《内网安全攻防:渗透测试实战指南》

第 1 章

链接 1-1

https://www.virtualbox.org

链接 1-2

https://my.vmware.com/web/vmware/downloads

链接 1-3

http://www.kali.org/downloads/

链接 1-4

http://www.offensive-security.com/kali-linux-vmware-arm-image-download

链接 1-5

https://www.ampliasecurity.com/research/windows-credentials-editor/

链接 1-6

https://github.com/gentilkiwi/mimikatz/releases/latest

链接 1-7

http://beefproject.com

链接 1-8

https://storage.googleapis.com/google-code-archive-source/v2/code.google.com/ptscripts/source-archive.zip

链接 1-9

https://github.com/PowerShellMafia/PowerSploit.git

链接 1-10

https://github.com/samratashok/nishang.git

链接 1-11

https://raw.githubusercontent.com/darkoperator/powershell_scripts/master/ps_encoder.py

链接 1-12

https://github.com/brav0hax/smbexec

链接 1-13

https://github.com/secretsquirrel/the-backdoor-factory.git

链接 1-14

https://github.com/Veil-Framework/Veil.git

链接 1-15

https://www.metasploit.com/

链接 1-16

https://www.cobaltstrike.com/

链接 1-17

http://www.oxid.it/cain.html

链接 1-18

https://github.com/mattifestation/PowerSploit

链接 1-19

https://github.com/samratashok/nishang

链接 1-20

https://raw.githubusercontent.com/cheetz/PowerSploit/master/CodeExecution/Invoke--Shellcode.ps1

链接 1-21

https://raw.githubusercontent.com/darkoperator/powershell_scripts/master/ps_encoder.py

链接 1-22

https://www.pstips.net/powershell-online-tutorials

链接 1-23

http://sourceforge.net/projects/metasploitable/files/Measploitable2

链接 1-24

https://github.com/rapid7/metasploitable3

链接 1-25

https://sourceforge.net/projects/owaspbwa/files/

链接 1-26

https://www.hackthissite.org/

第 2 章

链接 2-1

http://www.fuzzysecurity.com/scripts/files/wmic_info.rar

链接 2-2

http://www.securityfocus.com/bid

链接 2-3

http://www.exploit-db.com

链接 2-4

https://docs.microsoft.com/en-us/sysinternals/downloads/psloggedon

链接 2-5

https://github.com/chrisdee/Tools/tree/master/AD/ADFindUsersLoggedOn

链接 2-6

https://github.com/mubix/netview

链接 2-7

https://nmap.org/nsedoc/scripts/smb-enum-sessions.html

链接 2-8

https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView

链接 2-9

https://github.com/nullbind/Other-Projects/tree/master/GDA

链接 2-10

https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1

链接 2-11

https://github.com/BloodHoundAD/BloodHound/releases/download/2.0.4/BloodHound-win32-x64.zip

链接 2-12

https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.ps1

链接 2-13

https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/BloodHound_Old.ps1

链接 2-14

https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.exe

第 3 章

链接 3-1

https://curl.haxx.se/download/

链接 3-2

https://github.com/inquisb/icmpsh.git

链接 3-3

http://freshmeat.sourceforge.net/projects/ptunnel/

链接 3-4

http://www.tcpdump.org/release/libpcap-1.9.0.tar.gz

链接 3-5

http://sourceforge.net/projects/netcat/files/netcat/0.7.1/netcat-0.7.1.tar.gz/download

链接 3-6

https://joncraton.org/files/nc111nt.zip

链接 3-7

https://joncraton.org/files/nc111nt_safe.zip

链接 3-8

https://github.com/besimorhino/powercat.git

链接 3-9

https://github.com/iagox86/dnscat2.git

链接 3-10

https://github.com/besimorhino/powercat

链接 3-11

https://github.com/sensepost/reGeorg

链接 3-12

https://github.com/iagox86/dnscat2

链接 3-13

https://downloads.skullsecurity.org/dnscat2/

链接 3-14

https://github.com/lukebaggett/dnscat2-powershell

链接 3-15

https://raw.githubusercontent.com/lukebaggett/dnscat2-powershell/master/dnscat2.ps1

