After the HR data breach from a few weeks ago, your CEO has been receiving increased advertisements from cyber insurance providers with numerous worst-case scenarios.  He is now worried that your team might not be able to act quickly and decisively to resolve any issues that may occur and this will affect the image of the company.   You issue an incident handling policy that answers the following questions:

1. Which units should have representation on the IRT?

Any company should set up incident response team. No matter what kind of company will meet the unpredictable incidences or disasters. So the IRT can minimize the loss of the company, and prevent the occurrence of the incidents. For the large organization, they need multiple IRTs to reduce these risks. Also in order to take in consideration , IRT team can create a good technical analysis report over regarding the incidents where it becomes bible for all people in the organization at critical situations rather to panic it is good to follow the food steps of IRT Team. How ever in IRT team, not only technical incidents would be taken in consideration but also effective in consideration we would have HR, Building, Construction related ideology as well.   
   
 As per the image provided, we would have these many department which would give inputs to IRT, and take output from IRT team for there situation, circumstances.   
  
  
 Fig: Taken from Textbook .

1. Why is centralization of resources in terms of corporate security necessary?  
     
   Yes , Definitely centralization of resources is always considered to necessary under the terms of corporate security as because of the below mentioned following reasons.

(1): Reduce the work that stuffs of security department to monitor the network.

(2): Promote a good communication and redundancy in analysis.

(3): Convenience for Security team to integrate all the tools and knowledge base to have a depth implementation of defense.

1. How is the Incident Response Plan going to work in the following stages?  
     
     
   Referred link: <http://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide>   
   1. Preparation: Laying down the infrastructure to resolve an incident when it occurs.

Yes, for this The arrangement improvement group ought to meet with the inward innovation group, application group, and system administrator(s) and set up the extent of the action, e.g., inside components, outside resources, outsider assets, linkages to different workplaces/customers/merchants; make sure to brief IT office senior administration on these gatherings so they are legitimately educated. At that point, Gather all applicable system foundation reports, e.g., organize outlines, gear designs, databases.

* 1. Analysis: Figuring out and documenting as much of the incident as possible.

Direct the business affect examination (BIA). The business affect examination recognizes and organize basic IT frameworks and segments.

* 1. Containment: Given the results of the analysis, determine what is the best way to process and remove any lingering effects of the incident.

Build up an IT alternate course of action. The emergency course of action ought to contain point by point direction and strategies for reestablishing a harmed framework.

* 1. Lessons learned: Apply the newfound knowledge to remediate any issues found during the process, going back to the preparation phase.

Arrange testing, preparing and working out. Testing the arrangement recognizes arranging holes, while preparing gets ready recuperation work force for plan actuation; both exercises enhance arrange viability and general office readiness.

Upkeep arrange. The arrangement ought to be a living report that is refreshed consistently to stay current with framework upgrades.

1. What are the reporting requirements in your State in case of a breach?

Referred links : 1. <http://www.in.gov/attorneygeneral/2874.htm>  
 2. <http://www.in.gov/attorneygeneral/3037.htm>  
  
The Security Breach Statute requires that the business notify:

(1) Affected consumers following discovery of the breach. The disclosure must be made without unreasonable delay and must be provided to the affected persons by one of the following methods: a) mailed written notice, b) telephone notification, c) Facsimile (fax), or d) electronic mail notice, if an email address is available.  
  
(2) Consumer reporting agencies if more than 1,000 Indiana residents are to be notified. The contact information for the three nationwide consumer reporting agencies is as follows:

* EQUIFAX  
  Equifax:  
  Consumer Fraud Division  
  P.O. Box 740256  
  Atlanta, GA 30374  
  800-525-6285  
  [security.dataadministration@equifax.com](mailto:security.dataadministration@equifax.com)
* EXPERIAN  
  Consumer Fraud Assistance  
  P.O. Box 9556  
  Allen, TX 75013  
  888-397-3742  
  [businessrecordsvictimassistance@experian.com](mailto:businessrecordsvictimassistance@experian.com)
* TRANSUNION  
  Consumer Relations & Fraud Victim Assistance  
  1561 E. Orangethorpe Ave.  
  Fullerton, CA 92831  
  Tel: 800-372-8391 fax: 714-680-7290  
  [FVAD@Transunion.com](mailto:FVAD@Transunion.com)

