CYBERSECURITY

ENUMERATION: WINDOWS SIDS

SIDS = USERS & GROUPS

Logon to your local computer.

Find and download the “user2sid” and “sid2user” tools.

Also download the PSTools from Microsoft.

Try to retrieve the SID for your useraccount and check the SID with the tools:

What information do you learn from the SID structure?

Use the “net users” c ommand = lists local users.

Use the user2sid to check which user is the local administrator:

Use the wmic command: wmic useraccount get name

Do you see more information?

```
If powershell has been installed, use: Get-LocalUser
```

Do you see more information?

Type “net localgroup” and check which localgroups are present on your machine.

The “net localgroup “groupname”” lets you enumerate the members.

The “net user “username”” lists the groups that the user is a member of and some extra information

This might give clues as to which applications are installed and can be exploited. Or you can check which accounts are interesting to concentrate on regarding a hack.

Further exploration:

- Check the normal user interfaces based user administration tools (if possible)
- Install an advanced tool for user-enumeration & administration (hyena). With these tools sometimes a lot of information can be retrieved without being an administrator. See Hyena screenshot below:

DOMAINS AND WORKGROUPS

Type “net view”.

Do you only see your local machine, or is extra information retrieved?

SHARES

What are you sharing on your windows machine?

Type the “net share” command.

The IPC$ share is used for “null session” communication. Do you see it?

Are there other shares?

What’s the $ sign used for behind the sharenames?

NETBIOS

If a machine runs (the older protocol) of NETBIOS, much information can be obtained:

Run “nbtstat -A IP-address target”

Test if any machines from your collegues have netbios enabled.

Perform a “nbtstat -?” and check/test the available options.

PORTS

Use the “netstat -a” command to check which ports on your machine are open on which IP addresses.

Would you expect all these entries to be there?

Check and experiment with the other options of netstat.