CIS 193 – Linux Security

Jim's VM's on Opus

- ssh –x vmware@opus.cabrillo.edu (simmsr/funny-cabrillo)
- frodo & sam VM's have Internet access
- init 0 (to shutdown)

catbird.com – new security company formed by ex-SCO employees.

Cabrillo Linux Users Group
http://www.cabrillo.edu/associations/clug/
CLUG-subscribe@cabrillo.edu

Risks (proportional to) Threats * Vulnerabilities – Safeguards

Security = 1 / (1.072 * Convenience) p671 in text

Threats	Vulnerabilities	Safeguards
users malware o virus o worms o trojans natural disasters hw failures sw failures espionage	Users Software vulnerabilities o buffer overruns o design o input configuration	prevention o firewalls o updates o strong pw's o shutdown unused services o physical detection o intrusions o ports o vigilance correction recovery o backups

CIA Triad Principles behind Security(p. 674)

- Confidentiality
- Integrity

- Availability

Certifications

- CISSP
- SANS
- CISA

Standards

- U.S. Legislations: HIPAA, FISMA, Sarbanes-Oxley
- ISO/IEC 17799
    - Risk Assessment
    - Security policy - management direction
    - Organization of information security - governance of information security
    - Asset management - inventory and classification of information assets
    - Human resources security - security aspects for employees joining, moving and leaving an organization
    - Physical and environmental security - protection of the computer facilities
    - Communications and operations management - management of technical security controls in systems and networks
    - Access control - restriction of access rights to networks, systems, applications, functions and data
    - Information systems acquisition, development and maintenance - building security into applications
    - Information security incident management - anticipating and responding appropriately to information security breaches
    - Business continuity management - protecting, maintaining and recovering business-critical processes and systems
    - Compliance - ensuring conformance with information security policies, standards, laws and regulations
- PCI DSS
    * Build and Maintain a Secure Network
        - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
        - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
    * Protect Cardholder Data
        - Requirement 3: Protect stored cardholder data
        - Requirement 4: Encrypt transmission of cardholder data across open, public networks
    * Maintain a Vulnerability Management Program
        - Requirement 5: Use and regularly update anti-virus software
        - Requirement 6: Develop and maintain secure systems and applications
    * Implement Strong Access Control Measures
        - Requirement 7: Restrict access to cardholder data by business need-to-know
        - Requirement 8: Assign a unique ID to each person with computer access
        - Requirement 9: Restrict physical access to cardholder data
    * Regularly Monitor and Test Networks
        - Requirement 10: Track and monitor all access to network resources and cardholder data
        - Requirement 11: Regularly test security systems and processes
    * Maintain an Information Security Policy
        - Requirement 12: Maintain a policy that addresses information security

Vulnerabilities:

RH9 root login via grub single user boot

1. enter grub using e command
2. add “single” to end of kernel command
3. boot with b command
4. use passwd to set new password

Safeguard:

1. vi /etc/inittab
2. In #System initialization section add:
   s0:S:wait:/sbin/sulogin

```
     after:
          si::sysinit:etc/rc.d/...

RH9 alternate root login with no password (like admin)
  1. add user
  2. remove MD5 password from /etc/shadow
Safeguard:
  1. add MD5 password to /etc/shadow
To print out users with no passwords:
     perl -F: -ane 'print if not $F[1];' /etc/shadow
To print out UID=0 root users:
     perl -F: -ane 'print if not $F[2];' /etc/passwd


Windows single partition is a vulnerable to a user filling
the partition full with data which will choke the OS
(Denial of Service)
```

Commands:

```
fdisk –l       Shows current disk partitions
mount          Shows how key directories are mounted
passwd         Change password
ps –e          Show current processes
ps -ef         Show current processes and their owners

service xxx start   start xxx service
service xxx stop    stop xxx service
                   (use for non-essential services)
service xxx status  status of xxx service

Print out users with no passwords:
     perl -F: -ane 'print if not $F[1];' /etc/shadow

Force password aging:
     sudo chage –m 2 –M 90 –E 2007-07-31 –W 14 rsimms
       o  minimum days between changes: 2
       o  maximum days between changes: 90
       o  expiration date: July 31, 2007
       o  # days to warn the user before expiring: 14
```