(3) The Attorney General’s office.  Failure to do so may result in penalties under the breach notification statute.  Use our security breach reporting form.  You can submit your breach notification to the Indiana Attorney General's Office by completing the printable Breach Notification Form and mailing or faxing the form to:

 Identity Theft Unit—Data Breach  
Attorney General of Indiana   
Indiana Government Center South, 5th Floor   
302 West Washington Street   
Indianapolis, IN 46204   
317-232-6201

If you receive a letter informing you personal information may have been compromised due to a security breach, don't panic. A security breach does not necessarily mean you will become a victim of identity theft. However, you are encouraged to follow the steps outlined below to reduce your risk of becoming an identity theft victim.

1. Determine what type of breach has occurred
2. Notify the credit bureaus and establish a fraud alert
3. Order your credit reports and review carefully
4. Consider a credit freeze
5. Continue to monitor your accounts, mail, and credit reports

## Research the protection offered by the top 3 cyber insurance providers; what tasks and areas you will need to cover in order to make cyber insurance unnecessary for your company? The cyber insurance:

* Available limits up to $500 million
* Coverages available include: Network Security Liability, Privacy Liability (Including Employee Privacy), Breach Response, Privacy Regulatory Defense, Fines and Penalties, Errors and Omissions, Forensics, Multimedia Liability, PCI Fines and Penalties, Network Business Interruption, Data Loss, Cyber Extortion and Cyber Terrorism
* Access to a 24/7 team of Incident Response experts
* Contractual indemnifications available
* Worldwide coverage
* Premium financing program available

We can use our IRT to do these works that including Network Security Liability, Privacy Liability (Including Employee Privacy), Breach Response, Privacy Regulatory Defense, Fines and Penalties, Errors and Omissions, Forensics, Multimedia Liability, PCI Fines and Penalties, Network Business Interruption, Data Loss, Cyber Extortion and Cyber Terrorism.

## Hands On Activity Class activity results: Fig: Scripts are been executed Fig: Results and output executed Log Analysis : [www.sunshine.edu/ossec](http://www.sunshine.edu/ossec) events list. Latest events

**2017 Apr 14 12:00:22** Rule Id: [533](http://www.ossec.net/wiki/index.php/Rule:533) level: 7  
**Location:** sunshine->netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort   
**Src IP**: utput: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
**Listened ports status (netstat) changed (new port opened or closed).**

tcp 0 0 [0.0.0.0:22](http://0.0.0.0:22) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:3306](http://0.0.0.0:3306) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:50456](http://0.0.0.0:50456) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:53](http://0.0.0.0:53) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:5672](http://0.0.0.0:5672) 0.0.0.0:\* LISTEN  
tcp 0 0 ::1:25 :::\* LISTEN  
tcp 0 0 :::111 :::\* LISTEN  
tcp 0 0 :::2121 :::\* LISTEN  
tcp 0 0 :::22 :::\* LISTEN  
tcp 0 0 :::48320 :::\* LISTEN  
tcp 0 0 :::53 :::\* LISTEN  
tcp 0 0 :::5672 :::\* LISTEN  
tcp 0 0 :::80  
Previous output:  
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
tcp 0 0 [0.0.0.0:111](http://0.0.0.0:111) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:22](http://0.0.0.0:22) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:3306](http://0.0.0.0:3306) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:50456](http://0.0.0.0:50456) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:53](http://0.0.0.0:53) 0.0.0.0:\* LISTEN  
tcp 0 0 [0.0.0.0:5672](http://0.0.0.0:5672) 0.0.0.0:\* LISTEN  
tcp 0 0 ::1:25 :::\* LISTEN  
tcp 0 0 :::111 :::\* LISTEN  
tcp 0 0 :::22 :::\* LISTEN  
tcp 0 0 :::48320 :::\* LISTEN  
tcp 0 0 :::53 :::\* LISTEN  
tcp 0 0 :::5672 :::\* LISTEN  
tcp 0 0 :::80 :::\* LISTEN

