Linux Servers

Classroom Assignment 7 – Linux Security

Mikael Romanov

Document your commands or take screenshots. Answer questions in english or finnish.

1. Deny Root login

Deny root login from SSH. Test that you cannot SSH in with root.

I configured the routers sshd_config file. Uncommented the PermitRootLogin and set parameter no.

```
  GNU nano 2.3.1          File: /etc/ssh/sshd_config


# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

After reboot I tried to connect to router via putty:

```
192.168.1.107 - PuTTY
login as: root
root@192.168.1.107's password:
Access denied
root@192.168.1.107's password:
```

2. Virus scan

Install ClamAV and Freshclam (clamav clamav-update). Update the virus database and scan your whole Linux server. (Hint: See /etc/freshclam.conf)

Installing the clamav:

```
[root@router ~]# yum install -y clamav_
```

Updating clamav:

```
[root@router ~]# yum install clamav-update_
```

Updating virus database:

```
[root@router ~]# freshclam_
```

```
bytecode.cld updated (version: 283, sigs: 53, f-level: 63, builder: neo)
Database updated (5050462 signatures) from database.clamav.net (IP: 195.30.97.3)
```

Scanning the whole system:

```
[root@router ~]# clamscan -r /_
```

results:

```
----------- SCAN SUMMARY -----------
Known viruses: 5045042
Engine version: 0.99.2
Scanned directories: 10183
Scanned files: 43026
Infected files: 0
Total errors: 8615
Data scanned: 1740.74 MB
Data read: 1506.98 MB (ratio 1.16:1)
Time: 346.007 sec (5 m 46 s)
```

3. CVE lookup

Check https://lists.centos.org/pipermail/centos-announce/ for new Critical/Important security issues from this month. Select one of them and find out what components are affected. What packages need to be updated if installed?

https://lists.centos.org/pipermail/centos-announce/2016-October/022124.html

Security update java-1.8.0-openjdk

```
CentOS Errata and Security Advisory 2016:2079 Critical

Upstream details at : https://rhn.redhat.com/errata/RHSA-2016-2079.html

The following updated files have been uploaded and are currently
syncing to the mirrors: ( sha256sum Filename )

x86_64:
028b7d73cab8947df0f2fe08c028d6349aa7cb6a19ef01ac4ddc78939ab25f61  java-1.8.0-openjdk-1.8.0.111-1.b15.el7_2.x86_64.rpm
83fc734f15cd1891fb0c5fd5e692df9048cd7dc56ec468e7281eb2eaf6654e20  java-1.8.0-openjdk-accessibility-1.8.0.111-1.b15.el7_2.x86_64.rpm
84a58a7dab05f4230d4c30b35e0649de9e0f0acd1ea984428da31ca4d91dab92  java-1.8.0-openjdk-accessibility-debug-1.8.0.111-
1.b15.el7_2.x86_64.rpm
02488f4200afbba9b86c6f3cbf6054778afaf24164675fe1a7e3eca113999999  java-1.8.0-openjdk-debug-1.8.0.111-1.b15.el7_2.x86_64.rpm
7c5e7dc04f1286a18c1c5df06fa73dd5640ef9f631c91c2a3cd6c883cb7acf68  java-1.8.0-openjdk-demo-1.8.0.111-1.b15.el7_2.x86_64.rpm
11b2902c6c4d7dfe82b869903c894b05c7b768c337469f36310fc43b5b4611df  java-1.8.0-openjdk-demo-debug-1.8.0.111-1.b15.el7_2.x86_64.rpm
03433ad6c3f91643b9744acf870b875d7418593c60c31eb5cfe32f4619112a8f  java-1.8.0-openjdk-devel-1.8.0.111-1.b15.el7_2.x86_64.rpm
70c0c17a4dced2896b0f1d4c622615e2e3bfce16042017d0e424496a1386d680  java-1.8.0-openjdk-devel-debug-1.8.0.111-1.b15.el7_2.x86_64.rpm
ce6eed8d95c73553e83669594284cfb4d43959761499f1a2d90e040352eb8b1c  java-1.8.0-openjdk-headless-1.8.0.111-1.b15.el7_2.x86_64.rpm
b9f8e783b3f82a3fe567a6f343a3e7ab5acf3d838fb2bdf6670da3df52bc11bd  java-1.8.0-openjdk-headless-debug-1.8.0.111-
1.b15.el7_2.x86_64.rpm
5f2d8974a59c970489994bd9f74194122cfccd1d48e3078977e9840cccd4bae4  java-1.8.0-openjdk-javadoc-1.8.0.111-1.b15.el7_2.noarch.rpm
99764694bbfc61c98497d90f482f11b29edeb9a14ed583386e1fcd1f7685a003  java-1.8.0-openjdk-javadoc-debug-1.8.0.111-1.b15.el7_2.noarch.rpm
241163cc6cd5f82476b489dcaa3d02e2e97f71606de63af94178f0538648b9e2  java-1.8.0-openjdk-src-1.8.0.111-1.b15.el7_2.x86_64.rpm
749d9c3495ec107da97f6044016972877c75346e06f358559d8beb1dd0b013ad  java-1.8.0-openjdk-src-debug-1.8.0.111-1.b15.el7_2.x86_64.rpm

Source:
14dd2d91e721496277c119284a579fe2efd2433e3ee1841053bef94f5fb2f455  java-1.8.0-openjdk-1.8.0.111-1.b15.el7_2.src.rpm
```

4. SELinux

Check what is the SELinux boolean value for *httpd_can_network_connect_db*. What does this SELinux Boolean do? When should you enable it?

Does not allow apache http server scripts or modules to connect to database. If you want apache to be able to connect to a database, then you need to enable it.

```
[root@router ~]# semanage boolean -l | grep httpd_can_network
httpd_can_network_relay        (off  ,  off)  Allow httpd to can network relay
httpd_can_network_connect_db   (off  ,  off)  Allow httpd to can network connect
 db
```

5. Firewall

Allow the service bacula with firewall-cmd to public zone. What ports does this service use? What iptables commands would you use to allow this service (ports) from eth0 interface with source 10.0.0.1?

```
[root@router ~]# firewall-cmd --zone=public --add-service=bacula --permanent
success
```

Bacula ports are 9101, 9102 ja 9103. The information was from
http://www.bacula.org/5.0.xmanuals/en/problems/problems/Dealing_with_Firewalls.html

I would use this for input:

iptables -I INPUT --p tcp --d 10.0.0.1 --i eth0 --dport 9101:9103

I would use this for output:

iptables -A OUTPUT --p tcp --s 10.0.0.1 --i eth0 --sport 9101:9103