Austin Staton
Vice-President; UofSC Cybersecurity
October 8th, 2019

What is ~~Kali~~ Linux?

Why do we care?

What's better?

Windows, OSX, etc.

- Proprietary software
  - better support, but less customization
- Compatibility

Linux

- Open Source
- Performance
  - less Bloatware

What is Kali Linux?

- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

Popular Toolkits

- Nmap -- Port Scanning
- JohnTheRipper & RainbowCrack -- Password Cracking
- Radare2 -- Reverse Engineering
- Metasploit -- Penetration Testing
- Wireshark -- Packet Sniffing
- Scalpel -- Data Recovery

Nmap

- *Port Scanning* toolkit

- Commonly used for reconnaissance and vulnerability discovery

Nmap (cont.)

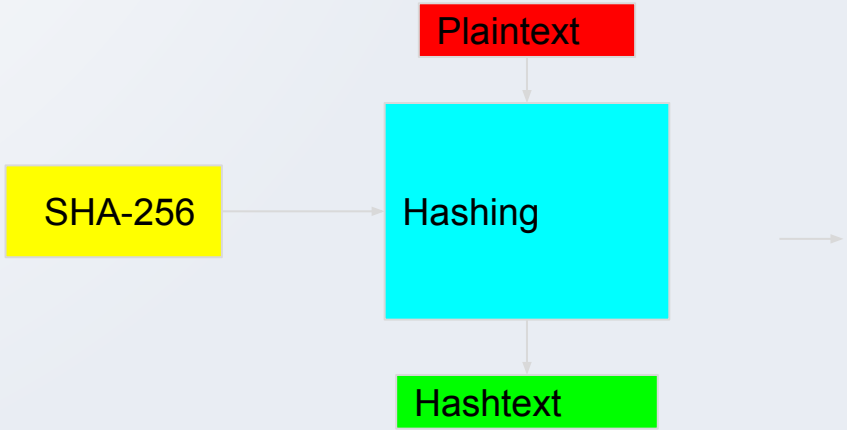
Nmap (cont.)

File: **nmapscan.txt**

```
/*************************************************************
** This command uses the nmap command to find open ports on a
** specified IP range.
**
** A "-timing <1-5>" option will speed up or slow down the port
** scan. 5 is fast end, slow is low.
*************************************************************
*/

nmap -sS -p 80,443,8080 --open --script http-title --script-args 'http.
useragent="Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Geck
o"' 10.10.2-6.0-254

// This works nearly the same. The "-timing" option described
// above was added.
nmap -sS -p 80,443,8080 --open --script http-title --script-args -timin
g 5 10.10.2-6.0-254

/*************************************************************
** This is a database scanning command with options that scan
** common mySQL ports. Looks for common vulnerabilities.
*************************************************************
*/

nmap -sS -p 1433,3306 --open --script ms-sql-info,ms-sql-empty-password
,mysql-info,mysql-empty-password 10.10.2-6.0-256

/*************************************************************
** This is an namp scan for FTP, SSH, and Telnet ports. It will
** check for anonymous FTP access.
*************************************************************
*/

nmap -sS -p 21,22,23 --open --script ftp-anon,banner 10.10.2-6.0-254
```

JohnTheRipper & RainbowCrack

- How are passwords stored?



https://hashes.org/leaks.php

JohnTheRipper & RainbowCrack (cont.)

User	Password
Stephen	auhsoJ
Lisa	hsifdrowS
James	1010NO1Z
Harry	sinocarD tupaC
Sarah	auhsoJ

User	Password Hash
Stephen	39e717cd3f5c4be78d97090c69f4e655
Lisa	f567c40623df407ba980bfad6dff5982
James	711f1f88006a48859616c3a5cbcc0377
Harry	fb74376102a049b9a7c5529784763c53
Sarah	39e717cd3f5c4be78d97090c69f4e655

User	Random Salt	Password Hash
Stephen	06917d7ed65c466fa180a6fb62313ab9	b65578786e544b6da70c3a9856cdb750
Lisa	51f2e43105164729bb46e7f20091adf8	2964e639aa7d457c8ec0358756cbffd9
James	fea659115b7541479c1f956a59f7ad2f	dd9e4cd20f134dda87f6ac771c48616f
Harry	30ebf72072134f1bb40faa8949db6e85	204767673a8d4fa9a7542ebc3eceb3a2
Sarah	711f51082ea84d949f6e3efecf29f270	e3afb27d59a34782b6b4baa0c37e2958