**2017 Apr 14 11:57:56** Rule Id: [5555](http://www.ossec.net/wiki/index.php/Rule:5555) level: 3  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:57:56 sunshine passwd: pam\_unix(passwd:chauthtok): password changed for r00t  
**User changed password.**

\*\* Alert 1492185476.99601: - pam,syslog,  
2017 Apr 14 11:57:56 sunshine->/var/log/secure  
Rule: 5502 (level 3) -> 'Login session closed.'  
Apr 14 11:57:56 sunshine sshd[3429]: pam\_unix(sshd:session): session closed for user root

**2017 Apr 14 11:57:54** Rule Id: [5501](http://www.ossec.net/wiki/index.php/Rule:5501) level: 3  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:57:53 sunshine sshd[3429]: pam\_unix(sshd:session): session opened for user root by (uid=0)  
**Login session opened.**

\*\* Alert 1492185476.98871: mail - syslog,elevation\_of\_privilege,  
2017 Apr 14 11:57:56 sunshine->/var/log/secure  
Rule: 40501 (level 15) -> 'Attacks followed by the addition of an user.'  
Apr 14 11:57:54 sunshine useradd[3449]: new user: name=r00t, UID=0, GID=100, home=/tmp/..., shell=/bin/bash  
Apr 14 11:57:53 sunshine sshd[3429]: Accepted keyboard-interactive/pam for root from ::1 port 36374 ssh2  
Apr 14 11:57:53 sunshine sshd[3429]: Accepted keyboard-interactive/pam for root from ::1 port 36374 ssh2

**2017 Apr 14 11:57:54** Rule Id: [40112](http://www.ossec.net/wiki/index.php/Rule:40112) level: 12  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**Multiple authentication failures followed by a success.**

Apr 14 11:57:53 sunshine sshd[3429]: Accepted keyboard-interactive/pam for root from ::1 port 36374 ssh2

**2017 Apr 14 11:57:52** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:57:52 sunshine sshd[3421]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185472.97960: mail - syslog,access\_control,authentication\_failed,  
2017 Apr 14 11:57:52 sunshine->/var/log/secure  
Rule: 2502 (level 10) -> 'User missed the password more than one time'  
Apr 14 11:57:52 sunshine sshd[3420]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:52** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:52 sunshine sshd[3420]: Failed password for root from ::1 port 36373 ssh2

**2017 Apr 14 11:57:50** Rule Id: [5720](http://www.ossec.net/wiki/index.php/Rule:5720) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**Multiple SSHD authentication failures.**

Apr 14 11:57:50 sunshine sshd[3420]: Failed password for root from ::1 port 36373 ssh2  
Apr 14 11:57:48 sunshine sshd[3420]: Failed password for root from ::1 port 36373 ssh2  
Apr 14 11:57:41 sunshine sshd[3409]: Failed password for root from ::1 port 36372 ssh2  
Apr 14 11:57:39 sunshine sshd[3409]: Failed password for root from ::1 port 36372 ssh2  
Apr 14 11:57:37 sunshine sshd[3409]: Failed password for root from ::1 port 36372 ssh2  
Apr 14 11:57:29 sunshine sshd[3400]: Failed password for root from ::1 port 36371 ssh2  
Apr 14 11:57:27 sunshine sshd[3400]: Failed password for root from ::1 port 36371 ssh2  
Apr 14 11:57:25 sunshine sshd[3400]: Failed password for root from ::1 port 36371 ssh2

**2017 Apr 14 11:57:50** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:48 sunshine sshd[3420]: Failed password for root from ::1 port 36373 ssh2

**2017 Apr 14 11:57:48** Rule Id: [5551](http://www.ossec.net/wiki/index.php/Rule:5551) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**Multiple failed logins in a small period of time.**

