Privilege Escalation

Baseline, Monitor, Detect, Analyze, Respond, & Recover

Based on SROC class given by Hervey Allen, Chris Evans, and Phil Regnauld 2009 Santiago, Chile

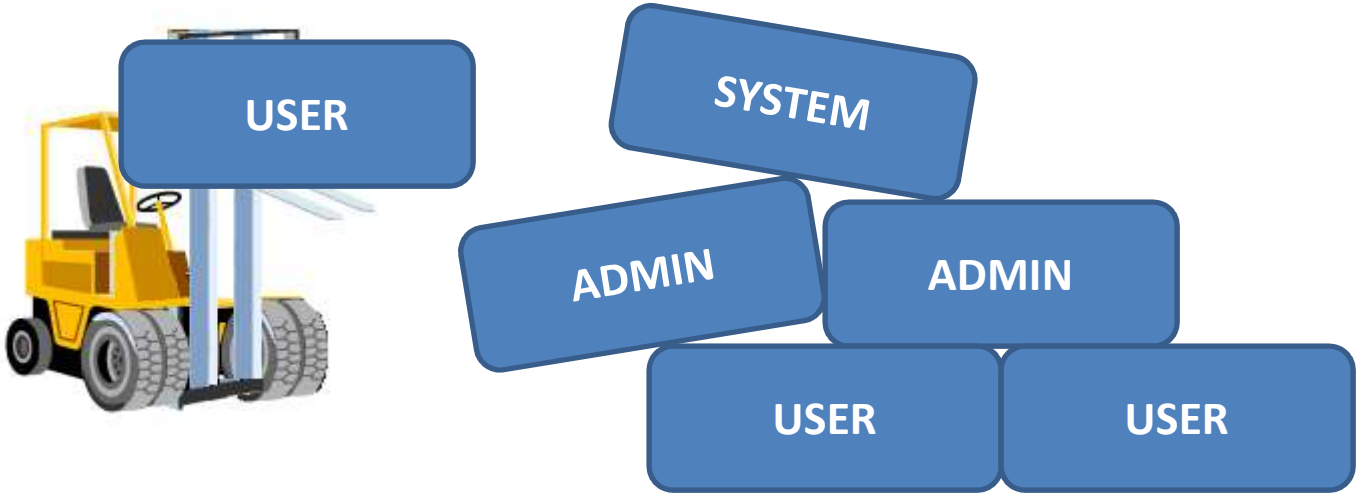
Network Startup Resource Center

Overview

- Privilege Escalation
  - Concepts, Examples, Motivations
- Hands-on Cyber Attack
  - Concept
  - Establishing a Baseline
  - Demonstration of the Attack
  - Monitoring & Detection
  - Analyzing the Attack
  - Response & Recovery
  - Enacting Mitigation Actions

Privilege Escalation

- Privilege Escalation is the act of obtaining credentials (usernames, passwords, key files, etc), beyond what is normally available to them, for the purpose of accessing systems or information.



Privilege Escalation

Some Examples:

- Username / Password Brute Forcing – try combinations of usernames and passwords until a working set is found
- Keystroke Loggers – installation of programs to capture keyboard input, with the purpose of finding usernames and passwords
- Social Engineering – eliciting information directly from personnel
- Exploits - Buffer overflows, impersonation, or other technical attacks against an operating system or application

Privilege Escalation

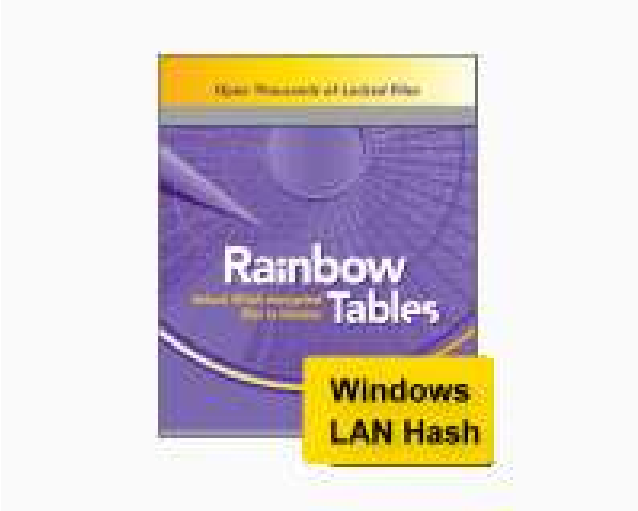
- Username / Password Guessing Requires 3 Pieces of Information:
  - An IP Address, Application, or other “Target”
  - A Username
  - A Password
- This is not so difficult for the attacker:
  - She will usually know the target already (2 pieces left)
  - She can usually guess the username (root , admin, or administrator – 1 piece left)
  - She only needs to guess the password

