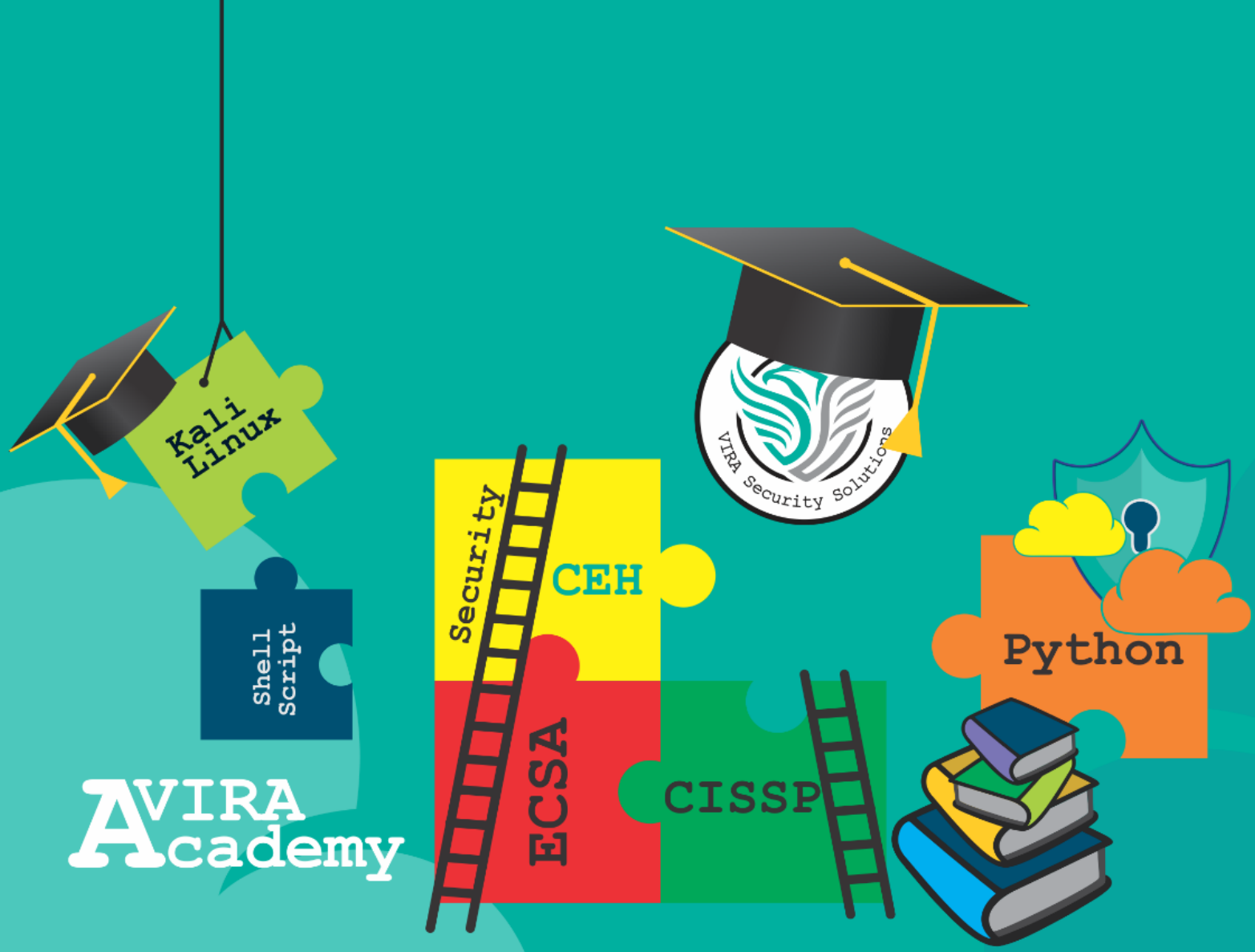

VIRA
Security
Solutions


راهکارهای امن ویرا
شماره ثبت: ۵۴۰۱۳۹
VIRA Security Solutions


Kali Linux
Shell Script
VIRA Security Solutions
Security
CEH
ECSA
CISSP
Python
AVIRA Academy

Linux

Part9

Mohammad Reza Gerami
Mrgerami@aut.ac.ir
gerami@virasec.ir

Linux Security

Security Tips

Check Update for Security and Vulnerabilities

cve.mitre.org
redhat.com
access.redhat.com

Security Tips

Check Update for Security and Vulnerabilities

Redhat or CentOS:
yum updateinfo
yum updateinfo list
yum updateinfo [PackageNAME]
yum updateinfo RHSA-2016:0176 | less #Advisiory ID