Apr 14 11:57:46 sunshine sshd[3420]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:44 sunshine sshd[3424]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:42 sunshine sshd[3423]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:41 sunshine sshd[3422]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:34 sunshine sshd[3409]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:32 sunshine sshd[3414]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:30 sunshine sshd[3412]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:29 sunshine sshd[3411]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:46** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:46 sunshine sshd[3420]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:46** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:44 sunshine sshd[3424]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:44** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:44 sunshine sshd[3420]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:42** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:42 sunshine sshd[3423]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:42** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:42 sunshine sshd[3420]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:42** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:41 sunshine sshd[3422]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:42** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:57:41 sunshine sshd[3410]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185462.92571: mail - syslog,access\_control,authentication\_failed,  
2017 Apr 14 11:57:42 sunshine->/var/log/secure  
Rule: 2502 (level 10) -> 'User missed the password more than one time'  
Apr 14 11:57:41 sunshine sshd[3409]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:42** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:41 sunshine sshd[3409]: Failed password for root from ::1 port 36372 ssh2

**2017 Apr 14 11:57:40** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:39 sunshine sshd[3409]: Failed password for root from ::1 port 36372 ssh2

**2017 Apr 14 11:57:38** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:37 sunshine sshd[3409]: Failed password for root from ::1 port 36372 ssh2

**2017 Apr 14 11:57:36** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:34 sunshine sshd[3409]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:36** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:34 sunshine sshd[3409]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:34** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:32 sunshine sshd[3414]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:34** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:32 sunshine sshd[3409]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:32** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:30 sunshine sshd[3412]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:32** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:30 sunshine sshd[3409]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:30** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:29 sunshine sshd[3411]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:30** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:57:29 sunshine sshd[3401]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185450.87738: mail - syslog,attacks,authentication\_failures,  
2017 Apr 14 11:57:30 sunshine->/var/log/secure  
Rule: 40111 (level 10) -> 'Multiple authentication failures.'  
Apr 14 11:57:29 sunshine sshd[3400]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:29 sunshine sshd[3401]: Disconnecting: Too many authentication failures for root  
Apr 14 11:57:17 sunshine sshd[3391]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:17 sunshine sshd[3392]: Disconnecting: Too many authentication failures for root  
Apr 14 11:57:05 sunshine sshd[3382]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:05 sunshine sshd[3383]: Disconnecting: Too many authentication failures for root  
Apr 14 11:56:51 sunshine sshd[3373]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:51 sunshine sshd[3374]: Disconnecting: Too many authentication failures for root  
Apr 14 11:56:40 sunshine sshd[3363]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:40 sunshine sshd[3364]: Disconnecting: Too many authentication failures for root  
Apr 14 11:56:28 sunshine sshd[3349]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:30** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:29 sunshine sshd[3400]: Failed password for root from ::1 port 36371 ssh2

**2017 Apr 14 11:57:28** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:27 sunshine sshd[3400]: Failed password for root from ::1 port 36371 ssh2

**2017 Apr 14 11:57:26** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:25 sunshine sshd[3400]: Failed password for root from ::1 port 36371 ssh2

**2017 Apr 14 11:57:24** Rule Id: [5551](http://www.ossec.net/wiki/index.php/Rule:5551) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**Multiple failed logins in a small period of time.**

Apr 14 11:57:23 sunshine sshd[3400]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:21 sunshine sshd[3404]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:19 sunshine sshd[3403]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:17 sunshine sshd[3402]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:12 sunshine sshd[3391]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:09 sunshine sshd[3395]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:07 sunshine sshd[3394]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:57:06 sunshine sshd[3393]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:24** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:23 sunshine sshd[3400]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:22** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:21 sunshine sshd[3404]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:22** Rule Id: [5720](http://www.ossec.net/wiki/index.php/Rule:5720) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**Multiple SSHD authentication failures.**

Apr 14 11:57:21 sunshine sshd[3400]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:57:19 sunshine sshd[3400]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:57:12 sunshine sshd[3391]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:57:09 sunshine sshd[3391]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:57:07 sunshine sshd[3391]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:56:59 sunshine sshd[3382]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:56:57 sunshine sshd[3382]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:56:55 sunshine sshd[3382]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:20** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:19 sunshine sshd[3403]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:20** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:19 sunshine sshd[3400]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:18** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:17 sunshine sshd[3402]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:18** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:57:17 sunshine sshd[3392]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185438.82265: mail - syslog,access\_control,authentication\_failed,  
2017 Apr 14 11:57:18 sunshine->/var/log/secure  
Rule: 2502 (level 10) -> 'User missed the password more than one time'  
Apr 14 11:57:17 sunshine sshd[3391]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:18** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:17 sunshine sshd[3391]: Failed password for root from ::1 port 36370 ssh2