Privilege Escalation

- Attackers use what's called a "dictionary attack" to build lists of possible passwords from dictionary words
  - Password dictionaries include thousands of words, and exist for just about every language, including Klingon…
  - Some dictionaries or password crackers (e.g. John the Ripper) will improve standard dictionary words by making typical substitutions and creating another possible password (e.g. root become r00t and root!) – usually referred to as "hybrid"
  - There are also dictionaries for "keyboard progression" passwords (e.g. !QAZXSW@)

Privilege Escalation

- If the dictionary attack doesn't work, an attacker may try to brute force the password
  - This takes an incredibly long time assuming ideal conditions, but is guaranteed to work at some point (perhaps in 150 years!)
  - There are ways to speed this up (parallel attempts, pre-computed password hashes, etc)



http://www.h11-digital-forensics.com/images-pm/rainbow-table-1-medium.jpg

Privilege Escalation

- Keystroke Loggers are Commonly Available
- The hard part for the attacker is getting one installed and the captured keystrokes out
- They can be installed by:
  - Malware or trojans (“check out this new game”)
  - Social engineering (“please copy this document from my USB pen drive”)
  - Physical access (unlocked computer)
- Once running, they send the captured information out through the network, or store it for later pickup

Privilege Escalation

- Keystroke Loggers

http://keyghostkeylogger.com/KeyGhost-USB-Keylogger.jpg

Privilege Escalation

- Social Engineering is Usually Easy!
  - Doesn't require any technical tricks
  - People are often very friendly and helpful
- For example, "Hi I'm Bob from Registrar X – please validate your account for me"
- The lower threat to the attacker, the more likely they are to try it:
  - Emails are free
  - Phone calls can be traced, but "throw away" phones are available

Privilege Escalation

- More subtle social engineering attempts are “spear” phishing messages which look like the real thing

From: "networksolutions.com Tech Support" <customerservice@networksolutions.com>

Date: October 29, 2008 1:48:14 PM PDT

To: [redacted]

Subject: Attention: domain will be expired soon

Dear Network Solutions Customer,

This is a fraudulent email

We recently notified you that the registration period for your Network Solutions domain name had expired. As a benefit of having previously registered a domain name(s) with Network Solutions, you are eligible to receive a percentage of the net proceeds that were generated from the renewal and transfer of the domain name you chose not to renew. Since you have chosen not to renew the domain name listed below during the applicable grace period, we were successful in securing a backorder for this domain name on your behalf and it has been transferred to another party in accordance with the Service Agreement.

Renew your domain now - http://www.networksolutions.com <http://www.networksolutions.com.com42.asia>

You must click on the following link, enter your domain name, and confirm your contact information in order to claim these funds. If your contact information is not correct, you must enter Account Manager and make the appropriate changes prior to clicking "submit" from the confirmation screen. If you do not do this, you will be confirming inaccurate information and will not receive any payment. Checks will only be made payable and mailed to the Account Holder of record.

Sincerely,

Network Solutions© Customer Support

Privilege Escalation

- The Technical Tricks of Privilege Escalation are Many
  - See MetaSploit, Core's IMPACT, or milw0rm.com

- Operating Systems
- Applications
- Web Applications

- Buffer / Heap / Stack Overflows
- SQL Injection
- Remote & Local

Privilege Escalation

- Who Does Privilege Escalation:
  - Employees – “I want to see some else’s inbox”
  - Hackers – “I need the router password to shut it down”
  - Competitors – “I need Bob’s password to see his files”
- Motivations:
  - Access information or systems they wouldn’t normally have access to
  - Corporate espionage
  - Conduct larger cyber attack

Privilege Escalation

- Why are these attacks important to you?
  - Violates the security policy of your system and allows people access they wouldn't normally have
  - Potentially compromise sensitive information
  - Potentially provide access for malicious attacks
- These attacks usually follow enumeration, as the attacker has found an "interesting" system and wants to access it
- These attacks may affect your network
  - Technical exploits are often unstable, causing seemingly random operating system or application crashes

Privilege Escalation

Cyber Attack
- SSH Brute Forcing -

- While we have chosen SSH to demonstrate this type of attack, there are many, many vectors for conducting brute force attacks.