Security Tips

Check Update for Security and Vulnerabilities


```
# Redhat & CentOS
yum installl yum-plugin-security
yum updateinfo
yum updateinfo list
yum updateinfo RHSA-2016:0176 | less
cve.mitre.org   > search package or year s like 2017 for vulnerabilities

updateinfo list --cve=CVE=2016-0728
```

Security Tips

Check Update for Security and Vulnerabilities

Ubuntu:
#Check updates
apt-get -s dist-upgrade

#Check update start with Installable
apt-get -s dist-upgrade | grep "^Inst"

#Check update Installable for security
apt-get -s dist-upgrade | grep "^Inst" | grep -i secur

Security Tips

Modifying Text Console Setting

#Text Console Security
/etc/issue
login
/etc/motd

Security Tips

Modifying Text Console Setting

vim /etc/issue

Authorized access only

vim /etc/motd

Welcome to this server

Security Tips

SSH Port

vi /etc/sshd/sshd_config
#Change
Port 22 > Port 2022

systemctl restart sshd
netstat -tulpen | grep 22

systemctl status sshd

Security Tips

Managing default permissions

```
cd
touch afile
ls -l afile

su - reza
touch arezafile
ls -l arezafile
```

```
# you can see the diffrent between files permision

Umask  - bitmask
files : 666        Directories:  777
Umask   022= 644                022 =755
umask   002= 644                002 =775
umask   027= 640                027 =750

 #umask 027
 #touch lfile
 #ls -l
```

Security Tips

Using extended attributes

Regular File Attribute
&
Extended Attribute
namespace.attribute
security > linux kernel security modules
system > kernel to start ACL
trusted > Used by processes gapsys admin
user > used for managing users

Security Tips

Using extended attributes

```
cd vira
chattr +i rootfile
lsattr *
rm -f rootfile

chattr -i rootfile
rm -f rootfile
```

Security Tips

Using extended attributes

#ubuntu
lsattr
e means extend

getfattr /home/

getfattr -d /home/

getfattr -m secur/home/

Security Tips

Check Listening Network Ports

With the help of ‘netstat‘ networking command you can view all open ports and associated programs. As I said above use ‘chkconfig‘ command to disable all unwanted network services from the system.

netstat -tulpn

Security Tips

Use Secure Shell(SSH)

Telnet and rlogin protocols uses plain text, not encrypted format which is the security breaches. SSH is a secure protocol that use encryption technology during communication with server.
Never login directly as root unless necessary. Use “sudo” to execute commands. sudo are specified in /etc/sudoers file also can be edited with the “visudo” utility which opens in VI editor.

netstat -tulpn

Security Tips

Use Secure Shell(SSH)

It's also recommended to change default SSH 22 port number with some other higher level port number. Open the main SSH configuration file and make some following parameters to restrict users to access.

vi /etc/ssh/sshd_config

Disable root Login

PermitRootLogin no

Only allow Specific Users

AllowUsers username

Use SSH Protocol 2 Version

Protocol 2

Security Tips

Turn Off IPv6

If you're not using a IPv6 protocol, then you should disable it because most of the applications or policies not required IPv6 protocol and currently it doesn't required on the server. Go to network configuration file and add followings lines to disable it.

```
vi /etc/sysconfig/network
        NETWORKING_IPV6=no
        IPV6INIT=no
```

Security Tips

Disable Ctrl+Alt+Delete in Inittab

In most Linux distributions, pressing 'CTRL-ALT-DELETE' will takes your system to reboot process. So, it's not a good idea to have this option enabled at least on production servers, if someone by mistakenly does this.
This is defined in '/etc/inittab' file, if you look closely in that file you will see a line similar to below. By default line is not commented out. We have to comment it out. This particular key sequence signalling will shut-down a system.

```
# Trap CTRL-ALT-DELETE
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Security Tips

Checking Accounts for Empty Passwords

Any account having an empty password means its opened for unauthorized access to anyone on the web and it's a part of security within a Linux server. So, you must make sure all accounts have strong passwords and no one has any authorized access. Empty password accounts are security risks and that can be easily hackable. To check if there were any accounts with empty password, use the following command.