Permissions

```
– – –  – – –  – – –  – – –
```

```
s s t  r w x  r w x  r w x

s s t = setuid  setgid sticky-bit

sticky-bit
  o  1777 = rwx rwx rwt
  o  ls –ld /tmp
  o  all users can read, but only owners can modify

setuid
  o  can be used to run a file as its owner rather the the
     user that is running it.  Allows running a file as
     root by non-root users (shows red in ls –l)
  o  ls –l /usr/bin/passwd
  o  4755 = rws r-x r-x
  o  chown root myfile
  o  chmod 4755 myfile
  o  chmod u+s myfile

setgid
  o  for directories, new files created in the directory
     inherit the group of the directory rather than the
     group of the user creating the file.  All files
     created in the directory will have the same group.
     New subdirectories will inherit the setgid bit (these
     files show green in ls –l)
  o  ls –l /usr/bin/wall
  o  2777 = rwx rws rwx
  o  chmod 2777 mydir
  o  or chmod g+s mydir
```

Tools

```
bastille (http://www.bastille-linux.org/)

rpm –hiv Bastille-3.0.9-1.0.noarch.rpm

rpm –hiv perl-Curses-1.20-1.rh9.rf.i386.rpm       (TUI)
     or
rpm –hiv perl-Tk-804.028-2.rh9.rf.i386.rpm        (GUI)


bastille –-assess             (generate html report)
bastille -[c|x] --os RH9      (harden)
bastille –r                   (revert to previous settings)
```

bastille –b (batch mode)

bastille -[c|x] --os RH9

To achieve 9.43/10 use:

File Permissions

- Set more restrictive permissions to the administrative utilities [y]
- Disable all setuid programs except for the X server, (XFree86).
- Disable the r-tools.

Account Security

- Disable clear text r-protocols
- Enforce password aging
- Disable cron use for all except super user
- Set the default umask to 027
- Prohibit root logins from using ttys 1-6

Boot Security

- Password protect GRUB
- Disable ctrl-alt-del from rebooting
- Password protect single-user mode

Restricting Xinetd

- Create a default deny on TCPWrappers under xinetd, except sshd and sendmail. Note: Bastille already excepts sshd; you will have to add the exception for sendmail.
- Display Authorized Use messages at log-in
- Granting authorization: its owner
- Disable telnet and ftp from running under xinetd.

Configure Misc PAM

- Set limits on system resource usage /etc/security/limits.conf
- restrict console access to root and rsimms

Logging

- Setup additional logging
- Setup process accounting

Disable User Tools

1. Disable the r-tools
2. Disable gcc and g++

Restricting other daemons

- Disable the following daemons from running at boot time.
  * acpid and/or apmd
  * NFS and Samba
  * PCMCIA
  * GPM
  * HP OfficeJet
  * ISDN
  * dhcpd and innd
  * routed and gated
  * nis server and client
  * snmpd and kudzu daemons

- Do not restrict sendmail
- Restrict all the httpd features like cgi-scripts, ssi and symlinks.
- Restrict the FTP features like anonymous ftp.
- Disable Printing (CUPS) and DNS
- Install TMPDIR/TMP scripts

Packet Filtering

- Do not implement packet filtering. Using Bastille's firewall complicates Linux's own netfilter settings which we will do later in the course.

nmap
-sT = try normal TCP ports in normal way:

```
[root@mitnick root]# nmap -sT 172.30.4.1

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (172.30.4.1):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
631/tcp    open        ipp
1024/tcp   open        kdm

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
[root@mitnick root]#
```

-O = try to figure out the OS:

```
[root@mitnick root]# nmap -O -sT 172.30.4.1

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (172.30.4.1):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
631/tcp    open        ipp
1024/tcp   open        kdm
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 6.912 days (since Mon Feb 11 19:16:41 2008)

Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
[root@mitnick root]#
```

