iSSH v. Auditd: Intrusion Detection in High Performance Computing

Computer System, Cluster, and Networking Summer Institute
David Karns, New Mexico State University
Katy Protin, The University of North Carolina at Chapel Hill
Justin Wolf, California State University, San Bernardino

Mentors:
Alex Malin, HPC-DO
Graham Van Heule, HPC-3
Jim Williams, HPC-3

Instructor: Dane Gardner, NMC

LA-UR-12-23588

Introduction

- Goal: To provide insight into intrusions in high performance computing, focusing on tracking intruders' motions through the system
- The current tools, such as pattern matching, do not provide sufficient tracking capabilities
- We tested two tools: an instrumented version of SSH (iSSH) and Linux Auditing Framework (Auditd)
- Questions:
  - How is each tool implemented?
  - Which is more effective?
  - How do they affect computer performance?

LA-UR-12-23588

Set Up

- Our head node had CentOS 6.2 installed
  - This was where the all of the logs were sent to.
  - For iSSH, this was where the logs were analyzed and turned into Bro events.
- Our child nodes had CentOS 5.3 installed
  - We had 7 child nodes, which were configured as clients to our server, the head node.
  - Installing an older operating system gave us a less secure environment, which was easier to attack
  - It also led to some configuration problems throughout our project.

LA-UR-12-23588

Methods

- Installed and configured each tool
- Modified these tools so that they would catch more types of suspicious behavior
- Tested each tool by attacking our computer cluster, then modifying again.
- Our attack methods were mainly root privilege escalation attacks.

LA-UR-12-23588

iSSH

- **I**nstrumented **S**ecure **Sh**ell: a version of SSH developed at Lawrence Berkeley National Laboratory
- Goal: To audit user activity within a computer system to increase security.
- Capabilities:
  - Keystroke logging
  - Records user names and authentication information
  - Catching suspicious remote and local commands