- Any externally visible server or application which accepts a username / password is vulnerable to this type of attack
  - SSH, Telnet, SCP, FTP, etc
  - Microsoft Terminal Services, VNC, other Remote Desktops
  - Web Applications

Privilege Escalation Cyber Attack – SSH

- Administrators frequently access systems via SSH to perform maintenance, monitor their systems…
  - SSH is an excellent replacement for TELNET, but is still susceptible to attack (its more difficult).
- Some administrators allow remote access to SSH so they can perform their administrative duties while on the road or from home

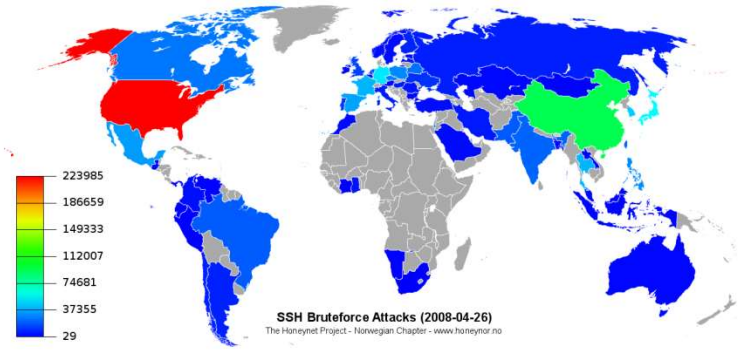
Privilege Escalation Cyber Attack – SSH

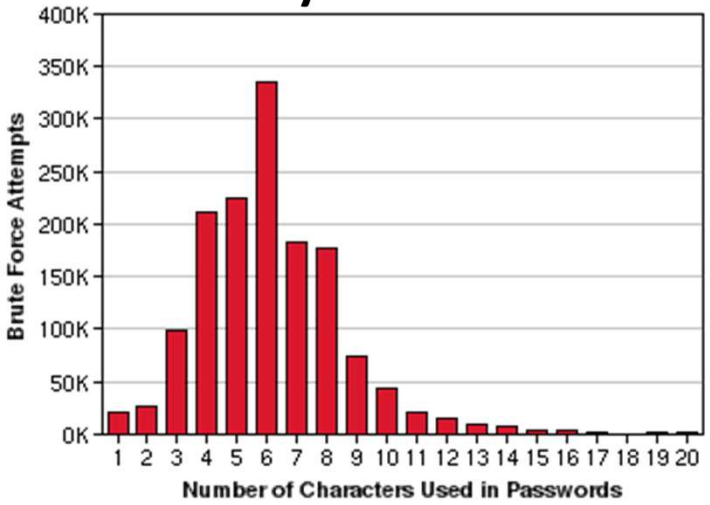
- Malicious actors might target SSH servers:
  - Because they are remotely accessible
  - Attempt to brute force a username / password
- Why?
  - Establish remote access
  - Find credentials they wouldn't normally have

Privilege Escalation Cyber Attack – SSH

- Recall the components needed for this attack
  - Target IP address, Username, Password