Key configuration files:

/etc/passwd all users
/etc/shadow users and MD5 encrypted passwords

/etc/rc.d/rc3.d/ all run level 3 service scripts

Finding a string of text on a Linux file system:

```
find –mount
     -type f
     -exec grep –l “string” {} \;
```

```
Base 64 encoding
http://www.paulschou.com/tools/xlate/

A-Z for 0 to 25
a-z for 26 51
0-9 for 52-61
+ for 62
/ for 63

R05VL0xpbnV4 (base64) = GNU/Linux (ascii)
R05
     = 17 52 57(decimal)
     = 010001 110100 111001 (binary)
     = 0100 0111 0100 1110 01?? (binary)
     = 47 4E ?? (hex)
     = GN (ascii)
```

0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/

Character Name	Char	Code	Decimal	Binary	Hex
Null	NUL	Ctrl @	0	00000000	00
Start of Heading	SOH	Ctrl A	1	00000001	01
Start of Text	STX	Ctrl B	2	00000010	02

End of Text	ETX	Ctrl C	3	00000011	03
End of Transmit	EOT	Ctrl D	4	00000100	04
Enquiry	ENQ	Ctrl E	5	00000101	05
Acknowledge	ACK	Ctrl F	6	00000110	06
Bell	BEL	Ctrl G	7	00000111	07
Back Space	BS	Ctrl H	8	00001000	08
Horizontal Tab	TAB	Ctrl I	9	00001001	09
Line Feed	LF	Ctrl J	10	00001010	0A
Vertical Tab	VT	Ctrl K	11	00001011	0B
Form Feed	FF	Ctrl L	12	00001100	0C
Carriage Return	CR	Ctrl M	13	00001101	0D
Shift Out	SO	Ctrl N	14	00001110	0E
Shift In	SI	Ctrl O	15	00001111	0F
Data Line Escape	DLE	Ctrl P	16	00010000	10
Device Control 1	DC1	Ctrl Q	17	00010001	11
Device Control 2	DC2	Ctrl R	18	00010010	12
Device Control 3	DC3	Ctrl S	19	00010011	13
Device Control 4	DC4	Ctrl T	20	00010100	14
Negative Acknowledge	NAK	Ctrl U	21	00010101	15
Synchronous Idle	SYN	Ctrl V	22	00010110	16
End of Transmit Block	ETB	Ctrl W	23	00010111	17
Cancel	CAN	Ctrl X	24	00011000	18
End of Medium	EM	Ctrl Y	25	00011001	19
Substitute	SUB	Ctrl Z	26	00011010	1A
Escape	ESC	Ctrl [	27	00011011	1B
File Separator	FS	Ctrl \	28	00011100	1C
Group Separator	GS	Ctrl]	29	00011101	1D
Record Separator	RS	Ctrl ^	30	00011110	1E
Unit Separator	US	Ctrl _	31	00011111	1F

Space			32	00100000	20
Exclamation Point	!	Shift 1	33	00100001	21
Double Quote	"	Shift ‘	34	00100010	22
Pound/Number Sign	#	Shift 3	35	00100011	23
Dollar Sign	$	Shift 4	36	00100100	24
Percent Sign	%	Shift 5	37	00100101	25
Ampersand	&	Shift 7	38	00100110	26
Single Quote	‘	‘	39	00100111	27
Left Parenthesis	(	Shift 9	40	00101000	28
Right Parenthesis	)	Shift 0	41	00101001	29
Asterisk	*	Shift 8	42	00101010	2A
Plus Sign	+	Shift =	43	00101011	2B
Comma	,	,	44	00101100	2C
Hyphen / Minus Sign	-	-	45	00101101	2D
Period	.	.	46	00101110	2E
Forward Slash	/	/	47	00101111	2F
Zero Digit	0	0	48	00110000	30
One Digit	1	1	49	00110001	31
Two Digit	2	2	50	00110010	32
Three Digit	3	3	51	00110011	33
Four Digit	4	4	52	00110100	34
Five Digit	5	5	53	00110101	35
Six Digit	6	6	54	00110110	36
Seven Digit	7	7	55	00110111	37
Eight Digit	8	8	56	00111000	38
Nine Digit	9	9	57	00111001	39
Colon	:	Shift ;	58	00111010	3A
Semicolon	;	;	59	00111011	3B
Less-Than Sign	<	Shift ,	60	00111100	3C

