints	- Finds thumbprints for all certificate store certs on the system
+ ChromiumBookmarks	- Parses any found Chrome/Edge/Brave/Opera bookmark files
+ ChromiumHistory	- Parses any found Chrome/Edge/Brave/Opera history files

- + ChromiumPresence - Checks if interesting Chrome/Edge/Brave/Opera files exist
- + CloudCredentials - AWS/Google/Azure/Bluemix cloud credential files
- + CloudSyncProviders - All configured Office 365 endpoints (tenants and teamsites)

which are synchronised by OneDrive.

- CredEnum - Enumerates the current user's saved credentials using CredEnumerate()
- + CredGuard - CredentialGuard configuration
- dir - Lists files/folders. By default, lists users' downloads, documents, and desktop folders (arguments == [directory] [maxDepth] [regex] [boolIgnoreErrors])
- + DNSCache - DNS cache entries (via WMI)
- + DotNet - DotNet versions
- + DpapiMasterKeys - List DPAPI master keys
- Dsregcmd - Return Tenant information - Replacement for Dsregcmd /status
- EnvironmentPath - Current environment %PATH\$ folders and SDDL information
- + EnvironmentVariables - Current environment variables
- + ExplicitLogonEvents - Explicit Logon events (Event ID 4648) from the security event log. Default of 7 days, argument == last X days.
- ExplorerMRUs - Explorer most recently used files (last 7 days, argument == last X days)
- + ExplorerRunCommands - Recent Explorer "run" commands
- FileInfo - Information about a file (version information, timestamps, basic PE info, etc. argument(s) == file path(s))
- + FileZilla - FileZilla configuration files
- + FirefoxHistory - Parses any found FireFox history files
- + FirefoxPresence - Checks if interesting Firefox files exist
- + Hotfixes - Installed hotfixes (via WMI)
- IdleTime - Returns the number of seconds since the current user's last input.
- + IEFavorites - Internet Explorer favorites
- IETabs - Open Internet Explorer tabs
- + IEUrls - Internet Explorer typed URLs (last 7 days, argument == last X days)
- + InstalledProducts - Installed products via the registry
- InterestingFiles - "Interesting" files matching various patterns in the user's folder. Note: takes non-trivial time.
- + InterestingProcesses - "Interesting" processes - defensive products and admin tools
- InternetSettings - Internet settings including proxy configs and zones configuration
- + KeePass - Finds KeePass configuration files
- + LAPS - LAPS settings, if installed