LA-UR-12-23588

iSSH Set Up

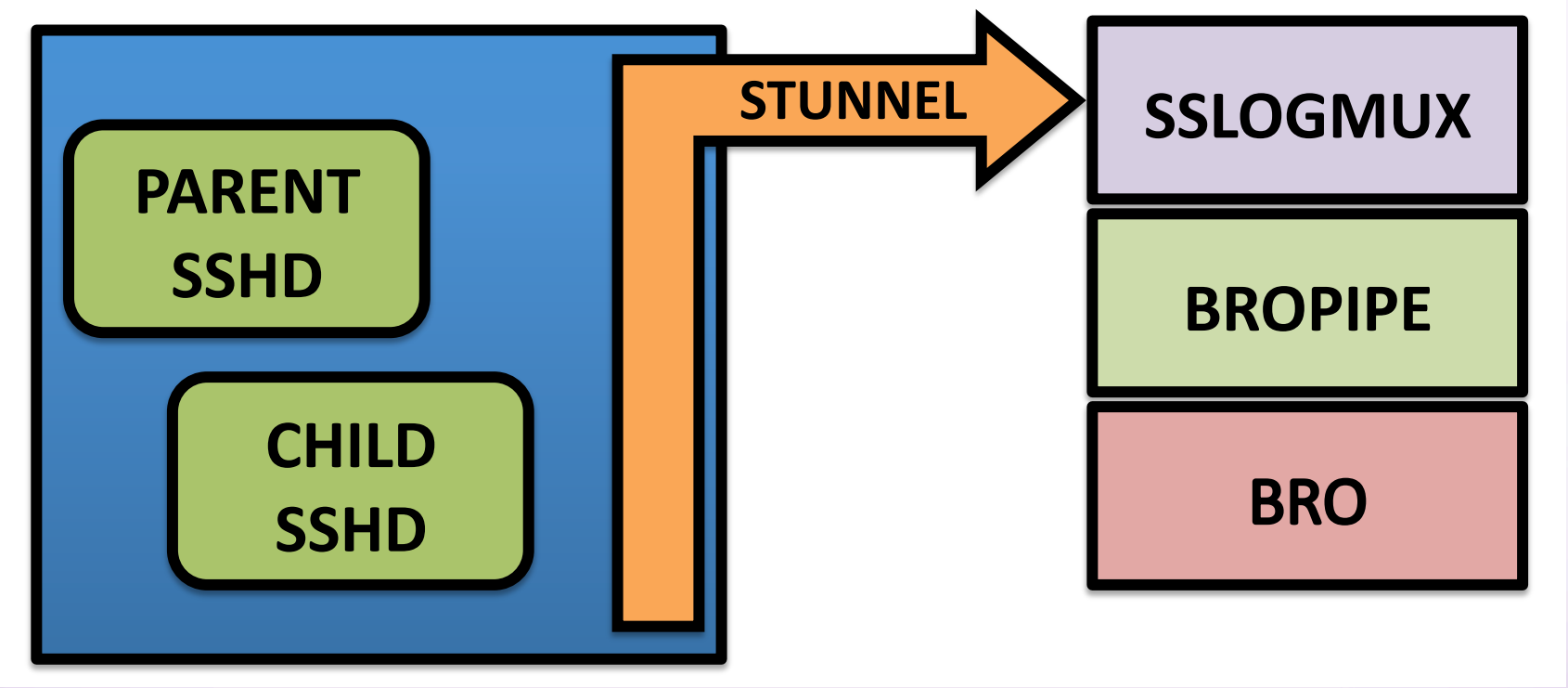


Photo from Scott Campbell's presentation "Local System Security via SSHD Instrumentation," 2011

Our Modifications

- Changing the alert level in Bro so that we received emails when:
  - A suspicious command was executed locally or remotely
  - The suspicious command threshold was passed
  - An unauthorized user attempts to access the system
- Adding commands to the list of suspicious commands: useradd, mkdir, nc, chmod
- Experimenting with the suspicious command threshold– default is 5.

Session Capture

sshd_connection_start_3 time=1343415761.842463
uristring=NMOD_3.08 uristring=0%3Achildnode02.localdomain
%3A2222 count=1444771597 uristring=127.0.0.1_10.0.2.13
addr=127.0.0.1 port=52966/tcp addr=:: **port=2222**/tcp count=0

auth_key_fingerprint_3 time=1343415762.2678
uristring=NMOD_3.08 uristring=0%3Achildnode02.localdomain
%3A2222 count=1444771597 uristring=fd
%3Ae3%3A05%3A16%3A38%3A6f%3A64%3A1f%3A2e%3A26%3A62%3A3e
%3A56%3A23%3A70%3A49 uristring=**RSA**

auth_info_3 time=1343415762.2927 uristring=NMOD_3.08
uristring=0%3Achildnode02.localdomain%3A2222
count=1444771597 uristring=**Accepted** uristring=**katy.protin**
uristring=publickey addr=127.0.0.1 port=52966/tcp addr=::
port=2222/tcp

session_new_3 time=1343415762.4036 uristring=NMOD_3.08
uristring=0%3Achildnode02.localdomain%3A2222
count=1444771597 int=32693 uristring=SSH2

Session Capture

```
channel_data_client_3 time=1343415766.864231 uristring=NMOD_3.08
uristring=0%3Achildnode02.localdomain%3A2222 count=1444771597
count=0 uristring=ls

channel_data_server_3 time=1343415766.873287 uristring=NMOD_3.08
uristring=0%3Achildnode02.localdomain%3A2222 count=1444771597
count=0 uristring=%0Abro-1.5.3.tar.gz++netperf-2.6.0.tar.gz
%09node1_backup.tgz

channel_data_client_3 time=1343415768.653347 uristring=NMOD_3.08
uristring=0%3Achildnode02.localdomain%3A2222 count=1444771597
count=0 uristring=exit

session_exit_3 time=1343415768.654962 uristring=NMOD_3.08
uristring=0%3Achildnode02.localdomain%3A2222 count=1444771597
count=0 count=32690 count=0

sshd_connection_end_3 time=1343415768.655196 uristring=NMOD_3.08
uristring=0%3Achildnode02.localdomain%3A2222 count=1444771597
addr=127.0.0.1 port=52966/tcp addr=:: port=2222/tcp
```