**2017 Apr 14 11:57:16** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:15 sunshine sshd[3391]: Failed password for root from ::1 port 36370 ssh2

**2017 Apr 14 11:57:14** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:13 sunshine sshd[3391]: Failed password for root from ::1 port 36370 ssh2

**2017 Apr 14 11:57:12** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:12 sunshine sshd[3391]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:12** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:12 sunshine sshd[3391]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:10** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:09 sunshine sshd[3395]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:10** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:09 sunshine sshd[3391]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:08** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:07 sunshine sshd[3394]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:08** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:57:07 sunshine sshd[3391]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:57:06** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:57:06 sunshine sshd[3393]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:06** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:57:05 sunshine sshd[3383]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185426.78588: mail - syslog,access\_control,authentication\_failed,  
2017 Apr 14 11:57:06 sunshine->/var/log/secure  
Rule: 2502 (level 10) -> 'User missed the password more than one time'  
Apr 14 11:57:05 sunshine sshd[3382]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:06** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:05 sunshine sshd[3382]: Failed password for root from ::1 port 36369 ssh2

**2017 Apr 14 11:57:04** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:02 sunshine sshd[3382]: Failed password for root from ::1 port 36369 ssh2

**2017 Apr 14 11:57:02** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:57:01 sunshine sshd[3382]: Failed password for root from ::1 port 36369 ssh2

**2017 Apr 14 11:57:00** Rule Id: [5551](http://www.ossec.net/wiki/index.php/Rule:5551) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**Multiple failed logins in a small period of time.**

Apr 14 11:56:59 sunshine sshd[3382]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:57 sunshine sshd[3386]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:55 sunshine sshd[3385]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:53 sunshine sshd[3384]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:46 sunshine sshd[3373]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:44 sunshine sshd[3377]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:42 sunshine sshd[3376]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:40 sunshine sshd[3375]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:57:00** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:59 sunshine sshd[3382]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:58** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:57 sunshine sshd[3386]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:58** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:57 sunshine sshd[3382]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:56** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:55 sunshine sshd[3385]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:56** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:55 sunshine sshd[3382]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:54** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:53 sunshine sshd[3384]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:52** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:56:51 sunshine sshd[3374]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185412.73828: mail - syslog,access\_control,authentication\_failed,  
2017 Apr 14 11:56:52 sunshine->/var/log/secure  
Rule: 2502 (level 10) -> 'User missed the password more than one time'  
Apr 14 11:56:51 sunshine sshd[3373]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:52** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:51 sunshine sshd[3373]: Failed password for root from ::1 port 36368 ssh2

**2017 Apr 14 11:56:50** Rule Id: [5720](http://www.ossec.net/wiki/index.php/Rule:5720) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**Multiple SSHD authentication failures.**

Apr 14 11:56:50 sunshine sshd[3373]: Failed password for root from ::1 port 36368 ssh2  
Apr 14 11:56:48 sunshine sshd[3373]: Failed password for root from ::1 port 36368 ssh2  
Apr 14 11:56:40 sunshine sshd[3363]: Failed password for root from ::1 port 36367 ssh2  
Apr 14 11:56:38 sunshine sshd[3363]: Failed password for root from ::1 port 36367 ssh2  
Apr 14 11:56:36 sunshine sshd[3363]: Failed password for root from ::1 port 36367 ssh2  
Apr 14 11:56:28 sunshine sshd[3349]: Failed password for root from ::1 port 36364 ssh2  
Apr 14 11:56:26 sunshine sshd[3349]: Failed password for root from ::1 port 36364 ssh2  
Apr 14 11:56:24 sunshine sshd[3349]: Failed password for root from ::1 port 36364 ssh2

**2017 Apr 14 11:56:48** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:48 sunshine sshd[3373]: Failed password for root from ::1 port 36368 ssh2