链接 3-16

https://github.com/Al1ex/iodine

链接 3-17

http://code.kryo.se/iodine

链接 3-18

https://code.kryo.se/iodine/check-it

链接 3-19

https://github.com/rootkiter/EarthWorm

链接 3-20

https://github.com/rootkiter/Termite

链接 3-21

http://www.sockscap64.com

链接 3-22

https://www.proxifier.com/

链接 3-23

http://proxychains.sourceforge.net/

链接 3-24

https://www.7-zip.org/

第 4 章

链接 4-1

https://github.com/SecWiki/windows-kernel-exploits

链接 4-2

https://raw.githubusercontent.com/Ridter/Pentest/master/powershell/MyShell/Invoke-MS16-032.ps1

链接 4-3

https://github.com/GDSSecurity/Windows-Exploit-Suggester

链接 4-4

https://github.com/rasta-mouse/Sherlock

链接 4-5

https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1

链接 4-6

http://technet.microsoft.com/ZH-cn/sysinternals/bb664922

链接 4-7

https://github.com/foxglovesec/RottenPotato.git

链接 4-8

https://github.com/SpiderLabs/Responder.git

第 5 章

链接 5-1

http://technet.microsoft.com/en-us/sysinternals/dd996900.aspx

链接 5-2

https://github.com/hashcat/hashcat/archive/v5.1.0.zip

链接 5-3

https://hashcat.net/wiki/doku.php?id=example_hashes

链接 5-4

http://www.cmd5.com/

链接 5-5

http://www.xmd5.com/

链接 5-6

https://github.com/gentilkiwi/kekeo

链接 5-7

https://download.sysinternals.com/files/PSTools.zip

链接 5-8

https://github.com/sunorr/smbexec

链接 5-9

https://github.com/brav0hax/smbexec

链接 5-10

https://github.com/brav0hax/smbexec.git

链接 5-11

https://github.com/PyroTek3/PowerShell-AD-Recon

链接 5-12

https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Discover-PSMSSQLServers

链接 5-13

https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Discover-PSInterestingServices

链接 5-14

https://github.com/nidem/kerberoast

链接 5-15

http://mail.domain/owa/

链接 5-16

http://webmail.domain/owa/

链接 5-17

http://mail.domain/ecp/

链接 5-18

http://webmail.domain/ecp/

第 6 章

链接 6-1

https://raw.githubusercontent.com/borigue/ptscripts/master/windows/vssown.vbs

链接 6-2

https://github.com/libyal/libesedb/releases/download/20170121/libesedb-experimental-20170121.tar.gz

链接 6-3

https://github.com/csababarta/ntdsxtract.git

链接 6-4

https://github.com/zcgonvh/NTDSDumpEx/releases/download/v0.3/NTDSDumpEx.zip

链接 6-5

https://gist.github.com/monoxgas/9d238accd969550136db

链接 6-6

https://github.com/quarkslab/quarkspwdump

链接 6-7

http://ophcrack.sourceforge.net/tables.php

链接 6-8

https://www.somd5.com/

链接 6-9

https://hashkiller.co.uk/ntlm-decrypter.aspx

链接 6-10

http://finder.insidepro.com/

链接 6-11

https://crackstation.net/

链接 6-12

http://www.objectif-securite.ch/ophcrack.php

链接 6-13

http://cracker.offensive-security.com/index.php

链接 6-14

https://github.com/mubix/pykek

链接 6-15

https://technet.microsoft.com/library/security/ms14-068

第 7 章

链接 7-1

http://www.joeware.net/freetools/tools/adfind/

链接 7-2

https://github.com/GhostPack/Rubeus

链接 7-3

https://github.com/leechristensen/SpoolSample

第 8 章

链接 8-1

https://github.com/PowerShellMafia/PowerSploit/blob/master/Persistence/Persistence.psm1

链接 8-2

https://github.com/epinna/weevely3

第 9 章

链接 9-1

https://www.oracle.com

链接 9-2

https://github.com/rsmudge/cortana-scripts

链接 9-3

http://sleep.dashnine.org/manual/

链接 9-4

https://www.cobaltstrike.com/aggressor-script/index.html