- + LastShutdown - Returns the DateTime of the last system shutdown (via the registry).
- LocalGPOs - Local Group Policy settings applied to the machine/local users
- + LocalGroups - Non-empty local groups, "-full" displays all groups (argument == computername to enumerate)
- + LocalUsers - Local users, whether they're active/disabled, and pwd last set (argument == computername to enumerate)
- + LogonEvents - Logon events (Event ID 4624) from the security event log. Default of 10 days, argument == last X days.
- + LogonSessions - Windows logon sessions
- LOLBAS - Locates Living Off The Land Binaries and Scripts (LOLBAS) on the system. Note: takes non-trivial time.
- + LSASettings - LSA settings (including auth packages)
- + MappedDrives - Users' mapped drives (via WMI)
- McAfeeConfigs - Finds McAfee configuration files
- McAfeeSiteList - Decrypt any found McAfee SiteList.xml configuration files.
- MicrosoftUpdates - All Microsoft updates (via COM)
- NamedPipes - Named pipe names, any readable ACL information and associated process information.
- + NetworkProfiles - Windows network profiles
- + NetworkShares - Network shares exposed by the machine (via WMI)
- + NTLMSettings - NTLM authentication settings
- OfficeMRUs - Office most recently used file list (last 7 days)
- OneNote - List OneNote backup files
- + OptionalFeatures - List Optional Features/Roles (via WMI)
- OracleSQLDeveloper - Finds Oracle SQLDeveloper connections.xml files
- + OSInfo - Basic OS info (i.e. architecture, OS version, etc.)
- + OutlookDownloads - List files downloaded by Outlook
- + PoweredOnEvents - Reboot and sleep schedule based on the System event log EIDs 1, 12, 13, 42, and 6008. Default of 7 days, argument == last X days.
- + PowerShell - PowerShell versions and security settings
- + PowerShellEvents - PowerShell script block logs (4104) with sensitive data.
- + PowerShellHistory - Searches PowerShell console history files for sensitive regex matches.
- Printers - Installed Printers (via WMI)
- + ProcessCreationEvents - Process creation logs (4688) with sensitive data.
- Processes - Running processes with file info company names that don't contain 'Microsoft', "-full" enumerates all processes
- + ProcessOwners - Running non-session 0 process list with owners. For remote use.
- + PSSessionSettings - Enumerates PS Session Settings from the registry

```

+ PuttyHostKeys          - Saved Putty SSH host keys
+ PuttySessions          - Saved Putty configuration (interesting fields) and SSH host
keys
  RDCManFiles            - Windows Remote Desktop Connection Manager settings files
+ RDPSavedConnections    - Saved RDP connections stored in the registry
+ RDPsessions            - Current incoming RDP sessions (argument == computername to
enumerate)
+ RDPsettings            - Remote Desktop Server/Client Settings
  RecycleBin             - Items in the Recycle Bin deleted in the last 30 days - only
works from a user context!
  reg                    - Registry key values (HKLM\Software by default) argument ==
[Path] [intDepth] [Regex] [boolIgnoreErrors]
  RPCMappedEndpoints     - Current RPC endpoints mapped
+ SCCM                   - System Center Configuration Manager (SCCM) settings, if
applicable
+ ScheduledTasks         - Scheduled tasks (via WMI) that aren't authored by 'Microsoft',
"-full" dumps all Scheduled tasks
  SearchIndex            - Query results from the Windows Search Index, default term of
'password'. (argument(s) == <search path> <pattern1,pattern2,...>
  SecPackageCreds        - Obtains credentials from security packages
  SecurityPackages       - Enumerates the security packages currently available using
EnumerateSecurityPackagesA()
  Services               - Services with file info company names that don't contain
'Microsoft', "-full" dumps all processes
+ SlackDownloads         - Parses any found 'slack-downloads' files
+ SlackPresence          - Checks if interesting Slack files exist
+ SlackWorkspaces        - Parses any found 'slack-workspaces' files
+ SuperPutty             - SuperPutty configuration files
+ Sysmon                 - Sysmon configuration from the registry
+ SysmonEvents           - Sysmon process creation logs (1) with sensitive data.
  TcpConnections         - Current TCP connections and their associated processes and
services
  TokenGroups            - The current token's local and domain groups
  TokenPrivileges        - Currently enabled token privileges (e.g. SeDebugPrivilege/etc.)
+ UAC                    - UAC system policies via the registry
  UdpConnections         - Current UDP connections and associated processes and services
  UserRightAssignments   - Configured User Right Assignments (e.g.
SeDenyNetworkLogonRight, SeShutdownPrivilege, etc.) argument == computername to enumerate
  WifiProfile            - Enumerates the saved Wifi profiles and extract the ssid,
authentication type, cleartext key/passphrase (when possible)

```

- + WindowsAutoLogon - Registry autologon information
- WindowsCredentialFiles - Windows credential DPAPI blobs
- + WindowsDefender - Windows Defender settings (including exclusion locations)
- + WindowsEventForwarding - Windows Event Forwarding (WEF) settings via the registry
- + WindowsFirewall - Non-standard firewall rules, "-full" dumps all (arguments == allow/deny/tcp/udp/in/out/domain/private/public)
- WindowsVault - Credentials saved in the Windows Vault (i.e. logins from Internet Explorer and Edge).
- + WMI - Runs a specified WMI query
- WMIEventConsumer - Lists WMI Event Consumers
- WMIEventFilter - Lists WMI Event Filters
- WMIFilterBinding - Lists WMI Filter to Consumer Bindings
- + WSUS - Windows Server Update Services (WSUS) settings, if applicable

