

Aa

ACE [b1/p18] Automation, Coverage and Effectiveness

Active Directory - Attack with a Domain Admin account [b5/p67] Describes the usage of a new domain admin account to attack

Active Directory - DCShadow [b5/p77] Overview of DCShadow, a follow-up on DCSync

Active Directory - DCSync [b5/p75] Overview of the dcsync tool to replicate a domain controller

Active Directory - DCSync Example [b5/p76] How to effectively use DCSync to replicate a domain and use that info to create a Golden Ticket

Active Directory - Domain Dominance Defenses [b5/p80] How to defend against or detect domain attacks

Active Directory - Skeleton Key [b5/p73] Description of what a Skeleton Key is and what it does

Assumed Breach Test [b1/p23] Find vulnerabilities in the network once an attacker gained access to a system in the network. Great for Active Directory and file permissions!

Bb

Bridged Networking [b1/p59] Network mode for a VM that makes the guest look like it is on the same subnet as the host machine

Cc

Conclusion phase [b1/p64] Perform detailed analysis and retest. Report and discuss findings.

Crypt(3) Linux and Unix Password Representations [b4/p54] Describes Linux/Unix Password hashing using crypt(3)

Cryptanalysis attack [b1/p23] Test focussing on bypassing or breaking the encryption of data stored on a local system or across the network.

Ee

Empire - Additional Module Categories [b3/p92] Describes additional modules in Empire like management, persistence, recon, situational awareness and trolls/ploit

Empire - Features [b3/p88] Describes notable Empire features

Empire - Modules [b3/p91] Describes Empire modules for use

Empire - Powershell Modules [b3/p90] Describes the different modules for use within Empire

Ethical Hacking [b1/p9] Tools for dealing with threats, vulnerabilities, risks and exploits and using them in a professional manner

Exploit [b1/p9] The "vehicle" by which the attacker uses a vulnerability to cause damage to the target system

Exploitation [b1/p24] Exploit target systems to compromise them, getting control over them or causing a DDoS attack

Exploitation - Antivirus Evasion Tactics [b3/p63] Discusses several ways to evade AV software on target systems

Exploitation - Categories of Exploits [b3/p9] Describes 3 categories of exploits; server-side, client-side and local privilege escalation

Exploitation - Client-Side Exploits [b3/p11] Describes client-side exploits

Exploitation - Client-Side Software Inventory Tools [b3/p15] How to build an inventory of client-side software in use by the target

Exploitation - Controlling Services with SC [b3/p115] How to control services using the sc command

Exploitation - Determining Client-Side Programs in Use [b3/p14] How to discover programs used by the target to exploit

Exploitation - Dropping SMB Sessions [b3/p114] Describes how and why to drop a SMB session from the command line

Exploitation - Firewall Inbound Traffic [b3/p111] How to set up a rule to allow inbound traffic on Windows Firewall

Exploitation - Interacting with processes using WMIC [b3/p128] Additional commands to use with WMIC

Exploitation - Interacting with the registry [b3/p112] How to interact with the registry from the command line

Exploitation - Local Privilege Escalation Attack Categories [b3/p19] Describes 3 categories of Local Privilege Escalation attacks

Exploitation - Make a service run [b3/p126] Describes how to run an executable as a service in Windows for more than 30 seconds

Exploitation - Making Client Software Access Test Systems *[b3/p16]* Describes 4 ways to make a client connect to a test system

Exploitation - Mounting a Client-Side Exploit Campaign *[b3/p13]* Discusses two approaches to client-side attacks

Exploitation - Netcat Relay *[b3/p79]* Explains how to set up a netcat relay to establish a connection on a blocked port

Exploitation - Notable Client-Side Exploits *[b3/p12]* Discusses commonly used target applications of client-side exploitation

Exploitation - Pivot Through Metasploit Route Command *[b3/p51]* Describes how to set up a pivot through Metasploit using the route command

Exploitation - Post Pivot Relay *[b3/p78]* Explains how to set up a post pivot relay to access a blocked port on a target system