Equals Sign	=	=	61	00111101	3D
Greater-Than Sign	>	Shift .	62	00111110	3E
Question Mark	?	Shift /	63	00111111	3F
At Sign	@	Shift 2	64	01000000	40
Capital A	A	Shift A	65	01000001	41
Capital B	B	Shift B	66	01000010	42
Capital C	C	Shift C	67	01000011	43
Capital D	D	Shift D	68	01000100	44
Capital E	E	Shift E	69	01000101	45
Capital F	F	Shift F	70	01000110	46
Capital G	G	Shift G	71	01000111	47
Capital H	H	Shift H	72	01001000	48
Capital I	I	Shift I	73	01001001	49
Capital J	J	Shift J	74	01001010	4A
Capital K	K	Shift K	75	01001011	4B
Capital L	L	Shift L	76	01001100	4C
Capital M	M	Shift M	77	01001101	4D
Capital N	N	Shift N	78	01001110	4E
Capital O	O	Shift O	79	01001111	4F
Capital P	P	Shift P	80	01010000	50
Capital Q	Q	Shift Q	81	01010001	51
Capital R	R	Shift R	82	01010010	52
Capital S	S	Shift S	83	01010011	53
Capital T	T	Shift T	84	01010100	54
Capital U	U	Shift U	85	01010101	55
Capital V	V	Shift V	86	01010110	56
Capital W	W	Shift W	87	01010111	57
Capital X	X	Shift X	88	01011000	58
Capital Y	Y	Shift Y	89	01011001	59

Capital Z	Z	Shift Z	90	01011010	5A
Left Bracket	[	[	91	01011011	5B
Backward Slash	\	\	92	01011100	5C
Right Bracket	]	]	93	01011101	5D
Caret	^	Shift 6	94	01011110	5E
Underscore	_	Shift -	95	01011111	5F
Back Quote	`	`	96	01100000	60
Lower-case A	a	A	97	01100001	61
Lower-case B	b	B	98	01100010	62
Lower-case C	c	C	99	01100011	63
Lower-case D	d	D	100	01100100	64
Lower-case E	e	E	101	01100101	65
Lower-case F	f	F	102	01100110	66
Lower-case G	g	G	103	01100111	67
Lower-case H	h	H	104	01101000	68
Lower-case I	I	I	105	01101001	69
Lower-case J	j	J	106	01101010	6A
Lower-case K	k	K	107	01101011	6B
Lower-case L	l	L	108	01101100	6C
Lower-case M	m	M	109	01101101	6D
Lower-case N	n	N	110	01101110	6E
Lower-case O	o	O	111	01101111	6F
Lower-case P	p	P	112	01110000	70
Lower-case Q	q	Q	113	01110001	71
Lower-case R	r	R	114	01110010	72
Lower-case S	s	S	115	01110011	73
Lower-case T	t	T	116	01110100	74
Lower-case U	u	U	117	01110101	75
Lower-case V	v	V	118	01110110	76

Lower-case W	w	W	119	01110111	77
Lower-case X	x	X	120	01111000	78
Lower-case Y	y	Y	121	01111001	79
Lower-case Z	z	Z	122	01111010	7A
Left Brace	{	Shift [	123	01111011	7B
Vertical Bar	|	Shift \	124	01111100	7C
Right Brace	}	Shift]	125	01111101	7D
Tilde	~	Shift `	126	01111110	7E
Delta	Δ		127	01111111	7F