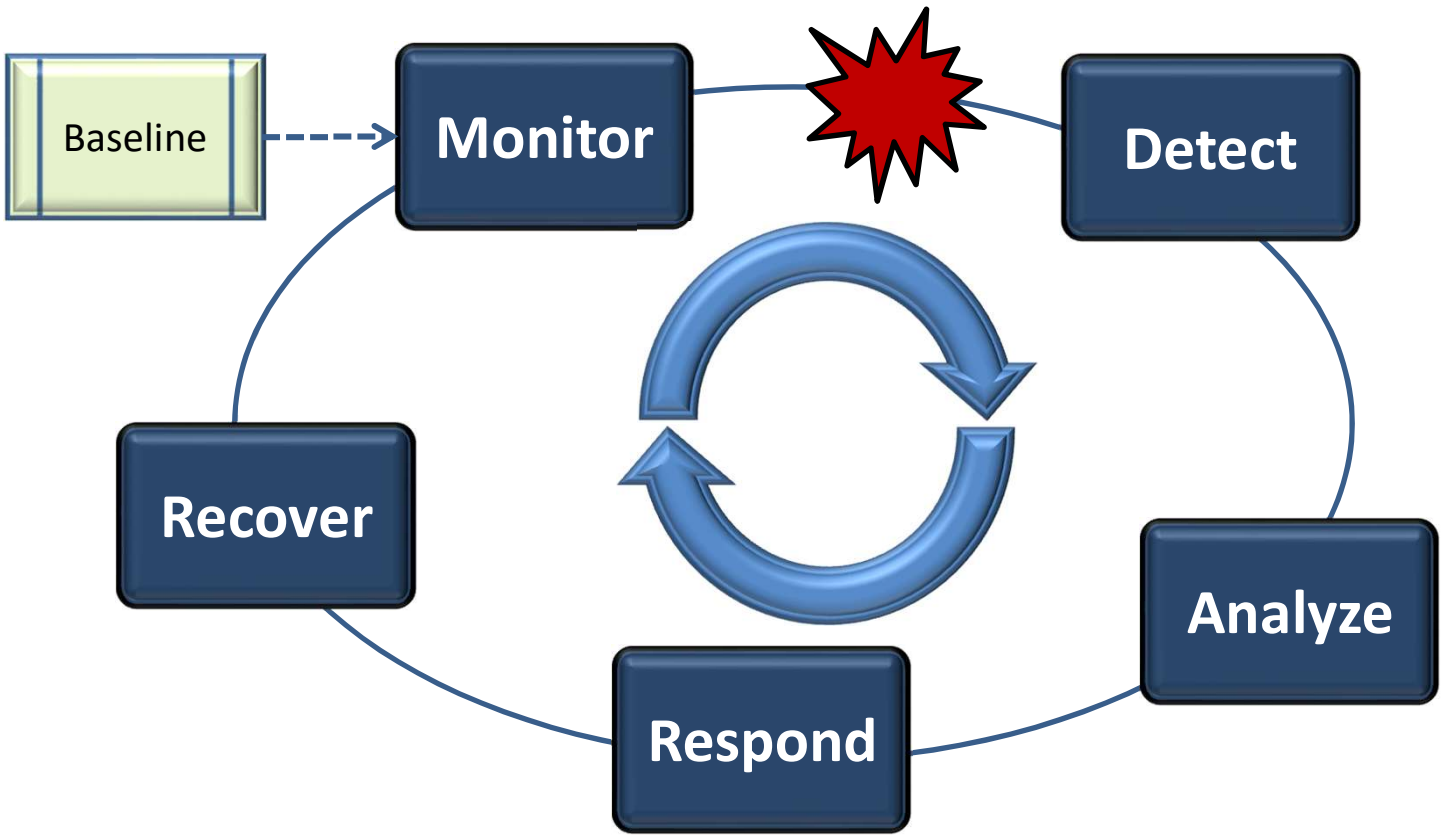
- We will try various username / password combinations on your externally visible SSH server





Privilege Escalation Cyber Attack – SSH

- Recall Our Secure Operations Framework



Privilege Escalation Cyber Attack – SSH

- Establish a Baseline for What's Normal for Your Network:
  - Who would connect via SSH to your servers? (username)
  - Where would they connect from? (source IP)
  - When would they do it? (time)

