

More about SANSFIRE, the ISC Conference: <http://isc.sans.org/sansfire>

SANS Internet Storm Center - <http://isc.sans.org>

Updates/Suggestions: <http://isc.sans.org/contact.html>

IP Address Information

ISC Summary: [http://isc.sans.org/ipinfo.html?ip=\[ip address\]](http://isc.sans.org/ipinfo.html?ip=[ip address]) for automated systems:

[http://isc.sans.org/ipinfo_ascii.html?ip=\[ip address\]](http://isc.sans.org/ipinfo_ascii.html?ip=[ip address])

Automated Malware Analysis

Virustotal: <http://www.virustotal.com>

Jotti's Malware Scan: <http://virusscan.jotti.org>

Sunbelt: <http://research.sunbelt-software.com/Submit.aspx>

Norman: <http://www.norman.com/microsites/nsic>

Threat Information and Internet Status

Shadowserver: <http://www.shadowserver.org>

Emerging Threats: <http://www.emergingthreats.org>

Malware Threat Center: <http://mtc.sri.com>

Castlecops: <http://www.castlecops.com>

Senderbase: <http://www.senderbase.com>

National Vulnerability Database: <http://nvd.nist.gov>

Mitre CVE: <http://cve.mitre.org>

Useful Tools

Sysinternals <http://technet.microsoft.com/en-us/sysinternals/default.aspx>

HiJackThis http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis

Sysinfo CLSIDs/Startup Info: <http://www.sysinfo.org>

<http://www.processlibrary.com>

<http://www.bleepingcomputer.com/filedb>

Services to Block Malicious Web Sites

Siteadvisor <http://www.siteadvisor.com>

Linkscanner <http://linkscanner.explabs.com>

OpenDNS <http://www.opendns.org>

Blacklist Checks

<http://relays.osirusoft.com/cgi-bin/rbcheck.cgi>

<http://www.mailradar.com/rbl>

PGP Keys: <https://isc.sans.org/PGPKEYS>; ID: 1F9D024D fingerprint 61A5 C22B 65C0 7740 8D21 E563 BC84 3887 1F9D 024D

Unix Commands	
<code>cut -f 1 -d ' '</code>	cut the first column from a file. Consider space (' ') as delimiter
<code>df</code>	check free disk space
<code>du</code>	list disk usage of each directory
<code>find</code>	find files
<code>grep -a "needle" file</code>	same, but treat binary file like ASCII
<code>grep -c "needle" file</code>	count lines that contain "needle"
<code>grep -v "needle" file</code>	return lines that DO NOT contain "needle"
<code>grep "needle" file</code>	extract all lines that contain "needle" from file
<code>history</code>	review recent commands
<code>id</code>	who am I?
<code>ls</code>	directory listing
<code>sort</code>	sort a file line by line
<code>sort -u</code>	sort, and only show unique lines
<code>strings</code>	extract printable strings from file
<code>uniq</code>	unique lines from sorted file

Top 10 sources from a tcpdump capture:

```
tcpdump -nr dumpfile | cut -f3 -d' ' | cut -f1-4 -d'.' | sort | uniq -c | sort -nr | head -10
```

Top 10 referrers from Apache access log:

```
cat access_log | cut -d' ' -f11 | cut -d '/' -f3 | sort | uniq -c | sort -nr | head -10
```

Windows Commands

(not all commands are available in all windows versions)

runas: run a program as a different user

assoc: associate programs with extensions

netsh: Network configuration tool (type '?' to get help)

sc: control services (startup / shutdown / auto-start on boot)

sigverif: Verify driver signatures

Kill Process: `wmic process [pid] delete`

`wmic process where name='cmd.exe' delete`

List local users: `wmic useraccount list full`

Startup Programs: `wmic startup list full`

use wmic on remote system: `wmic /user:userID /`

`password:password /node:hostname share list full`

More: <http://blogs.technet.com/jhoward/archive/2005/02/23/378726.aspx>,

<http://isc.sans.org/diary.html?storyid=1229>

Frequently Scanned Ports

also see [http://isc.sans.org/port.html?port=\[portnumber\]](http://isc.sans.org/port.html?port=[portnumber])