Exploitation - Post-Exploitation *[b3/p76]* Overview of the goal and meaning of post-exploitation

Exploitation - PsExec *[b3/p119]* Describes how to use PsExec to run a command remotely on a target machine

Exploitation - Risks of Exploitation *[b3/p7]* Discusses risks of exploitation

Exploitation - Searching The Filesystem *[b3/p107]* Describes how to search the file system for files

Exploitation - Service-side Exploits *[b3/p10]* Describes a service-side exploit

Exploitation - Setting up SMB Sessions *[b3/p113]* How to set up a SMB connection from the command line

Exploitation - Using sc to invoke an executable *[b3/p125]* Describes how to run an executable as a service in Windows

Exploitation - Using WMIC to Invoke a Program *[b3/p127]* Describes how to use WMIC to invoke a program remotely

Exploitation - Why Exploit? *[b3/p6]* Discusses reasons to exploit a system

Exploitation - Windows Command Line *[b3/p105]* Describes commands to analyse a system and scrape through files

Exploitation - Windows Command Live Variables *[b3/p106]* Useful environment variables in Windows

Exploitation - Windows Firewall *[b3/p110]* Introduction to use the netsh command

Gg

Google Search Directives for File Types *[b1/p150]* How to use Google to search for certain filetypes

Google Search Directives for Page Titles and URLs *[b1/p149]* How to use Google for pages that match the title of your search or a specific URL

Google Search Directives for Sites and Links *[b1/p148]* How to use Google to search within a given domain and show similar pages

Hh

Hashcat - Dictionaries and Word Mangling Rules *[b4/p96]* Discusses how Hashcat can work with dictionaries and word mangling

Hashcat - Files *[b4/p95]* Describes the different files Hashcat uses like potfiles, show and restore

Hashcat - Introduction *[b4/p93]* Overview of Hashcat

Hashcat - Most Common World Mangling Rules *[b4/p97]* Describes the most used word mangling rules for Hashcat

Hashcat - Specifying Hash Types *[b4/p94]* How to determine and specify the correct hash type for Hashcat

Hashcat - Status and Temp Sensor *[b4/p98]* Describes how you can monitor the status while Hashcat is running and the usage of the temp sensor

Hashdump *[b4/p60]* Explains the usage of the hashdump tool to obtain hashes from a Windows box

Host-Only Networking *[b1/p44]* Network mode for a VM that allows the guest VM only to reach the host and no other systems. Not used for testing.

Hydra *[b4/p36]* Overview of the password guessing tool Hydra

Hydra - pw-inspector *[b4/p36]* Describes the usage of pw-inspector in the Hydra suite

Ii

Injection Attacks [b5/p102] Overview of different injection attacks like XSRF, XSS, SQL and command injection

Injection Attacks - Command Injection [b5/p104] Overview of command injection

Injection Attacks - Downside of ping [b5/p107] Downside of ping when using it for command injection

Injection Attacks - More on ping [b5/p106] More reasons why ping is good command to use for command injection

Injection Attacks - Which Command to inject [b5/p105] Overview of commands to inject and in particular the ping command to test command injection

Jj

John The Ripper [b4/p85] Overview of John The Ripper

John The Ripper - Distributed John Cracking [b4/p91] Describes ways to speed up cracking by distributing the workload

John The Ripper - File and Cracking Modes [b4/p86] Describes the several modes for password cracking to use with John The Ripper

John The Ripper - Interpreting John's Output [b4/p89] How to interpret John's output correctly

John The Ripper - Speed [b4/p90] Describes various methods to speed up the password cracking process with John

John The Ripper - The john.pot file [b4/p87] Describes the contents and usage of the john.pot file

John The Ripper - The john.rec file [b4/p88] Describes the contents and usage of the john.rec file

Kk

Kerberos [b5/p5] Introduction to Kerberos

Kerberos - AS-REQ [b5/p9] Describes the Authentication Server Request step of the Kerberos authentication process