**2017 Apr 14 11:56:46** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:46 sunshine sshd[3373]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:46** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:46 sunshine sshd[3373]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:44** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:44 sunshine sshd[3377]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:44** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:44 sunshine sshd[3373]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:44** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:42 sunshine sshd[3376]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:44** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:42 sunshine sshd[3373]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:42** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:40 sunshine sshd[3375]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:40** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:56:40 sunshine sshd[3364]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185400.69522: mail - syslog,access\_control,authentication\_failed,  
2017 Apr 14 11:56:40 sunshine->/var/log/secure  
Rule: 2502 (level 10) -> 'User missed the password more than one time'  
Apr 14 11:56:40 sunshine sshd[3363]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:40** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:40 sunshine sshd[3363]: Failed password for root from ::1 port 36367 ssh2

**2017 Apr 14 11:56:38** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:38 sunshine sshd[3363]: Failed password for root from ::1 port 36367 ssh2

**2017 Apr 14 11:56:36** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:36 sunshine sshd[3363]: Failed password for root from ::1 port 36367 ssh2

**2017 Apr 14 11:56:34** Rule Id: [5551](http://www.ossec.net/wiki/index.php/Rule:5551) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**Multiple failed logins in a small period of time.**

Apr 14 11:56:34 sunshine sshd[3363]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:32 sunshine sshd[3367]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:30 sunshine sshd[3366]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:29 sunshine sshd[3365]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:22 sunshine sshd[3349]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:20 sunshine sshd[3356]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:18 sunshine sshd[3353]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:17 sunshine sshd[3351]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:34** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:34 sunshine sshd[3363]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:32** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:32 sunshine sshd[3367]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:32** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:32 sunshine sshd[3363]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:32** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:30 sunshine sshd[3366]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:32** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:30 sunshine sshd[3363]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:30** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:29 sunshine sshd[3365]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:30** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:56:28 sunshine sshd[3350]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185390.64762: mail - syslog,access\_control,authentication\_failed,  
2017 Apr 14 11:56:30 sunshine->/var/log/secure  
Rule: 2502 (level 10) -> 'User missed the password more than one time'  
Apr 14 11:56:28 sunshine sshd[3349]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:30** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:28 sunshine sshd[3349]: Failed password for root from ::1 port 36364 ssh2

**2017 Apr 14 11:56:28** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:26 sunshine sshd[3349]: Failed password for root from ::1 port 36364 ssh2

**2017 Apr 14 11:56:26** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:24 sunshine sshd[3349]: Failed password for root from ::1 port 36364 ssh2

**2017 Apr 14 11:56:24** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:22 sunshine sshd[3349]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:24** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:22 sunshine sshd[3349]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:20** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:20 sunshine sshd[3356]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:20** Rule Id: [5720](http://www.ossec.net/wiki/index.php/Rule:5720) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**Multiple SSHD authentication failures.**

Apr 14 11:56:20 sunshine sshd[3349]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:56:18 sunshine sshd[3349]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:56:10 sunshine sshd[3331]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:56:08 sunshine sshd[3331]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:56:07 sunshine sshd[3331]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:55:58 sunshine sshd[3311]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:55:56 sunshine sshd[3311]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)  
Apr 14 11:55:54 sunshine sshd[3311]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:20** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:18 sunshine sshd[3353]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:20** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:18 sunshine sshd[3349]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:18** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:17 sunshine sshd[3351]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:18** Rule Id: [2501](http://www.ossec.net/wiki/index.php/Rule:2501) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: 1:56:16 sunshine sshd[3332]: Disconnecting: Too many authentication failures for root  
**User authentication failure.**

\*\* Alert 1492185378.59195: mail - syslog,attacks,authentication\_failures,  
2017 Apr 14 11:56:18 sunshine->/var/log/secure  
Rule: 40111 (level 10) -> 'Multiple authentication failures.'  
Apr 14 11:56:16 sunshine sshd[3331]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:16 sunshine sshd[3332]: Disconnecting: Too many authentication failures for root  
Apr 14 11:56:05 sunshine sshd[3311]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:05 sunshine sshd[3312]: Disconnecting: Too many authentication failures for root  
Apr 14 11:55:40 sunshine sshd[3256]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=charlie  
Apr 14 11:55:40 sunshine sshd[3257]: Disconnecting: Too many authentication failures for charlie  
Apr 14 11:55:27 sunshine sshd[3245]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=charlie  
Apr 14 11:55:27 sunshine sshd[3246]: Disconnecting: Too many authentication failures for charlie  
Apr 14 11:55:15 sunshine sshd[3231]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=charlie  
Apr 14 11:55:15 sunshine sshd[3232]: Disconnecting: Too many authentication failures for charlie  
Apr 14 11:55:01 sunshine sshd[3220]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=charlie