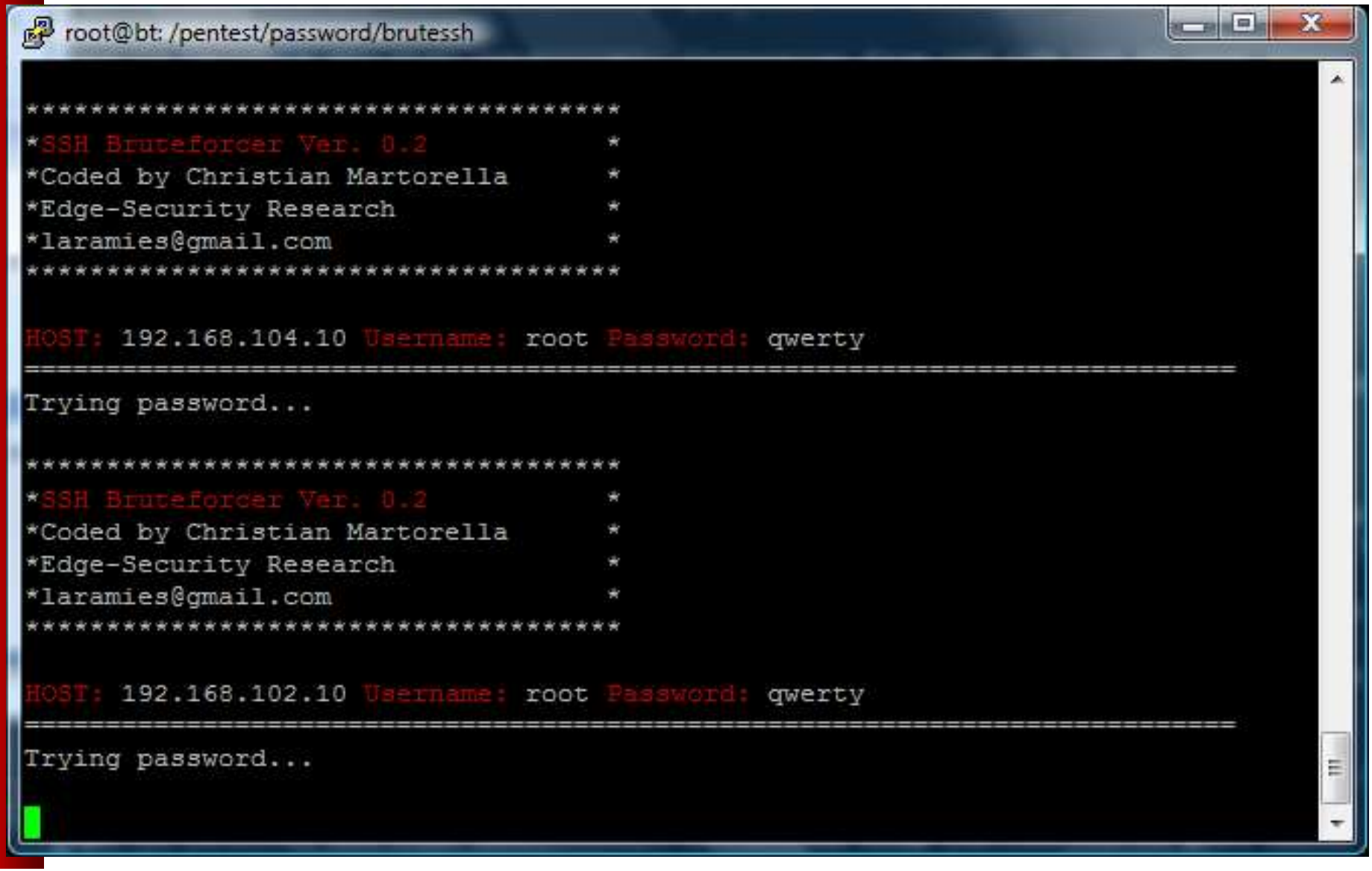
- Use this baseline to compare what you currently see to what you expect
  - Any differences are an indication of something going on!