Port	Service
21	FTP
23	telnet
25	SMTP (Sendmail)
53	DNS
67, 68	DHCP
80	Web
113	authd/ident
135	Windows Name Resolution
137	Windows File Sharing
139	Windows File Sharing
143	IMAP
161	SNMP
443	HTTPS
445	Common Internet File System
1026	Windows RPC
1027	Windows RPC
1028	Windows RPC
1080	Proxy Server
1433	SQL Server (connect)
1434	SQL Server (Slammer Worm)
2967	Symantec System Center
3128	Squid Proxy
3306	MySQL
3389	MS Terminal Services
4662	eMule P2P file sharing
4672	eMule P2P file sharing
4672	remote access server
4899	remote admin
5060	SIP (VoIP)
5900	VNC
6881	Bittorrent
8000	irdmi/http
8010	Wingate / HTTP

IPv4 Header																															
Byte 0							Byte 1							Byte 2							Byte 3										
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Version							Length							TOS							Total Packet Length										
IP ID / Fragment ID														X	D	M	F	Fragment Offset													
TTL							Protocol							Checksum																	
Source Address																															
Destination Address																															

IPv6 Header																															
Byte 0							Byte 1							Byte 2							Byte 3										
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Version							Traffic Class							Flow Label																	
Payload Length														Next Header							Hop Limit										
Source Address (128 bits, 16 bytes)																															
Destination Address (128 bits, 16 bytes)																															

Protocols			
1	ICMP	51	AH
2	IGMP	55	IP Mobility
4	IP in IP	58	IPv6 ICMP
6	TCP	59	IPv6 no header
8	EGP	60	IPv6 Options
9	IGP	88	EIGRP
17	UDP	89	OSPF/IGP
41	IPv6 in IPv4	111	IPX in IP
43	IPv6 Routing	115	L2TP
44	IPv6 Fragment	133	FC
47	GRE	135	Mobility
50	ESP	255	Reserved

<http://www.iana.org/assignments/protocol-numbers>
<http://www.networksorcery.com>

ASCII/HEX Lookup																
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	TAB	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2	SPC	!	"	#	\$	%	&	()	*	+	,	-	.	/	
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL

HEX/DEC Conversion																
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
3	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
4	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
5	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
6	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
7	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
8	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
9	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
A	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
B	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
C	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
D	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
E	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
F	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

© 2008 SANS Institute - unaltered redistribution permitted

Outshare the bad guys! Submit your observations at <https://isc.sans.org/contact.html>

Compare Window to Unix shell commands		
Windows	Unix	
assign / mklink	ln -s	create symbolic link
cacls	chmod	change file permissions
chdir	pwd	display current directory
cls	clear	clear screen
comp / fc	diff	compare files
copy	cp	
date/time	date	show date or time
del/erase	rm	delete file
dir	ls	directory listing
doskey /h	history	get recent commands
find	grep	find matching lines
format	mke2fs	format a disk
help	man	get help
ipconfig	ifconfig	check network configuration
mkdir/md	mkdir	create directory
netstat	netstat	network info
print	lpr	print file
shutdown -r -t 0	shutdown -r now	reboot system
rename/move	mv	rename file or move file
route print	route -n	check routing configuration
tasklist	ps	list of running programs
tracert	tracert	trace route
type	cat	print file content
ver	uname -a	OS version

Convert Windows text files to Unix (remove CR and ^Z):
| tr -d '\15\32' < windows.txt > unix.txt |
Convert Unix text file to Windows:
| awk 'sub("\$", "\r")' unix.txt > windows.txt |
Note: Unix/Windows variation vary. (see <http://bhami.com/rosetta.html>) Consider the following extensions to add Unix-like commands to Windows: <http://www.cygwin.com>, <http://gnuwin32.sourceforge.net>, <http://unxutils.sourceforge.net>. Also look for Microsoft's "Windows Services for Unix".