Figure 1. Password and Hash Tables

http://project-rainbowcrack.com/table.htm

Radare2

- What is Reverse Engineering?
  - High-Level Languages->...->Assembly ->...->Binaries

- How do we interpret these collections of numbers?

https://github.com/aj-staton/assembly/

OPCODES, BASE CONVERSION, ASCII SYMBOLS

③

MIPS opcode (31:26)	(1) MIPS funct (5:0)	(2) MIPS funct (5:0)	Binary	Decimal	Hexadecimal	ASCII Character	Decimal	Hexadecimal	ASCII Character
(1)	sll	add.*f*	00 0000	0	0	NUL	64	40	@
		sub.*f*	00 0001	1	1	SOH	65	41	A
j	srl	mul.*f*	00 0010	2	2	STX	66	42	B
jal	sra	div.*f*	00 0011	3	3	ETX	67	43	C
beq	sllv	sqrt.*f*	00 0100	4	4	EOT	68	44	D
bne		abs.*f*	00 0101	5	5	ENQ	69	45	E
blez	srlv	mov.*f*	00 0110	6	6	ACK	70	46	F
bgtz	srav	neg.*f*	00 0111	7	7	BEL	71	47	G
addi	jr		00 1000	8	8	BS	72	48	H
addiu	jalr		00 1001	9	9	HT	73	49	I
slti	movz		00 1010	10	a	LF	74	4a	J
sltiu	movn		00 1011	11	b	VT	75	4b	K
andi	syscall	round.*w.f*	00 1100	12	c	FF	76	4c	L
ori	break	trunc.*w.f*	00 1101	13	d	CR	77	4d	M
xori		ceil.*w.f*	00 1110	14	e	SO	78	4e	N
lui	sync	floor.*w.f*	00 1111	15	f	SI	79	4f	O
	mfhi		01 0000	16	10	DLE	80	50	P
(2)	mthi		01 0001	17	11	DC1	81	51	Q
	mflo	movz.*f*	01 0010	18	12	DC2	82	52	R
	mtlo	movn.*f*	01 0011	19	13	DC3	83	53	S
			01 0100	20	14	DC4	84	54	T
			01 0101	21	15	NAK	85	55	U
			01 0110	22	16	SYN	86	56	V
			01 0111	23	17	ETB	87	57	W
	mult		01 1000	24	18	CAN	88	58	X
	multu		01 1001	25	19	EM	89	59	Y
	div		01 1010	26	1a	SUB	90	5a	Z
	divu		01 1011	27	1b	ESC	91	5b	[
			01 1100	28	1c	FS	92	5c	\
			01 1101	29	1d	GS	93	5d	]
			01 1110	30	1e	RS	94	5e	^
			01 1111	31	1f	US	95	5f	_
lb	add	cvt.*s.f*	10 0000	32	20	Space	96	60	`
lh	addu	cvt.*d.f*	10 0001	33	21	!	97	61	a
lwl	sub		10 0010	34	22	"	98	62	b
lw	subu		10 0011	35	23	#	99	63	c
lbu	and	cvt.*w.f*	10 0100	36	24	$	100	64	d
lhu	or		10 0101	37	25	%	101	65	e
lwr	xor		10 0110	38	26	&	102	66	f
	nor		10 0111	39	27	'	103	67	g
sb			10 1000	40	28	(	104	68	h
sh			10 1001	41	29	)	105	69	i
swl	slt		10 1010	42	2a	*	106	6a	j
sw	sltu		10 1011	43	2b	+	107	6b	k
			10 1100	44	2c	,	108	6c	l
			10 1101	45	2d	-	109	6d	m
swr			10 1110	46	2e	.	110	6e	n
cache			10 1111	47	2f	/	111	6f	o
ll	tge	c.*f.f*	11 0000	48	30	0	112	70	p
lwc1	tgeu	c.un.*f*	11 0001	49	31	1	113	71	q
lwc2	tlt	c.eq.*f*	11 0010	50	32	2	114	72	r
pref	tltu	c.ueq.*f*	11 0011	51	33	3	115	73	s
	teq	c.olt.*f*	11 0100	52	34	4	116	74	t
ldc1		c.ult.*f*	11 0101	53	35	5	117	75	u
ldc2	tne	c.ole.*f*	11 0110	54	36	6	118	76	v
		c.ule.*f*	11 0111	55	37	7	119	77	w
sc		c.sf.*f*	11 1000	56	38	8	120	78	x
swc1		c.ngle.*f*	11 1001	57	39	9	121	79	y
swc2		c.seq.*f*	11 1010	58	3a	:	122	7a	z
		c.ngl.*f*	11 1011	59	3b	;	123	7b	{
		c.lt.*f*	11 1100	60	3c	<	124	7c	|
sdc1		c.nge.*f*	11 1101	61	3d	=	125	7d	}
sdc2		c.le.*f*	11 1110	62	3e	>	126	7e	~
		c.ngt.*f*	11 1111	63	3f	?	127	7f	DEL