Privilege Escalation Cyber Attack – SSH

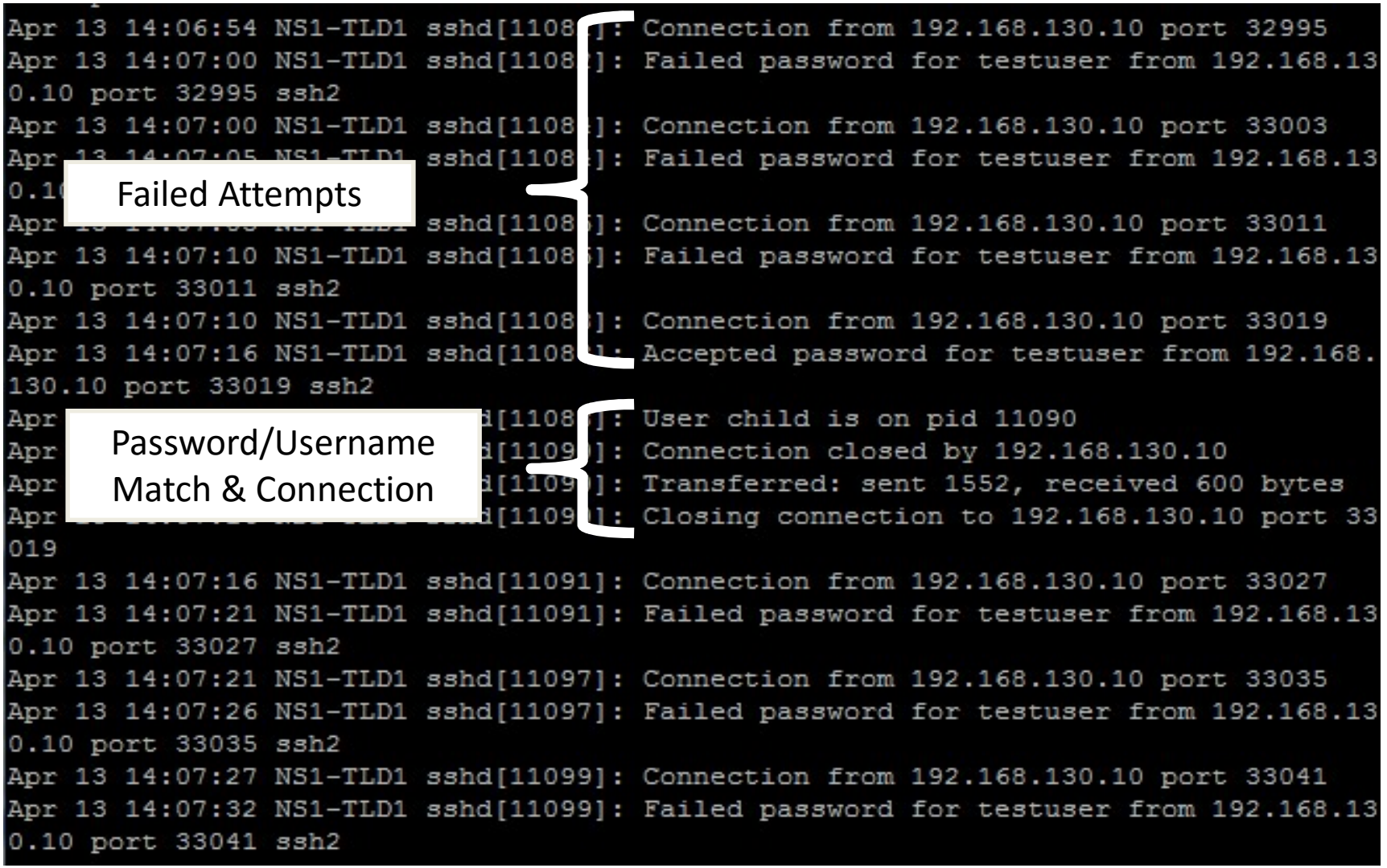
Tail –n 40 –f /var/log/auth.log

Attack Demonstration

SSH Brute Force Attack



SSH Brute Force Attack




```
Apr 13 14:06:54 NS1-TLD1 sshd[1108 ]: Connection from 192.168.130.10 port 32995
Apr 13 14:07:00 NS1-TLD1 sshd[1108 ]: Failed password for testuser from 192.168.13
0.10 port 32995 ssh2
Apr 13 14:07:00 NS1-TLD1 sshd[1108 ]: Connection from 192.168.130.10 port 33003
Apr 13 14:07:05 NS1-TLD1 sshd[1108 ]: Failed password for testuser from 192.168.13
0.10
Apr 13 14:07:10 NS1-TLD1 sshd[1108 ]: Connection from 192.168.130.10 port 33011
Apr 13 14:07:10 NS1-TLD1 sshd[1108 ]: Failed password for testuser from 192.168.13
0.10 port 33011 ssh2
Apr 13 14:07:10 NS1-TLD1 sshd[1108 ]: Connection from 192.168.130.10 port 33019
Apr 13 14:07:16 NS1-TLD1 sshd[1108 ]: Accepted password for testuser from 192.168.
130.10 port 33019 ssh2
Apr 13 14:07:16 NS1-TLD1 sshd[1108 ]: User child is on pid 11090
Apr 13 14:07:16 NS1-TLD1 sshd[1109 ]: Connection closed by 192.168.130.10
Apr 13 14:07:16 NS1-TLD1 sshd[1109 ]: Transferred: sent 1552, received 600 bytes
Apr 13 14:07:16 NS1-TLD1 sshd[1109 ]: Closing connection to 192.168.130.10 port 33
019
Apr 13 14:07:16 NS1-TLD1 sshd[11091]: Connection from 192.168.130.10 port 33027
Apr 13 14:07:21 NS1-TLD1 sshd[11091]: Failed password for testuser from 192.168.13
0.10 port 33027 ssh2
Apr 13 14:07:21 NS1-TLD1 sshd[11097]: Connection from 192.168.130.10 port 33035
Apr 13 14:07:26 NS1-TLD1 sshd[11097]: Failed password for testuser from 192.168.13
0.10 port 33035 ssh2
Apr 13 14:07:27 NS1-TLD1 sshd[11099]: Connection from 192.168.130.10 port 33041
Apr 13 14:07:32 NS1-TLD1 sshd[11099]: Failed password for testuser from 192.168.13
0.10 port 33041 ssh2
```

Privilege Escalation Cyber Attack – SSH

- Monitoring & Detection
  - Configure your network to detect SSH login attempts
  - Monitor your detection tool(s)
  - Establish a Baseline

Privilege Escalation Cyber Attack – SSH

Attack Demonstration

(This time you can see how your network views the attack)

Privilege Escalation Cyber Attack – SSH

- Analysis - what did your detection tools report? Is this really an attack?
  - SSH Server Logging
  - Log Analysis
- What usernames were attempted?