Kerberos - Authentication Flow [b5/p6]

Describes the authentication flow of Kerberos and the tickets that come with it

Kerberos - Defenses [b5/p21] A few steps how you could defend yourself against Kerberos attacks

Kerberos - Defenses (2) [b5/p22] More defenses against Kerberos attacks

Kerberos - Encryption Types [b5/p8] Describes which encryption types are supported by Kerberos

Kerberos - Golden Ticket [b5/p68] Introduction to the Golden Ticket of Kerberos and how to obtain it

Kerberos - Golden Ticket Creation [b5/p71] Explains how you can create a Golden Ticket with the necessary inputs using Mimikatz

Kerberos - Golden Ticket Creation (2) [b5/p72] How to use a Golden Ticket with Kerberos after creation

Kerberos - Golden Ticket Properties [b5/p70] Describes the contents of a Golden Ticket

Kerberos - Interesting Service Accounts to crack [b5/p15] A few examples of interesting service accounts and where to look for when finding a good service account to crack

Kerberos - Kerberoasting [b5/p13] Describes the overview of a Kerberoasting attack to use Kerberos to obtain further domain credentials

Kerberos - Kerberoasting (2) [b5/p14] Describes how a Kerberoasting attack works

Kerberos - Long-Term Keys [b5/p7] Describes three long term keys of Kerberos (client long-term, target long-term and KDC long-term keys)

Kerberos - NTLMv2 [b5/p28] Describes the sense of using NTLMv2 and when it's used in Kerberos environments

Kerberos - Over-Pass-The-Hash [b5/p20] Describes the usage of overpassing the hash (NTLM hash) to kick-off the Kerberos process

Kerberos - PAC Validation [b5/p12] Discusses how PAC validation is done and what "leaks" are available in a TGT or ST for this reason

Kerberos - Pass The Ticket Attack [b5/p18] Describes a Pass-The-Ticket attack using Mimikatz

Kerberos - Service Ticket [b5/p11] Describes the parts that the Service Ticket contains after receiving a TGS-REP (Ticket Granting Service Response)

Kerberos - Silver Ticket Attack [b5/p17] Overview of a Kerberos Silver Ticket Attack

Kerberos - Ticket Granting Ticket [b5/p10] Describes the contents of a TGT and how it's

encrypted. Also PAC is discussed (Privilege Attribute Certificate)

L

LANMAN and NTLMv1 Challenge/Response [b4/p51] Describes how LANMAN Challenge/Response is used in 3 pieces vs NTLMv1 usage

LANMAN Challenge/Response [b4/p50] Describes the usage of LANMAN Challenge/Response

LANMAN Hashes [b4/p47] Description of the LANMAN hash algorithm

Linux/Unix DES Password Scheme [b4/p55] Describes how Linux hashes are salted using DES

Linux/Unix MD5 Password Scheme [b4/p56] Describes how Linux hashes are salted using MD5

M

Metadata - Document Types [b1/p129] Document types that are rich of metadata

Metadata - Exiftool [b1/p132] The purpose, goals and functions of Exiftool

Metadata - Retrieving documents for metadata analysis [b1/p131] How to retrieve documents from the target organization for metadata analysis

Metadata - Strings command [b1/p133] How to use the strings command properly on Linux to gather metadata in different formats

Metadata - Useful entries [b1/p119] Useful pieces of metadata for reconnaissance

Metasploit - Components [b3/p25] Describes the components of Metasploit (documentation, user interfaces, modules, exploit creation tools & other items)

Metasploit - Exploits and Payloads [b3/p22] Describes how Metasploit is built up from exploits and payloads

Metasploit - Modules [b3/p27] Describes the modules in Metasploit (auxiliary, encodes, exploits, nops, payloads & post)

Metasploit - Payloads [b3/p31] Describes Metasploit payload types (singles, stagers & stages)

Metasploit - Pivoting [b4/p71] Describes how to pivot through Metasploit

Metasploit - PsExec and Pass-The-Hash [b4/p124] How to use hashes with psexec in Metasploit to perform pass-the-hash attacks