(1) opcode(31:26) == 0

(2) opcode(31:26) == 17_{ten} (11_{hex}); if fmt(25:21)== 16_{ten} (10_{hex}) *f* = s (single); if fmt(25:21)==17_{ten} (11_{hex}) *f* = d (double)

IEEE 754 FLOATING-POINT STANDARD

$(-1)^S \times (1 + \text{Fraction}) \times 2^{(\text{Exponent} - \text{Bias})}$

where Single Precision Bias = 127, Double Precision Bias = 1023.

IEEE Single Precision and Double Precision Formats:

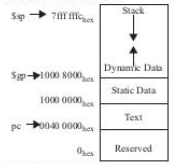
④

IEEE 754 Symbols

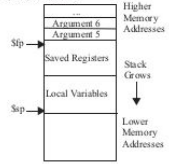
Exponent	Fraction	Object
0	0	± 0
0	≠0	± Denorm
1 to MAX - 1	anything	± Fl. Pt. Num.
MAX	0	±∞
MAX	≠0	NaN

S.P. MAX = 255, D.P. MAX = 2047

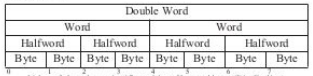
MEMORY ALLOCATION



STACK FRAME

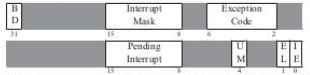


DATA ALIGNMENT



Value of three least significant bits of byte address (Big Endian)

EXCEPTION CONTROL REGISTERS: CAUSE AND STATUS



BD = Branch Delay, UM = User Mode, EL = Exception Level, IE =Interrupt Enable

EXCEPTION CODES

Number	Name	Cause of Exception	Number	Name	Cause of Exception
0	Int	Interrupt (hardware)	9	Bp	Breakpoint Exception
4	AdEL	Address Error Exception (load or instruction fetch)	10	RI	Reserved Instruction Exception
5	AdES	Address Error Exception (store)	11	CpU	Coprocessor Unimplemented
6	IBE	Bus Error on Instruction Fetch	12	Ov	Arithmetic Overflow Exception
7	DBE	Bus Error on Load or Store	13	Tr	Trap
8	Sys	Syscall Exception	15	FPE	Floating Point Exception

SIZE PREFIXES (10^x for Disk, Communication; 2^x for Memory)