- Where is attack coming from?
- Did any of the attempts work?
  - You may have to correlate multiple sources of information to determine this:
  - Failed attempts & Successful Attempts
  - If you see many failed attempts and they stop – one of two things has happened – they gave up or it worked!

Privilege Escalation Cyber Attack – SSH

- Response Actions
  - aka “I’m Under Attack – What Do I Do Now?!”
  1) Prioritize – is anything else happening?
  2) Temporarily lock or deactivate the account being used
  3) Shut down SSH server
  4) Block source IPs at the firewall

- The action you take must depend on:
  - What you’re willing to do (firewall discipline)
  - What you’re willing to live without (shut down SSH)
  - What you can do quickly (deactivate an account)

Privilege Escalation Cyber Attack – SSH

- Recovery Actions
  - The attack is over – how do I prevent this again?
  1) Ask yourself “What _*could*_ have happened here?”
  2) Use Strong Passwords on Accounts
  3) “Whitelist” access to certain IPs
  4) Use Identity Key Files for SSH logins
  5) Restrict SSH access to specific accounts
  6) Configure Max Attempts in SSH
  7) Configure Firewall Settings as additional protection
     - See sshguard for more information
  8) Require VPN use

Privilege Escalation Cyber Attack – SSH

- What Other Mitigation Steps Would You Take?
  - What is appropriate for your network & resources?
  - Make the attacker's job as difficult as possible without affecting your ability to your job
    - If your network is difficult to crack, all but the dedicated hackers will move on to someone else!

Privilege Escalation Cyber Attack – SSH

- Enact Mitigation Actions
  - Secure your SSH Configuration

Privilege Escalation Cyber Attack – SSH

Final Attack Demonstration

Privilege Escalation Cyber Attack – SSH

- Attack Discussion
  - Did the mitigation steps help?
  - How else can you protect your network?
  - Remember the risk decision:
    - If the risk of remote access by an attacker is greater than the benefit of allowing your admins remote access – turn it off!
- Other Thoughts Before We Move On?

QUESTIONS?

- Do you have any questions about …
  - Privilege Escalation
  - Detecting This Type of Attack
  - Responding & Recovering From This Type of Attack