Strengthening Security

BanCoppel

Remediation actions

Ruben Sebastian Velis

04/01/2021

Content

Target………………………………………………………………………………………………………………………………… …………………2

Files required for execution ………………………………………………………………………………………………… 3

Configuration Files ………………………………………………………………………………………………………………… 4

Hosts and Inventory Configuration ………………………………………………………………………………… 5.

Execution …………………………………………………………………………………… 10

# Instructions for running remediation PLAYBOOKS

## Remediation objective

* Successful and unsuccessful authentication attempts, with priority on network services.
* / var / log / faillog deprecated log.
* /var/log/auth.log For Debian and derived servers.
* / var / log / secure For Redhat servers and derivatives.
* Use of any invocation of the “root” or privileged account, such as the “su” command (eg “sudoers” registry).
* /var/log/auth.log For Debian and derived servers.
* / var / log / secure For Redhat servers and derivatives.
* Incoming connections denied (eg those blocked by iptables).
* /var/log/kern.log For Debian and derivative servers.
* / var / log / messages For Redhat servers and derivatives.
* Command history (eg bash shell history logs), including date records.
* Install auditd, psacct, or acct.
* Install and configure psacct, or acct depending on the operating system RHEL CentOS Debian, Ubuntu and derivatives.
* Start services.
* Configure auditd, edit the /etc/audit/auditd.conf file.
* adaptation of playbook to run on SUSE
* SSH Rhel / Multi OS security fix.
* Validation and correction of user that should not log in.

Audit.rules Rules Management.

Configure in rsyslog.

•/var/log/audit/audit.log.  
•/var/log/auth.log.  
•/var/log/cron.  
•/var/log/dpkg.log.  
•/var/log/messages.  
•/var/log/secure.  
•/var/log/sudo.  
•/var/log/syslog.  
•/var/log/wtmp.  
•/var/log/yum.log.  
•/var/log/httpd/access\_log.  
•/var/log/apache2/access.log.

## Files required for execution

* RedHat
* CentOs
* Ubuntu
* Debian

|  |  |  |
| --- | --- | --- |
| FILES | | |
| /Debian.yaml | /Debian/logrotatedebian.yml | /CentOS/rsyslog.conf |
| /RedHat.yaml | /Debian/rsyslogdebian.conf | /CentOS/rsyslogother.conf |
| /main.yaml | /Debian/copy.yml | /CentOS/rsyslogrhel.conf |
| /hosts | /inventario.tux | /CentOS/rules.yml |
| /README.md | /Ubuntu | /CentOS/uuid.yml |
| /Debian | /Ubuntu/50-default.conf | /RedHat |
| /Debian/50-default.conf | /Ubuntu/audit.yml | /RedHat/50-default.conf |
| /Debian/listen.conf | /Ubuntu/fecha.yml | /RedHat/listen.conf |
| /Debian/rsyslog.conf | /Ubuntu/rules.yml | /RedHat/logrotateother.yml |
| /Debian/kernel.yml | /Ubuntu/uuid.yml | /RedHat/rsyslog.conf |
| /Debian/fecha.yml | /Ubuntu/copy.yml | /RedHat/rsyslogother.conf |
| /Debian/uuid.yml | /Ubuntu/rsyslogdebian.conf | /RedHat/rsyslogrhel.conf |
| /Debian/pkgother.yml | /CentOS | /RedHat/logrotaterhel.yml |
| /Debian/pkgaudit.yml | /CentOS/50-default.conf | /RedHat/kernel.yml |
| /Debian/rules.yml | /CentOS/audit.yml | /RedHat/uuid.yml |
| /Debian/audit.yml | /CentOS/cfgedit.yml | /RedHat/audit.yml |
| /Ubuntu/kernel.yml | /CentOS/copy.yml | /RedHat/fecha.yml |
| /Ubuntu/listen.conf | /CentOS/fecha.yml | /RedHat/rhelyum.yml |
| /Ubuntu/logrotateother.yml | /CentOS/kernel.yml | /RedHat/rules.yml |
| /Ubuntu/pkgaudit.yml | /CentOS/listen.conf | /RedHat/logrotate.yml |
| /Ubuntu/pkgother.yml | /CentOS/logrotateother.yml | /RedHat/cfgedit.yml |
| /Ubuntu/rsyslog.conf | /CentOS/logrotaterhel.yml | /RedHat/copy.yml |
| /Ubuntu/rsyslogother.conf | /CentOS/logrotate.yml | /Ubuntu.yaml |
| /Ubuntu/rsyslogrhel.conf | /CentOS/rhelyum.yml | /CentOS.yaml |