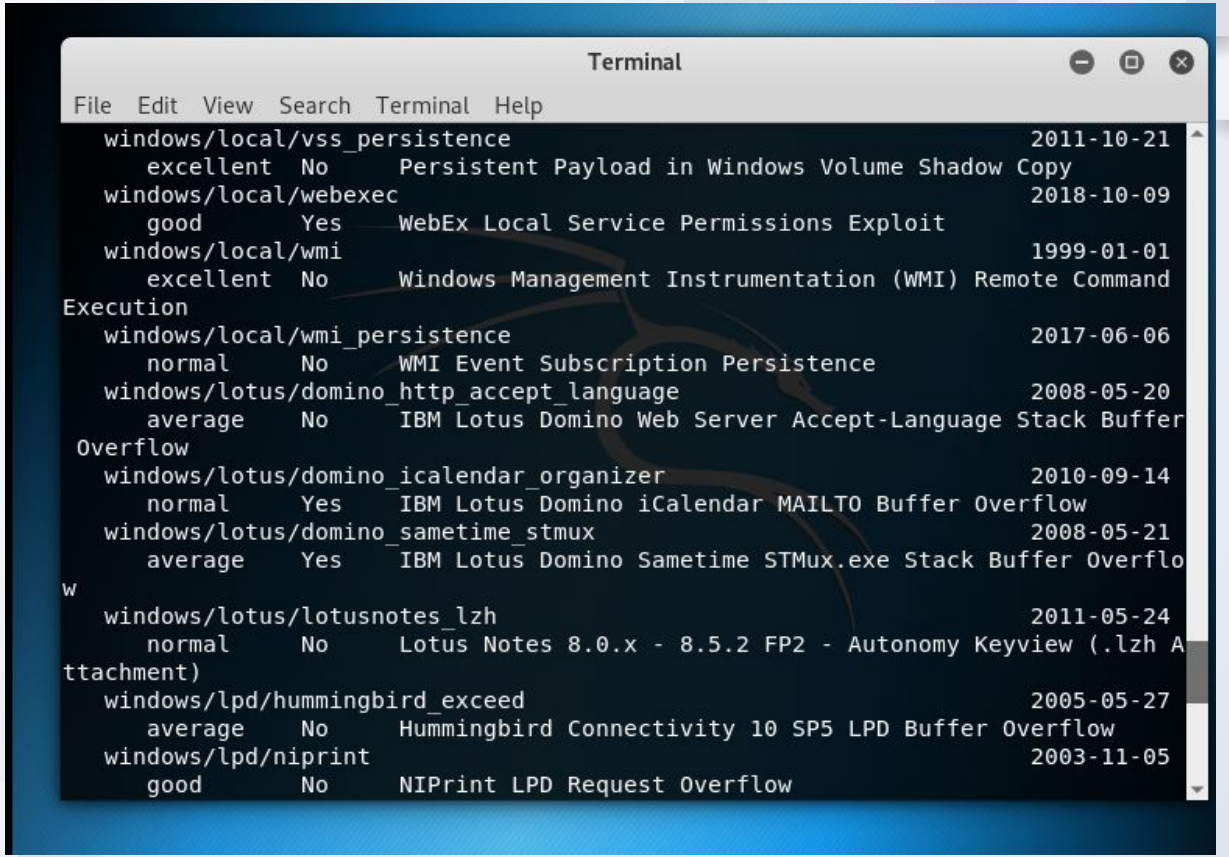
SI Size	Prefix	Symbol	IEC Size	Prefix	Symbol
10^3	Kilo-	K	2^{10}	Kibi-	Ki
10^6	Mega-	M	2^{20}	Mebi-	Mi
10^9	Giga-	G	2^{30}	Gibi-	Gi
10^{12}	Tera-	T	2^{40}	Tebi-	Ti
10^{15}	Peta-	P	2^{50}	Pebi-	Pi
10^{18}	Exa-	E	2^{60}	Exbi-	Ei
10^{21}	Zetta-	Z	2^{70}	Zebi-	Zi
10^{24}	Yotta-	Y	2^{80}	Yobi-	Yi

MIPS Reference Data Card ("Green Card") 1. Pull along perforation to separate card 2. Fold bottom side (columns 3 and 4) together

Metasploit

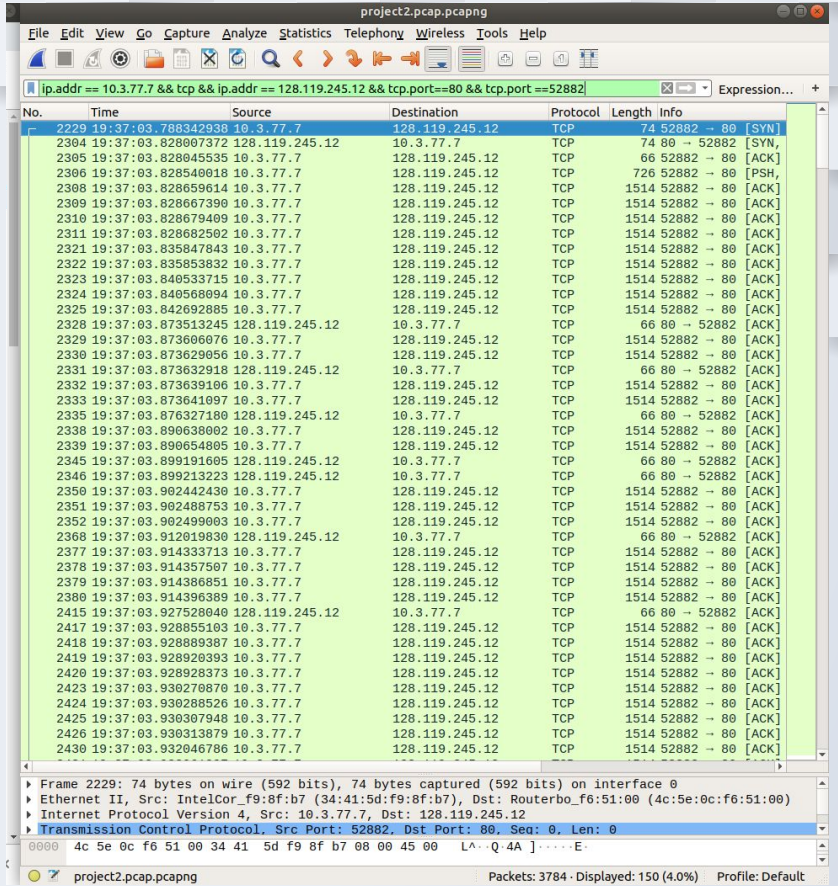
- Metasploit is a toolkit that stores vulnerabilities, along with their exploits.