113

SeatBelt

Chromium

```
"Seatbelt.exe -group=all" runs all commands

"Seatbelt.exe -group=user" runs the following commands:

Certificates, CertificateThumbprints, ChromiumPresence, CloudCredentials, CloudSyncProviders,
CredEnum, dir, DpapiMasterKeys, Dsregcmd,
ExplorerMRUs, ExplorerRunCommands, FileZilla, FirefoxPresence,
IdleTime, IEFavorites, IETabs, IEUrls,
Keepass, MappedDrives, OfficeMRUs, OracleSQLDeveloper,
PowerShellHistory, PuttyHostKeys, PuttySessions, RDCManFiles,
RDPsavedConnections, SecPackageCreds, SlackDownloads, SlackPresence,
SlackWorkspaces, SuperPutty, TokenGroups, WindowsCredentialFiles,
WindowsVault

"Seatbelt.exe -group=system" runs the following commands:

AMSIProviders, AntiVirus, AppLocker, ARPTable, AuditPolicies,
AuditPolicyRegistry, AutoRuns, Certificates, CertificateThumbprints,
CredGuard, DNSCache, DotNet, EnvironmentPath,
EnvironmentVariables, Hotfixes, InterestingProcesses, InternetSettings,
LAPS, LastShutdown, LocalGPOs, LocalGroups,
LocalUsers, LogonSessions, LSASettings, McAfeeConfigs,
NamedPipes, NetworkProfiles, NetworkShares, NTLMSettings,
OptionalFeatures, OSInfo, PoweredOnEvents, PowerShell,
Processes, PSSessionSettings, RDPsessions, RDPsettings,
SCCM, Services, Sysmon, TcpConnections,
TokenPrivileges, UAC, UdpConnections, UserRightAssignments,
WindowsAutoLogon, WindowsDefender, WindowsEventForwarding, WindowsFirewall,
WMI, WMIEventConsumer, WMIEventFilter, WMIFilterBinding,
WSUS

"Seatbelt.exe -group=slack" runs the following commands:

SlackDownloads, SlackPresence, SlackWorkspaces

"Seatbelt.exe -group=chromium" runs the following commands:

ChromiumBookmarks, ChromiumHistory, ChromiumPresence
```

"Seatbelt.exe -group=remote" runs the following commands:

```
AMSIProviders, AntiVirus, AuditPolicyRegistry, ChromiumPresence, CloudCredentials,
DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables,
ExplicitLogonEvents, ExplorerRunCommands, FileZilla, Hotfixes,
InterestingProcesses, KeePass, LastShutdown, LocalGroups,
LocalUsers, LogonEvents, LogonSessions, LSASettings,
MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings,
OptionalFeatures, OSInfo, PoweredOnEvents, PowerShell,
ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessions,
RDPSavedConnections, RDPsessions, RDPsettings, Sysmon,
WindowsDefender, WindowsEventForwarding, WindowsFirewall
```

"Seatbelt.exe -group=misc" runs the following commands:

```
ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo, FirefoxHistory,
InstalledProducts, InterestingFiles, LogonEvents, LOLBAS,
McAfeeSiteList, MicrosoftUpdates, OutlookDownloads, PowerShellEvents,
Printers, ProcessCreationEvents, ProcessOwners, RecycleBin,
reg, RPCMappedEndpoints, ScheduledTasks, SearchIndex,
SecurityPackages, SysmonEvents
```

<https://trustedsec.com/blog/walking-the-tightrope-maximizing-information-gathering-while-avoiding-detection-for-red-teams>

---

Revision #6

Created 10 March 2023 23:12:07 by

Updated 15 May 2024 03:16:25 by unknown