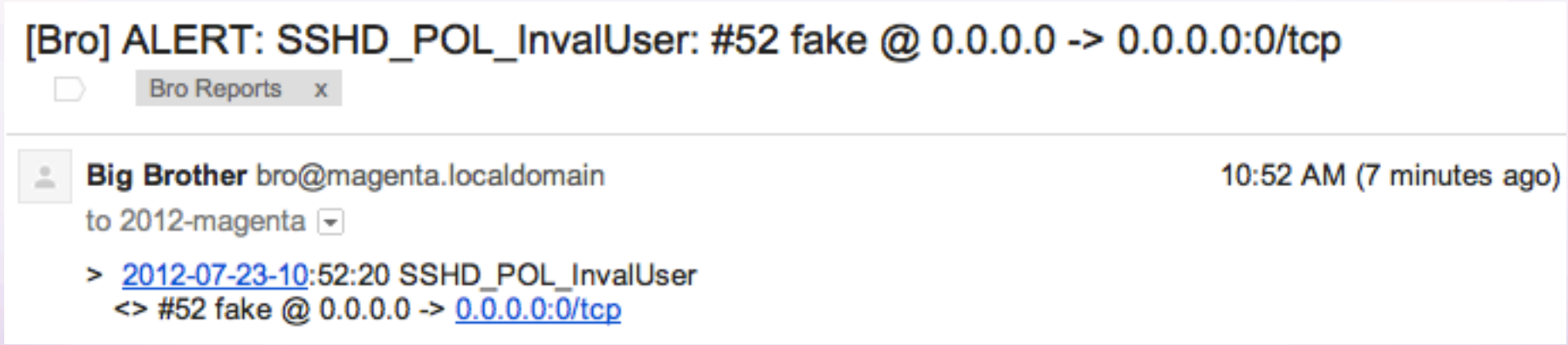
Example: Invalid User

- The attacker types `ssh -p 2222 fake@localhost` to attempt to login to the system.
- This action is recorded by iSSH, then encrypted and sent through Stunnel.
- Once it reaches the head node, this data is decrypted by the SSLLogMux, and sent to Bro through the bropipe.
- In the Bro logs, this event looks like:

```
1343070435.563349 #4 - childnode02.localdomain
1668641255 INVALID_USER  0.0.0.0:0/tcp >
0.0.0.0 @ 0/tcp:fake
```

Example: Invalid User

- In the Bro policy files, Bro is configured to send an email when an invalid user attempts to login:



Analyzing iSSH

Strengths

- Good for keystroke logging, making it easier to track malicious users by catching suspicious commands
- Works with Bro to send alerts; could be configured to send pages to systems administrators
- Creates visibility into SSH sessions

Weaknesses

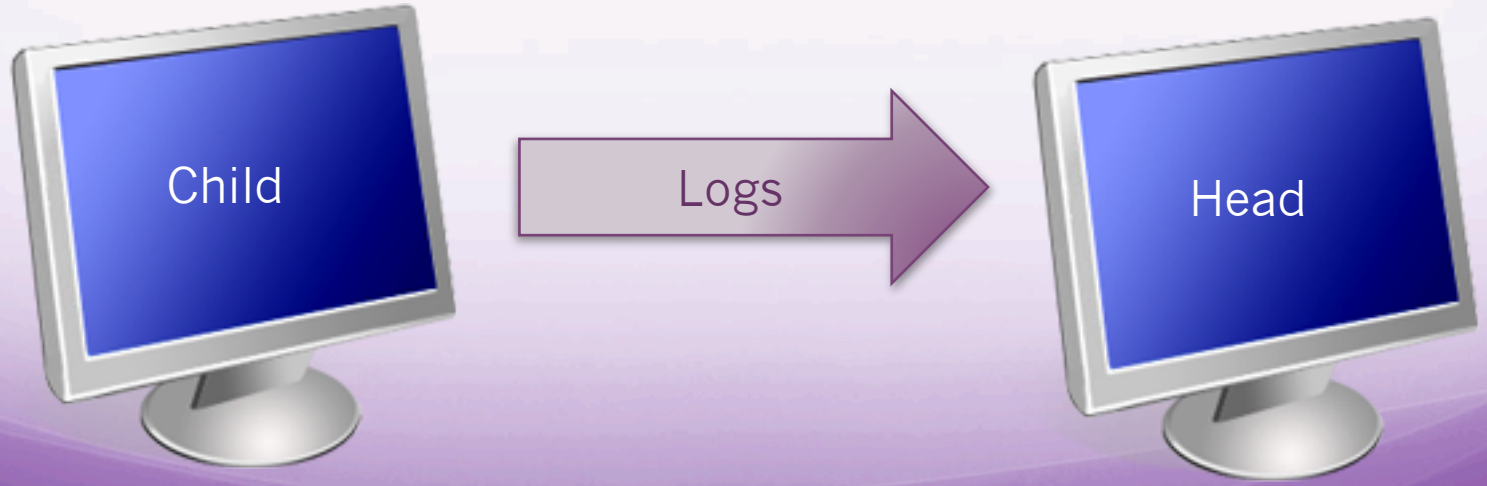
- Relatively new, so not very well documented
- No capabilities to see if files have been edited, moved, or copied within the system