- Mainly used as a Penetration Testing toolkit.


Terminal
File Edit View Search Terminal Help
windows/local/vss_persistence 2011-10-21
excellent No Persistent Payload in Windows Volume Shadow Copy
windows/local/webexec 2018-10-09
good Yes WebEx Local Service Permissions Exploit
windows/local/wmi 1999-01-01
excellent No Windows Management Instrumentation (WMI) Remote Command Execution
windows/local/wmi_persistence 2017-06-06
normal No WMI Event Subscription Persistence
windows/lotus/domino_http_accept_language 2008-05-20
average No IBM Lotus Domino Web Server Accept-Language Stack Buffer Overflow
windows/lotus/domino_icalendar_organizer 2010-09-14
normal Yes IBM Lotus Domino iCalendar MAILTO Buffer Overflow
windows/lotus/domino_sametime_stmux 2008-05-21
average Yes IBM Lotus Domino Sametime STMux.exe Stack Buffer Overflow
windows/lotus/lotusnotes_lzh 2011-05-24
normal No Lotus Notes 8.0.x - 8.5.2 FP2 - Autonomy Keyview (.lzh Attachment)
windows/lpd/hummingbird_exceed 2005-05-27
average No Hummingbird Connectivity 10 SP5 LPD Buffer Overflow
windows/lpd/niprint 2003-11-05
good No NIPrint LPD Request Overflow

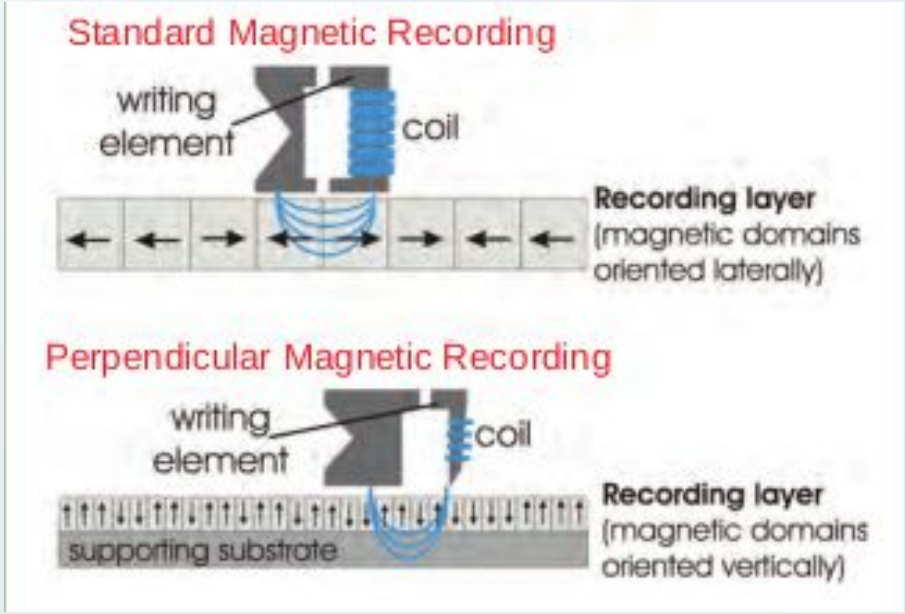
Wireshark

- Monitors network traffic
- Can be used to intercept passwords, files, or other desired information



Scalpel

- How is data stored on a disk?



Scalpel (cont.)

- File Signatures (a.k.a. “Magic Numbers”) identify the leading, and occasionally trailing, bits of a file.
- This strategy of data recovery relies on no specific file system.

File Type	Leading Bits	Trailing Bits
JPEG	0xFFD8FFE3	0xFFD9

https://filesignatures.net/index.php

Questions?

Resources

- www.overthewire.org -- Bandit War Games
- www.kali.org -- Kali Linux Image Download

- UofSC Cybersecurity:
  - Mondays at 1900 in SWGN 2A14

My Email Address:

me@gmail.com