Metasploit - PsExec Module [b3/p121] Describes usage of the Metasploit PsExec module

Metasploit - User Interfaces [b3/p26] Discusses the Metasploit user interfaces (msfconsole, msfd, msfrpcd, msfcgi and msfvenom)

Metasploit - Windows Singles [b3/p32] Describes Metasploit Windows Single Payloads to use for exploitation

Metasploit - Windows Stagers [b3/p33] Describes Stagers for Windows to use in Metasploit

Meterpreter - Keylogger [b3/p50] Describes the functionality of the built-in keylogger of Meterpreter

Meterpreter - Networking Commands [b3/p47] Describes meterpreter networking commands like ipconfig, route and portfwd

Meterpreter - Priv getsystem command [b3/p53] Describes the use of the priv extension in Meterpreter to escalate privileges

Meterpreter - Process Commands [b3/p45] Describes various process command in Meterpreter (getpid, getuid, ps, kill, execute & migrate)

Mimikatz [b4/p61] Describes the usage of Mimikatz to obtain passwords from the memory (LSASS process) on Windows boxes

Moving Files - Additional Protocols [b4/p7] Describes some additional protocols to transfer files (Windows File Sharing, NFS & Netcat)

Moving files - Metasploit, paste and echo [b4/p8] Describes a few more ways to transfer files from/to a target (Meterpreter, echo and copy-paste)

Moving files - Protocols [b4/p6] Describes different protocols for file transfer (TFTP, FTP, SCP, HTTP)

Moving Files - Push vs Pull [b4/p5] Describes differences between pushing or pulling a file from/to a target machine

N

NAT Networking [b1/p44] Network mode for a VM that performs Network Address Translation on the packets, altering them and potentially dropping them if the NAT table fills up.

Nessus - Dangerous Plugins [b2/p91] Describes "dangerous plugins" in Nessus and how you can disable/enable them

Nessus - Plugin Feed Information [b2/p90]

Instructions how to record the plugin feed information before using Nessus in a scan

Netcat - Listener Grabbing Client Info [b2/p108]

/Describes how to set up Netcat as a listener to grab information from a connecting client

Netcat - Port Scanner to Grab Banners

[b2/p106] Describes how to set up netcat to grab banners from a range of IP's and ports

Netcat - Uses for Client Grabbing Service Info

[b2/p105] Use cases to use netcat to grab banners / version information

Network Services Test [b1/p23] Finding target systems on the network, look for openings in their operating systems and network services, then exploiting them

Nmap - 2nd Gen OS Fingerprinting [b2/p63]

Mechanisms Nmap uses to OS fingerprint

Nmap - Active OS Fingerprinting [b2/p62]

Describes how Nmap tries to fingerprint the OS running on a target

Nmap - Additional NSE Script Categories

[b2/p79] Overview of the additional NSE Script categories

Nmap - Additional TCP scan options [b2/p51]

Describes additional options for Nmap like ACK,FIN,Null,Xmas Tree and Maimon scans

Nmap - Address Probing [b2/p44]

Nmap - Connect Scan [b2/p49] Describes a connect scan using Nmap -sT

Nmap - Custom Control Bits [b2/p52] Describes how you can set scanflags yourself (--scanflags)

Nmap - IPv6 options [b2/p54] Describes the ability to scan IPv6 networks using Nmap

Nmap - IPv6 Targets and Scanning [b2/p55]

How to find IPv6 targets and scan them using Nmap

Nmap - Network Probe/Sweeping Options

[b2/p46] Useful probing options for a network sweep with Nmap

Nmap - Network Sweeping [b2/p45] Command for performing a network sweep with Nmap (nmap -sP)

Nmap - NSE Script Categories [b2/p78]

Overview of the NSE Script categories

Nmap - Optimizing Host Detection [b2/p47]