**2017 Apr 14 11:56:18** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:16 sunshine sshd[3331]: Failed password for root from ::1 port 36363 ssh2

**2017 Apr 14 11:56:16** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:14 sunshine sshd[3331]: Failed password for root from ::1 port 36363 ssh2

**2017 Apr 14 11:56:14** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: ::1  
**SSHD authentication failed.**

Apr 14 11:56:12 sunshine sshd[3331]: Failed password for root from ::1 port 36363 ssh2

**2017 Apr 14 11:56:12** Rule Id: [5551](http://www.ossec.net/wiki/index.php/Rule:5551) level: 10  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**Multiple failed logins in a small period of time.**

Apr 14 11:56:10 sunshine sshd[3331]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:08 sunshine sshd[3337]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:07 sunshine sshd[3335]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:56:05 sunshine sshd[3333]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:55:58 sunshine sshd[3311]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:55:56 sunshine sshd[3326]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:55:54 sunshine sshd[3325]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
Apr 14 11:55:52 sunshine sshd[3313]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:12** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:10 sunshine sshd[3331]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:10** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:08 sunshine sshd[3337]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:10** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:08 sunshine sshd[3331]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:08** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:07 sunshine sshd[3335]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root

**2017 Apr 14 11:56:08** Rule Id: [5716](http://www.ossec.net/wiki/index.php/Rule:5716) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**SSHD authentication failed.**

Apr 14 11:56:07 sunshine sshd[3331]: error: PAM: Authentication failure for root from [sunshine.edu](http://sunshine.edu)

**2017 Apr 14 11:56:06** Rule Id: [5503](http://www.ossec.net/wiki/index.php/Rule:5503) level: 5  
**Location:** sunshine->/var/log/secure   
**Src IP**: [sunshine.edu](http://sunshine.edu)  
**User login failed.**

Apr 14 11:56:05 sunshine sshd[3333]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[sunshine.edu](http://sunshine.edu) user=root  
  
  
  
  
 **Questions regarding on Hands on Activity :** 1. How did attacker attempt to access the system? What account was his/her target?  
  
Attacker was trying to access the account using root, and the script main focus was to hack the root account and enter the account make the necessary changes as per the requirement.  
  
 2. Once the account was compromised, were any other accounts compromised?  
  
No, No other account was been compromised as because of the root account was been not authorized to access because of wrong username and password and it was tried to gain multiple try and attempts to root account with incorrect username and password.   
  
  
 3. Was any new software installed?  
  
No, As there was no access to root even with different username or password attempts and also with different ports resolves with same error of authentication failed, then the attacker was not allowed to install an kind of application without any kind of root access permissions, so the criminal black hat scenario was not able to process.  
  
 4. Were any new network ports opened or closed?  
  
Yes, Attacker tried to access to root account by using different ports to get access to root which was not successful. How ever here are some of the ports which are been tried to get access are 36369, 36373, 36372, 36371.. etc., for example.   
  
  
 5. Were any accounts added to the system?  
  
No, As there was no access to root, he was not allowed to create a new user account.  
  
 6. Generate a time line of the major events that occurred in this incident. A Microsoft Word template for the timeline can be downloaded from http://office.microsoft.com/en-us/templates/timeline-TC001016265.aspx  
  
  
<https://templates.office.com/?legRedir=true&CorrelationId=b8970b80-d392-46c7-aed1-4350ecf95c1e>  
  
Here is the link to which was redirected when the <http://office.microsoft.com/en-us/templates/timeline-TC001016265.aspx> was opened and then we had choosen one template to generate the timeline which is been downloaded on above mentioned link .  
  
  
  
  