## Configuration Files

|  |
| --- |
| FILES |
| /Debian/50-default.conf |
| /Debian/listen.conf |
| /Debian/rsyslog.conf |
| /Debian/rsyslogdebian.conf |
| /Ubuntu/50-default.conf |
| /Ubuntu/listen.conf |
| /Ubuntu/rsyslog.conf |
| /Ubuntu/rsyslogother.conf |
| /Ubuntu/rsyslogrhel.conf |
| /CentOS/50-default.conf |
| /CentOS/listen.conf |
| /CentOS/rsyslog.conf |
| /CentOS/rsyslogother.conf |
| /CentOS/rsyslogrhel.conf |
| /RedHat/50-default.conf |
| /RedHat/listen.conf |
| /RedHat/rsyslog.conf |
| /RedHat/rsyslogother.conf |
| /RedHat/rsyslogrhel.conf |

Adaptation of playbook to run on SUSE

|  |
| --- |
| FILES |
| Suse |
| Suse  50-default.conf  audit.yml  audit.yml.bak  copy.yml  copy.yml.bak  fecha.yml  fecha.yml.bak  kernel.ym  kernel.yml  kernel.yml.bak  listen.conf  logrotatedebian.yml  logrotatesuse.yml  logrotatesuse.yml.bak  pkgaudit.yml  pkgaudit.yml.bak  pkgother.yml  pkgother.yml.bak  rsyslog.conf  rsyslogdebian.conf  rules.yml  rules.yml.bak  uuid.yml  Suse.yaml |

SSH Rhel / Multi OS security fix. V1

Remediation was done for RHEL(V7.9-V8)/DEBIAN(v8.7-V10.2)

It is recommended to be somewhat more delicate is that in each of the playbooks you specify the IP where it will be executed to minimize execution by mistake.

Execute

Example

- hosts: 10.92.192.250 xxx.xxx.xxx.xxx  
  gather\_facts: yes  
  become: true  
  become\_method: su  
  become\_user: root

|  |
| --- |
| FILES |
| DEBIAN |
| sshd\_config\_debian102  sshd\_config\_debian78  sshdebian102.yml  sshdebian87.yml |
| REDHAT |
| sshd\_config  sshd\_config\_rhel8  sshrehl73.yml  sshrehl8.yml |

It was requested that a multi-OS playbook be made to apply since I only wanted to put the IPs and that the playbook perform the intelligence when applying the conf.

SSH Rhel / Multi OS security fix. V2.

|  |
| --- |
| FILES |
| DEBIAN |
| source.list\_bullseye  source.list\_buster  source.list\_stable  source.list\_stretch  source.list\_testing  source.list\_unstable  sshd\_config\_debian\_10x  sshd\_config\_debian\_8x  debianParserSSHD.yaml  debianPreChecks.yaml  debianReloadSSHServer.yaml  debianRepoSetup.yaml  main\_Debian.yaml  main\_Debian.yaml.bak |
| REDHAT |
| RhelParserSSHD.yaml  RhelParserSSHD.yaml.bak  RhelReloadSSHServer.yaml  sshd\_config  sshd\_config\_rhel8  main\_RHEL.yaml  main\_RHEL.yaml.bak  inventario.tux  inventario.tux.bak  main.yaml |

Unlike the previous one, this one has the intelligence that seeks OS / and specific version

Example

when:

- ansible\_distribution == "Redhat"

- ansible\_distribution\_major\_version == "7.3"

when:

- ansible\_distribution == "Redhat"

- ansible\_distribution\_major\_version == "8.0"

Validation and correction of user that should not login

the task is carried out by blocking the user, changing the login flag and by expiration of the same

|  |
| --- |
| USER NOT LOGIN |
| bitdefender  clam  clamav  games  lleono  nessus  nesus  operator  pruebas  splunk  splunkadm  storage  sys  test  www-data  FILE  blockUsersFinalTUX.yaml |

should be run with inventory

**HOSTS File Configuration / SSH-KEY**

The ip's and the names of the servers must be declared in the hosts file

example:

[root@ss os\_detector]# cat /etc/hosts  
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4  
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

10.92.192.10 ubuntu.lab  
10.92.192.250 rhel.lab

[root@ss os\_detector]#

The cert must be accepted. Ssh from the vm that runs ansible to the vm to hit.

## File Settings Inventario.tux

The user who will execute the tasks must be declared  
example  
[all:vars]  
ansible\_become=yes  
ansible\_become\_user=root  
ansible\_become\_password=07cf04cv  
ansible\_become\_method=su  
ansible\_python\_interpreter=auto\_silent

**Then declare the servers by SO**

**example**

[DebianHosts]  
ubuntu.lab

[UbuntuHosts]  
ubuntu.lab

[CentOSHost]  
rhel.lab

[RedHatHost]  
rhel.lab

## EXECUTION

This Playbook will differentiate the OS and will execute the task for each of the distributions.

ansible-playbook -i inventario.tux main.yaml -v

#VERSION 0.1