Auditd

- The user component of the Linux Auditing System
- Creates logs of user behavior
- Monitors systems calls and file accesses
- Goal: Improve system security by keeping track of users' actions within the system

Auditd Setup

- Auditd was installed on each of the nodes
- Each of the child nodes sent their logs to the head node for easier observation
- We modified it by adding rules to record and monitor different user behaviors.



LA-UR-12-23588

Example: Permissions Change

- An attacker is on a child node. They want to gain access to the /etc/sudoers file, which contains a list of users with root privileges.
- If the permissions were set up correctly, they won't be able to write to the file.
- A well-meaning user types `chmod 777 /etc/sudoers`, allowing anyone to read from, write to, or execute this file
- The Auditd logs pick up this action

Example: Permission Changes

- The child node log is forwarded to the head node:

```
Jul 24 11:31:42 childnode04 audispd:
node=childnode04.localdomain type=SYSCALL
msg=audit(1343151102.258:3810): arch=c000003e syscall=90
success=yes exit=0 a0=1cd980b0 a1=1ff a2=1ff a3=1ff items=1
ppid=8025 pid=8042 auid=502 uid=0 gid=0 euid=0 suid=0
fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=489 comm="chmod"
exe="/bin/chmod" subj=user_u:system_r:unconfined_t:s0
key="perm_mod"

Jul 24 11:31:42 childnode04 audispd:
node=childnode04.localdomain type=CWD
msg=audit(1343151102.258:3810):  cwd="/home/david.karns"

Jul 24 11:31:42 childnode04 audispd:
node=childnode04.localdomain type=PATH
msg=audit(1343151102.258:3810): item=0 name="/etc/sudoers"
inode=47056695 dev=fd:00 mode=0100440 ouid=0 ogid=0
rdev=00:00 obj=system_u:object_r:etc_t:s0
```

Analyzing Auditd

Strengths

- Very thorough logs
- Wider variety of tracking abilities than iSSH
- Older, so better documented

Weaknesses

- Logs record everything, not just malicious behavior
- The size of the logs can lead to overflowing directories
- This level of logging leads to a lot of false alarms

LA-UR-12-23588

Attacking Methods

- Root privilege escalation:
  - We assume that the hacker has access to the system, but is trying to gain root privileges, which are normally only given to systems administrators.
  - This allows them to modify files and perform commands that regular users cannot.
- Taking advantage of improper file permissions and operating system vulnerabilities

