Security+ Commands for Windows and Linux Cheat Sheet

by Nero via cheatography.com/148398/cs/32366/

Networking

Windows	Linux	
tracert	traceroute	displays possible routes and measuring transit delays of packets
nslookup	nslook-up/dig	determines the IP address associated with a domain name, obtain the mail server settings for a domain
ipconfig	ifconfig	displays all the network configura-tions of the currently connected network devices and can modify the DHCP & DNS settings
nmap	nmap	open-source network scanner that is used to discover hosts and services on a computer network by sending packets and analyzing their responses
pathping		used to determine if a host is reachable
hping	hping	open-source packet generator and analyzer for the TCP/IP protocol that is used for security auditing and testing of firewalls and networks

Networking (cont)

netstat	netstat	displays network connections for TCP, routing tables, and a number of network interface and network protocol stats
	netcat	for reading from and writing to network connections using TCP or UDP which is dependable back-end that can be used directly or easily driven by other programs and scripts
arp	arp	utility for viewing and modifying the local Address Resolution Protocol (ARP) cache on a given host or server
route	route	used to view and manipulate the IP routing tables on a host or server
curl	curl	tool to transfer data to or from a server, using any of the supported protocol (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP, or FILE)

Networking (cont)

the harvester	the harvester	python script that is used to gather emails, subdom-ains, hosts, employee, names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN database
sn1per	sn1per	an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabi-lities across a network
scanless	scanless	used to create an exploitation website that can perform open port scans in a more stealth-like manner
dnsenum	dnsenum	used for DNS enumeration to locate all DNS servers and DNS entries for a given organization
Nessus	Nessus	proprietary vulner-ability scanner that can remotely scan a computer or network for vulner-abilities
Cuckoo	Cuckoo	open source software for automating analysis of suspicious files

By **Nero**
cheatography.com/nero/

Published 8th June, 2022.
Last updated 8th June, 2022.

File Manipulation

Linux	
head	command-line utility for outputting the first ten lines of a file provided
tail	command-line utility for outputting the last ten lines of a file provided to it
cat	command-line utility for outputting the content of a file to the screen
grep	command-line utility for searching plain-text data sets for lines that match a regular expression or patter
chmod	command-line utility used to change the access permissions of file system objects
logger	utility that provides an easy way to add messages to the /var/log/-syslog files from the command line or from other files

Packet Capture

Windows	Linux	
windump	tcpdump	a suite of free open source utilities for editing and replaying previously captured network traffic
Wireshark	Wireshark	a popular network analysis tool to capture network packets and display them at a granular level for real-time or offline analysis

Exploitation

Metasploit (msfco-nsole)	Metasploit (msfco-nsole)	a computer security tool that offers information about software vulnerabilities, IDS signature development, and improves penetration test
Browser Exploi-tation Framework (BeEF)	Browser Exploi-tation Framework (BeEF)	a tool that can hook one or more browsers and can use them as a beachhead of launching various direct commands and further attack against the system from within the browser

Exploitation (cont)

Cain and Abel (cain)	Cain and Abel (cain)	a password recovery tool that can be used through sniffing the network, cracking encrypted passwords using dictio-nary, brute-force and cryptanalysis attack, recording VoIP conver-sations, decoding scrambled passwords, revealing password boxes, and analyzing routing protocols
John the Ripper (john)	John the Ripper (john	an open source password security auditing and password recovery tool available for many operating systems

Shells and Scripts

Windows	Linux	
SSH	SSH	utility that supports encrypted data transfer between two computers for secure logins, file transfers, or general purpose connectons
PowerShell		a task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language
Python	Python	An interpreted, high-level and general-purpose programming language
OpenSSL	OpenSSL	a software library for applic-ation that secure communications over computer networks against eavesdropping or need to identify the party at the other end

Forensics

Windows	Linux	
	dd	a command line utility to copy disk images using a bit by bit copying process

Forensics (cont)

FTK Imager	FTK Imager	a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is needed
	memdump	a command line utility to dump system memory to the standard output stream by skipping over holes in memory maps
WinHex	WinHex	a commercial disk editor and universal hexade-cimal editor used for recovery and digital forensics
Autopsy	Autopsy	a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics