

Team Number	
Round #	Date: / /
<b>Operating Syst</b>	em

Securing a LAMP server

	•	N I		1	1		
L	П	N	u	U	J	х	

- 1. Update the machine
  - a. apt-get update
  - b. apt-get upgrade
  - c. apt-get dist-upgrade
- Install clamtk
  - a. apt-get install clamtk
  - b. Run the scan
    - i. freshclam
- 3. Set automatic Updates
  - a. System settings>software & updates>Updates
    - i. Automatically check for updates
    - ii. Important security updates
- Search for all prohibited files
  - a. find / -name "\*.{extension}" -type f
- Configure the firewall
  - a. apt-get install ufw / yum install ufw
  - b. ufw enable
  - c. ufw status
- 6. Edit the lightdm.conf file
  - a. Ubuntu
    - i. Edit /etc/lightdm/lightdm.conf or /usr/share/lightdm/lightdm.conf/50-ubuntu.conf
    - ii. allow-quest=false
    - iii. greeter0hide-users=true
    - iv. greeter-show-manual-login=true
    - v. autologin-user=none
  - b. Debian
    - i. Edit /etc/lightdm/lightdm.conf
      - 1. Greeter-hide-users=true
      - 2. Greeter-allow-guest=false
      - 3. Greeter-show-manual-login=true
      - 4. Allow-quest=false
      - 5. Autologin-user=none
    - ii. Edit /etc/gdm3/greeter.dconf-defaults
      - 1. Disable-user-list=true
      - 2. Disable-restart-buttons=true
      - 3. AutomaticLoginEnable = false
- 7. Create any missing users

a.	
b.	

- 8. Change all the user passwords to "Cyb3rPatr!0t\$"
- Edit the /etc/login.defs
  - a. FAILLOG\_ENAB YES
  - b. LOG UNKFAIL ENAB YES
  - c. SYSLOG\_SU\_ENAB YES
  - d. SYSLOG SG ENAB YES
  - e. PASS MAX DAYS 90
  - PASS MIN DAYS 10
  - PASS\_WARN\_AGE 7
    - i. Add the following to the line that ends in difok=3 to /etc/pam.d/common-password
    - ii. ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1



Team Number	
Round #	Date: / /
<b>Operating Syst</b>	em

10.	Delete a	ny users			
	a.			_	
	b.			_	
	С.			_	
11.	Check th	ne /etc/pa	asswd fil	e	
	a.	Look for	any rep	eating UI	D or GID
	b.	Make su	re no pr	ograms ł	nave a /bin/sh or /bin/bash
	c.	Only roc	t should	have a l	JID and GID of 0
12.	Check th	-			age the groups
	a.	_	-		sudo and adm group.
13.	Disable t	the root a			5 1
	a.	passwd			
14.	-	SH if requ			
	a.	edit /etc		d confia	
	۵.			a_eon,.g aceTime	60
			_	RootLogir	
			Protoco	-	
					swords no
					ntication yes
				arding n	
			UsePAN	_	0
		vii. viii.			gration vas
15	Socuro t	viii. he <i>/etc/s</i>			aration yes
15.					
10	a.	chmod 6			
16.		any bad			1
	a.			ACKAGE	
		i. ::		e Ripper	(JTK)
			Hydra		
			Nginx		
		iv.	Samba		
			Bind9	c.	
		vi.	Vsftpd/	•	
			1.	•	red then secure the /etc/vsftpd.conf
				а.	anonymous_enable=ON
				b.	- · · · · <del>-</del> · · · · · · · ·
					write_enable=YES
				d.	chroot_local_user=YES
			Tftpd	_	
		viii.	X11vnc/	tightvnc/	server
		ix.	Snmp		
		х.	Nfs		
		xi.	Sendmo	iil/postfix	(
		xii.	Xinetd		
17.	Configur	re /etc/sy	sctl.conf		
	a.	Sysctl -p			
	b.	Add this	to the b	ottom of	the /etc/sysctl.conf file
		i.	Disable	ICMP red	
			1.	net.ipv4	1.conf.all.accept_redirects = 0
		ii.	Disable	IP redire	cting
			1.	net.ipv4	1.ip_forward = 0