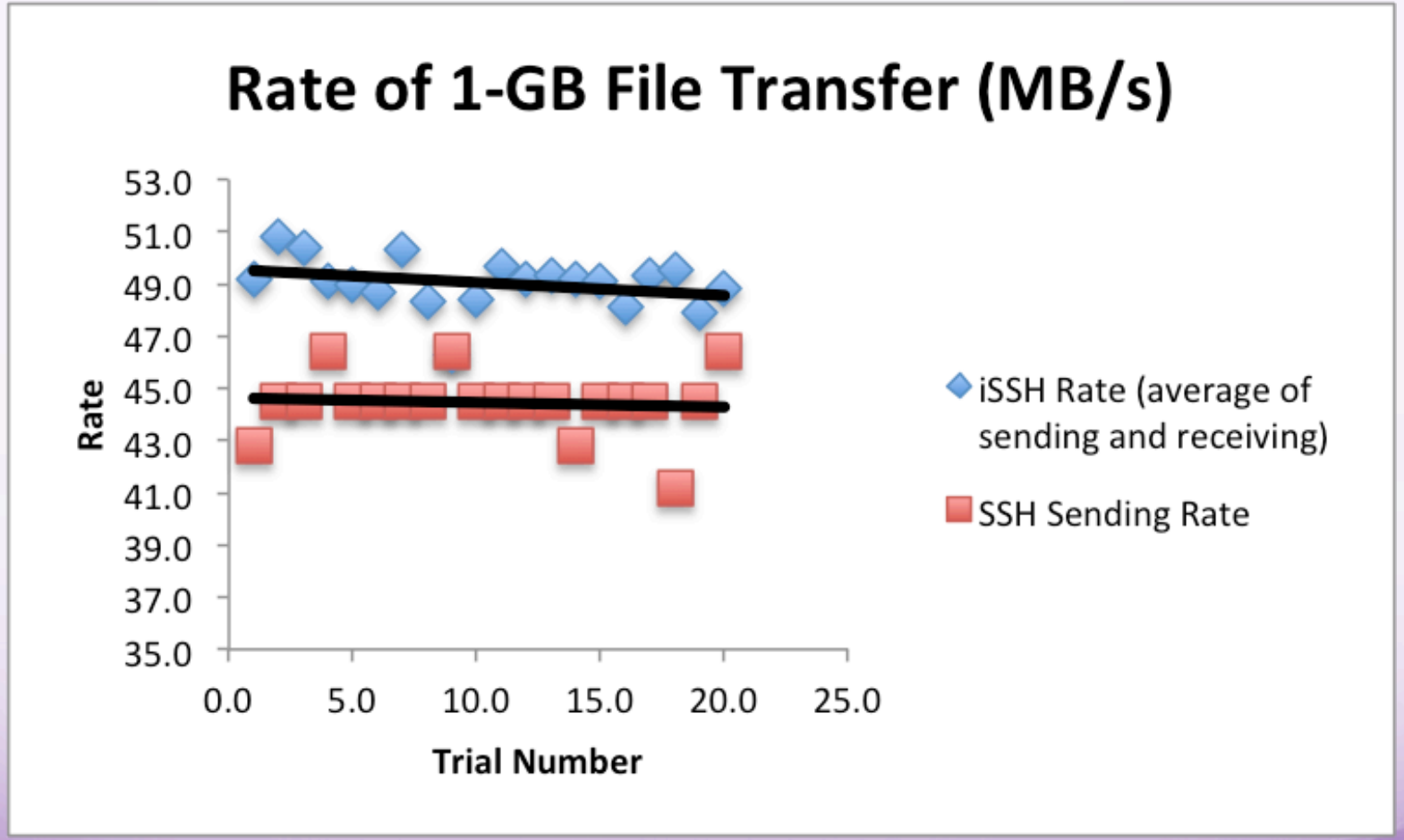
Example Attack

- Once on the system, the attacker goes into the cron.hourly directory
- Seeing that the file permissions on a file here are writable by everyone, he adds

```
echo ‘John     ALL=(ALL)          ALL’ >> /etc/sudoers
```