Optimizing Host Detection using common ports

Nmap - Output Options [b2/p43] Describes how to handle Nmap output in files

Nmap - Port Scanning [b2/p48] Describes the scan process Nmap uses by default and how to perform the right scan

Nmap - Scripting Engine [b2/p76] Overview of the Nmap Scripting Engine

Nmap - SYN Scan [b2/p50] Describes a SYN scan using Nmap -sS (the default scan in Nmap)

Nmap - Timing Options [b2/p41] Describes the scanning speeds of nmap 0 (Paranoid) to 5 (Insane)

Nmap - Timing Options (2) [b2/p42] Finer-Grained Nmap Timing Options for advanced scanning

Nmap - UDP scans [b2/p53] Describes options for UDP scanning with Nmap (-sU)

Nmap - Version Scanning [b2/p65] Describes how to scan for software versions using Nmap (-sV flag)

nslookup [b1/p143] How to use nslookup to gain information from a DNS server including zone transfers

nslookup - recurse vs norecurse [b1/p144] How to apply recursion or no recursion on a DNS server to cache a record in the cache

NT Hash Algorithm [b4/p48] Description of the NT Hash Algorithm

NTLMv2 - More ways to obtain credentials

[b5/p33] Four more ways how to get NTLMv2 credentials from users

NTLMv2 - Offline Brute Force NetNTLMv2 challenge responses [b5/p34] Brute-forcing NetNTLMv2 hashes with hashcat

NTLMv2 - Responder [b5/p30] Describes how to sniff NTLMv2 challenge/response hashes with Responder

NTLMv2 - Responder Abusing WPAD [b5/p32]

How Responder can abuse the Web Proxy Auto-Discovery feature of Windows to get hashes

NTLMv2 - Responder Defenses [b5/p37] How a organization can defend itself against Responder attacks

NTLMv2 - SMB Relaying [b5/p35] How to obtain access using an SMB Relay Attack

NTLMv2 - SMB Relaying with Responder

[b5/p36] How to combine an SMB Relaying attack with Responder

NTLMv2 Challenge/Response [b4/p52]

Describes the differences in NTLMv2 Challenge/Response versus v1

NTLMv2 Graphically [b4/p53] Graphical overview of NTLMv2 challenge/response

Oo

Overall Penetration Testing Process [b1/p64]

Three phases of overall penetration testing include: preparation, testing and conclusion phases

Pp

Password - The importance of passwords in pentesting [b4/p14]

Describes why passwords are important in pen-testing

Password Guessing vs Password Cracking [b4/p15]

Discusses differences between password guessing and cracking

Passwords - Account Lockout [b4/p28] How to deal with account lockout policies

Passwords - Account Lockout on Linux [b4/p31]

Describes account lockout possibilities on Linux and Unix

Passwords - Account Lockout on Windows [b4/p29]

Settings on account lockout on Windows

Passwords - Active Directory Passwords [b4/p46]

Describes where AD passwords are stored (NTDS.dit file)

Passwords - Admin Account Lockout on Windows [b4/p30]

Describes the possibilities on account lockout for admin accounts on Windows

Passwords - Cracking Sniffed Credentials [b4/p109]

How to crack sniffed credentials using tcpdump, PCredz and John/Hashcat

Passwords - Credential Stuffing [b4/p18]

Describes credential stuffing attacks and password less authentication

Passwords - Custom Dictionaries [b4/p21]

Describes the usefulness of custom dictionaries to use for password cracking

Passwords - Dictionary Attacks [b4/p20]

Describes the usage of dictionaries to crack passwords

Passwords - Extracting Audio from an RTP stream [b4/p113]

How to extract audio with Wireshark from RTP stream (phone conversation tap)

Passwords - Getting hashes from the PCredz log [b4/p111]

How to grep useful hashes from the PCredz log file to use with John or Hashcat

Passwords - How to report [b4/p27] How to report on cracked passwords to make the result effective

Passwords - Improving Cracking Speed [b4/p23]

Describes ways to improve the speed of password cracking using cloud resources

Passwords - LANMAN hashes [b4/p19]