2. net.ipv4.conf.all.send\_redirects = 0 3. net.ipv4.conf.default.send\_redirects = 0

iii. Disable IP spoofing



Team Number	
Round #	Date: / /
<b>Operating Syst</b>	em

# **CyberPatriot Categorized Checklist**

- 1. net.ipv4.conf.all.rp\_filter=1
- iv. Disable IP source routing
  - 1. net.ipv4.conf.all.accept source route=0
- v. SYN Flood Protection
  - 1. net.ipv4.tcp\_max\_syn\_backlog = 2048
  - 2. net.ipv4.tcp\_synack\_retries = 2
  - 3. net.ipv4.tcp syn retries = 5
  - 4. net.ipv4.tcp\_syncookies = 1
- vi. Disable IPV6
  - 1. net.ipv6.conf.all.disable ipv6 = 1
  - 2. net.ipv6.conf.default.disable\_ipv6
  - 3. net.ipv6.conf.lo.disable\_ipv6
- 18. Check cronjobs
  - a. Check these folders
    - i. /etc/cron.\*
    - ii. /etc/crontab
    - iii. /var/spool/cron/crontabs
  - b. Check the init files
    - i. /etc/init
    - ii. /etc/init.d
  - c. Check for each user
    - i. crontab -u {USER} -l
- 19. Check sudoers
  - a. When using the sudo su command it should always ask for a password, if not
    - i. Check /etc/sudoers
    - ii. Or /etc/sudoers.d
  - b. Make sure that there are no NOPASSWD values set
    - i. Change all of them to ALL=(ALL:ALL) ALL
- 20. Check the runlevels if unable to boot into GUI
  - a. To check the run level
    - i. runlevel
  - b. Runlevels
    - i. O-System halt;No activity
    - ii. 1-Single user
    - iii. 2-Multi-user, no filesystem
    - iv. 3-Multi-user, commandline only
    - v. 4-user defineable
    - vi. 5-multi-users, GUI
    - vii. 6-Reboot
  - c. To change the run level
    - i. Telinit {level}

# **APACHE**

- 1. Hide Apache Version number.
  - a. Add the following lines to the bottom of /etc/apache2/apache2.conf
    - i. ServerSignature Off
    - ii. ServerTokens Prod
- 2. Make sure Apache is running under its own user account and group.
  - a. Add a separate user "apache"
  - b. Edit the /etc/apache2/apache2.conf file
    - i. User apache
    - ii. Group apache
- 3. Ensure that file outside the web root directory are not accessed. /etc/apache2/apache2.conf
  - a. <Directory />



Team Number	
Round #	Date: / /
<b>Operating Syst</b>	em

Order Deny, Allow Dent from all Options -Indexes AllowOverride None </Directory> <Directory /html>

Order Allow, Denv

Allow from all

- </Directory>
- Turn off directory browsing, Follow symbolic links and CGI execution
  - a. Add Options None to a < Directory /html > tag
- Install modsecurity
  - a. apt-get install mod security
  - b. service httpd restart
- Lower the Timeout value in /etc/apache2/apache2.conf
  - a. Timeout 45

## MySQL

- Restrict remote MySQL access
  - a. Edit /etc/mysql/my.cnf
    - i. Bind-address=127.0.0.1
- Disable use of LOCAL INFILE
  - a. Edit /etc/mysql/my.cnf
    - i. [mysqld]
    - ii. local-infile=0
- 3. Create Application Specific user
  - a. root@Ubuntu:~# mysql -u root -p
  - b. mysql> CREATE USER 'myusr'@'localhost' IDENTIFIED BY 'password';
  - c. mysql> GRANT SELECT,INSERT,UPDATE,DELETE ON mydb.\* TO 'myusr'@'localhost' IDENTIFIED BY 'password';
  - d. mysql> FLUSH PRIVILEGES;
- 4. Improve Security with mysql secure-installation
  - a. root@Ubuntu:~# mysql\_secure\_installation
    - i. change the root password?: y
    - ii. Remove anonymous users?: y
    - iii. Disallow root login remotely?: y
    - iv. Remove test database and access to it?: y
    - v. Reload privilege tables now?: y

## **PHP**

- **Restrict PHP Information Leakage** 
  - a. Edit /etc/php5/apaceh2/php.ini
    - i. expose\_php = off
- Disable Remote Code Execution
  - a. Edit /etc/php5/apache2/php.ini
    - i. allow\_url\_fopen=Off
    - ii. allow url include=Off
- Disable dangerous PHP Functions
  - a. Edit /etc/php5/apache2/php.ini
    - $i. \quad \textit{disable\_functions=exec,shell\_exec,passthru,system,popen,curl\_exec,curl\_multi\_exec,par} \\$ se ini file, show source, proc open, pcntl exec
- **Enable Limits in PHP** 
  - a. Edit /etc/php5/apache2/php.ini
    - i. upload\_max\_filesize = 2M
    - ii. max\_execution\_time = 30
    - iii. max\_input\_time = 60



Team Number	
Round #	Date: / /
<b>Operating Syst</b>	:em