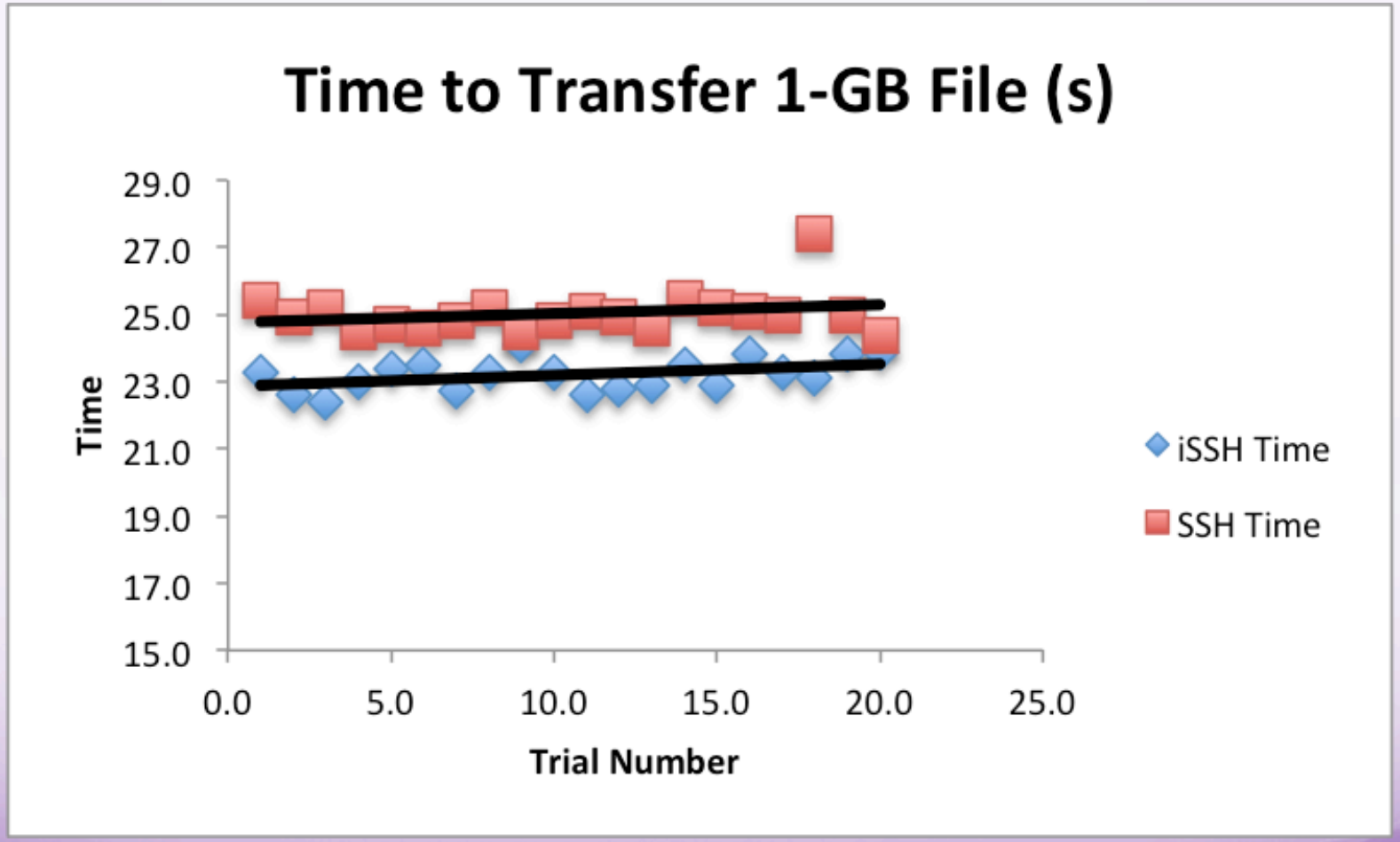
- He also copies the /etc/password and /etc/shadow files to his own computer

Performance Testing: File Transfer Test



LA-UR-12-23588

Performance Testing: File Transfer Test



Performance Testing: Networking Tests

	TCP Throughput While Idle(Mb/s)		
	Control	iSSH	Auditd
Average	941.42	941.42	941.42
Standard Deviation	0.0	0.0	0.0

	UDP Receive Throughput While Idle (Mb/s)		
	Control	iSSH	Auditd
Average	958.63	961.105	961.6
Standard Deviation	2.1	0.3	0.0

Performance Testing: Network Tests

	TCP Throughput With User Activity (Mb/s)		
	Control	iSSH	Auditd
Average	941.41	941.15	941.41
Standard Deviation	0.0	0.1	0.0

	UDP Receive Throughput With User Activity (Mb/s)		
	Control	iSSH	Auditd
Average	961.18	959.13	960.64
Standard Deviation	0.5	0.8	0.6

Conclusions

- Auditd is better documented than iSSH, which would help administrators during set up and troubleshooting
- iSSH has a cleaner notification system, but the logs are not as detailed as Auditd
- From our performance testing:
  - File transfer speed using SCP is increased when using iSSH
  - Network benchmarks were roughly the same regardless of which tool was running.

LA-UR-12-23588

Future Work

- More performance testing
  - With iSSH, the creators also tested the speed of remotely executed commands.
  - Complete more extensive network tests
- Creating new events in iSSH
  - Should be possible because of Bro
- Modifying Auditd so that it had an alarm system or enabling some other way to simplify sorting through the logs

Any questions?

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

NM STATE UNIVERSITY

CALIFORNIA STATE UNIVERSITY SAN BERNARDINO

Los Alamos NATIONAL LABORATORY EST.1943

New Mexico CONSORTIUM

PRObE Parallel Reconfigurable Observational Environment

NSF

ISTI INFORMATION SCIENCE & TECHNOLOGY INSTITUTE

LA-UR-12-23588