```
cat /etc/shadow | awk -F: '($2==""){print $1}'
```

Security Tips

Ignore ICMP or Broadcast Request

Add following line in “/etc/sysctl.conf” file to ignore ping or broadcast request.

- Ignore ICMP request:
- net.ipv4.icmp_echo_ignore_all = 1

- Ignore Broadcast request:
- net.ipv4.icmp_echo_ignore_broadcasts = 1
- Load new settings or changes, by running following command

- #sysctl -p

Security Tips

Set Up Password Aging For Linux Users For Better Security

The changes the number of days between password changes and the date of the last password change. This information is used by the system to determine when a user must change his/her password. The /etc/login.defs file defines the site-specific configuration for the shadow password suite including password aging configuration. To disable password aging, enter:

```
# chage -M 99999 userName
```

To get password expiration information, enter:

```
# chage -l userName
```

Security Tips

Locking User Accounts After Login Failures

Under Linux you can use the faillog command to display faillog records or to set login failure limits. faillog formats the contents of the failure log from /var/log/faillog database / log file. It also can be used for maintains failure counters and limits.To see failed login attempts, enter:

```
faillog
```

To unlock an account after login failures, run:

```
faillog -r -u userName
```

Note you can use passwd command to lock and unlock accounts:

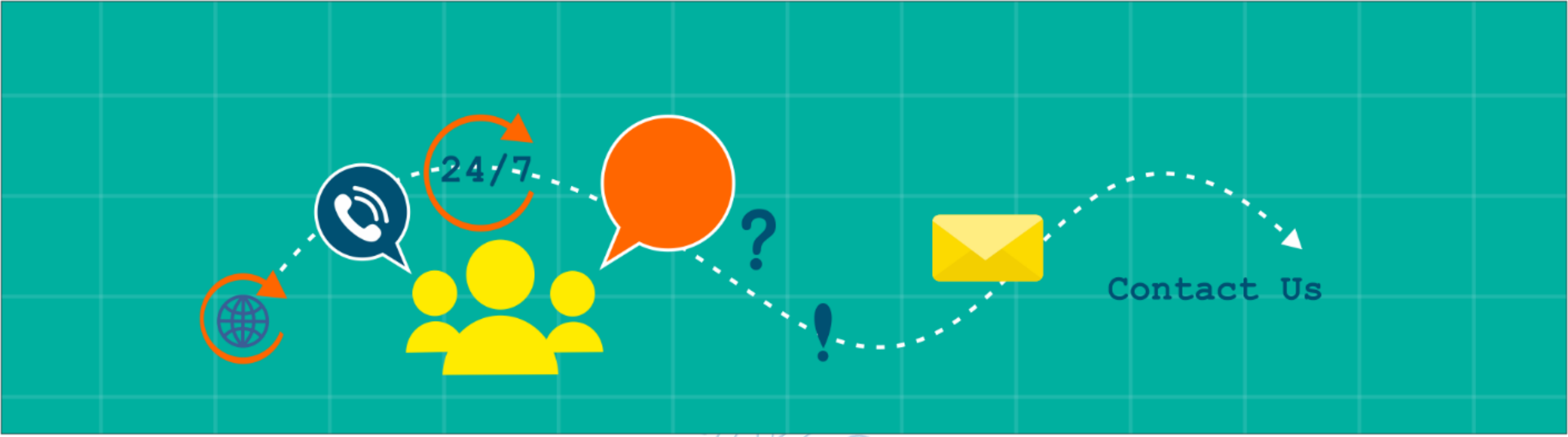
```
# lock Linux account
passwd -l userName
# unlock Linux account
passwd -u userName
```

Security Tips

Review Logs Regularly

Move logs in dedicated log server, this may prevents intruders to easily modify local logs. Below are the Common Linux default log files name and their usage:

- /var/log/message – Where whole system logs or current activity logs are available.
- /var/log/auth.log – Authentication logs.
- /var/log/kern.log – Kernel logs.
- /var/log/cron.log – Crond logs (cron job).
- /var/log/maillog – Mail server logs.
- /var/log/boot.log – System boot log.
- /var/log/mysqld.log – MySQL database server log file.
- /var/log/secure – Authentication log.
- /var/log/utmp or /var/log/wtmp : Login records file.
- /var/log/yum.log: Yum log files.



Visiting Address: Unit 20, Floor 4, No 53 Vafa Manesh Ave

Heravi, Pasdaran Ave, TEHRAN-IRAN

Post Code:1668838803

Tel No: 0098 21 2298 1027-09125792641

Email: info@ virasecsolutions.com

Website: www.virasecsolutions.com

آدرس: تهران، پاسداران، هروی، خیابان وفامنش، پلاک ۵۳

طبقه چهارم، واحد ۲۰

کد پستی: ۱۶۶۸۸۳۸۸۰۳

شماره تماس: ۰۹۱۲۵۷۹۲۶۴۱-۰۲۱۲۲۹۸۱۰۲۷