Discusses LANMAN hashes and why they are weak

Passwords - Microsoft Pass-the-Hash mitigations [b4/p125]

Overview of what Microsoft has done to mitigate pass-the-hash attacks over time

Passwords - More Account Lockout Approaches [b4/p33]

Two more methods of account lockout detection

Passwords - Obtain hashes and passwords using VSS [b4/p62]

Describes how to obtain hashes and passwords using the VSS service on Windows boxes

Passwords - Obtaining Password Representations on Linux/Unix [b4/p58]

Describes where hashes and representations of passwords are stored on Linux/Unix machines

Passwords - Obtaining Password Representations on Windows [b4/p59]

Describes where hashes and representations of passwords are stored on Windows machines

Passwords - Pass-The-Hash Advantages [b4/p122]

Advantages of Pass-The-Hash over password guessing/cracking

Passwords - Pass-The-Hash Technique [b4/p121]

Overview of Pass-The-Hash

Passwords - Pass-The-Hash with Windows Credentials Editor [b4/p123]

Overview of the WCE tool for pass-the-hash attacks on Windows

Passwords - Password leakage [b4/p25]

Describes how to prevent password leaking as a pen-tester

Passwords - Passwords without cracking [b4/p24]

Describes obtaining passwords without cracking

Passwords - Safe Account Lockout Approaches [b4/p32]

Approaches to avoid account lockout

Passwords - Secure Copying and Transferring [b4/p26]

How to handle passwords files securely when using them

Passwords - Sniffing and Cracking Windows Challenge/Response [b4/p108]

Describes two ways to sniff Windows Challenge/Response authentications

Passwords - Synced Password [b4/p17]

The importance of compromising and saving every password we can get and how synced passwords are used

Passwords - VSS Extract from NTDS.dit

[b4/p63] How to obtain hashes from the NTDS.dit file after compromising the file using VSS

Passwords - When to Use Each Technique

[b4/p131] Describes in which case you may want to use a certain technique to crack passwords

Passwords - Windows Challenge/Response on the network

[b4/p49] Describes differences between LANMAN and LANMAN challenge/response as well as NT hash and NTLMv1/v2

Passwords - Windows Passwords in the SAM

[b4/p45] Overview of hashes used in the SAM databases on Windows

Penetration Testing [b1/p9] Model the activities of real-world threats to discover vulnerabilities and exploit them in a controlled way to determine business risk associated with these flaws.

Permission Memo / Get Out of Jail Free Card

[b1/p68] The importance of getting a signed permission from the target organization before you start to test

Physical Security Test [b1/p24] Test that looks for flaws in the physical security of a target organization

Pivoting [b4/p70] What is pivoting and how can you use it on Linux and Windows

Pivoting - Port Forwarding through

Meterpreter [b4/p75] Explains how to set up port forwarding through a meterpreter session

Pivoting - SSH Dynamic Port Forwarding

[b4/p74] Describes SSH Dynamic Port Forwarding using SSH

Pivoting - SSH Local Port Forwarding

[b4/p72] Describes SSH Local Port Forwarding using SSH

Pivoting - SSH Reverse Port Forwarding

[b4/p73] Describes SSH Remote Port Forwarding using SSH

Post-exploitation - Local files [b4/p10] Discusses useful local files to get after compromise (passwd/shadow files, SAM database, PGP/GPG keys)

Post-exploitation - Local Files (2) [b4/p11] More useful files to gather from a system (PHP/Perl and other web code, scripts, WLAN profiles)

Post-exploitation - Local Files (3) [b4/p12] More files to gather including ARP cache, DNS cache, Routing table, DNS zone files, e-mail inventory

Powershell - Select-Object [b2/p128] Describes the uses of the Select-Object cmdlet to select certain properties of an object

Powershell - Cmdlets [b2/p117] Overview of foundational cmdlets in Powershell (how they are constructed)

Powershell - Complete Ping Sweep Syntax

[b2/p135] A complete port scanner command string to use in Powershell

Powershell - