JAVELIN

11

Commands for Corporate Domain Compromise

What is so special about these commands?

Once inside a network, attackers disguise themselves as normal, authenticated users. This ensures they won’t be detected during any reconnaissance or lateral movement activities.

The commands listed in this brochure are native queries to the Active Directory (no binaries or malicious code). Once completed, they return information about any and all resources inside, including: users, servers, applications, identities, and naming conventions. With this information, attackers then assemble their plan to move laterally and ultimately steal data, encrypt computers, or sabotage the organization.

I.

Fundamental Reconnaissance

1.
```
whoami
```
Tells us which user we are authenticated as

2.
```
gpresult
```
Gives us the effective user permissions and the group policies enabled of the account

3.
```
nltest /dclist:domain.demo
```
Lists all Domain Controllers

4.
```
[System.DirectoryServices.ActiveDirectory Forest]::GetCurrent Forest().Sites | select Name, Subnets
```
Shows us the Subnets of the network

II.

Servers, Computers & Applications Reconnaissance

5.
```
net group “domain computers” / domain
```
Gives us a full list of all the workstations and servers joined to the domain

6.
```
([adsisearcher]”(&(objectClass=Computer)(name=**))”).FindAll().properties
```
Gives us all attributes associated with a particular computer

7.
```
([adsisearcher]”(&(objectClass=Computer)(servicePrincipalName=*X*))”).FindAll()
```
Enumerates all of the computers and servers in the domain that are running X application (dfs, MSSQL)

III.

Identities, Credentials & Privileged Users Reconnaissance

8

```
net group “domain admins” / domain
```

Gives us a list of the designated administrators joined to the domain

9

```
([adsisearcher]”(&(objectClass=person)(objectClass=User)(admincount=1))”).FindAll()
```

Filters for all privileged accounts

10

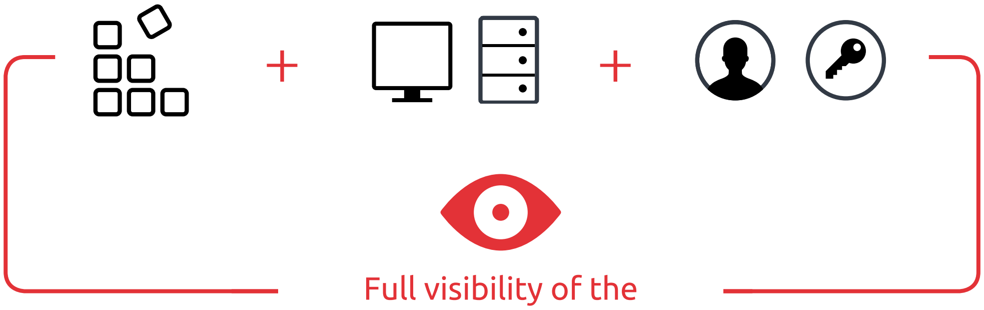
```
([adsisearcher]”(&(objectClass=person)(objectClass=User)(name=**))”).FindAll().properties
```

Gives us all attributes associated with a particular user

11

```
([adsisearcher]”(&(objectClass=User)(primarygroupid=513(servicePrincipalName=*))”).FindAll() | ForEach-Object { "Name: $($_.properties.name)""SPN: $($_.properties.serviceprincipalname)""Path: $($_.Path)"""}
```

Enumerates all of the crackable service accounts



Full visibility of the Corporate Domain

Note: this list is in no way comprehensive of all commands. If you want more information, please contact us.

About Javelin

Javelin is the first and only company to provide a comprehensive defense solution for the entire Corporate Domain.

Javelin's revolutionary agentless solution immediately contains attackers after they compromise a machine, preventing them from using Active Directory credentials and moving laterally into the network. Javelin greatly reduces the effort, time, and error involved in detecting and containing a breach.

For more information about how Javelin protects Corporate Domain environments, visit: **javelin-networks.com**

99.34%

Detection on the
first attacker move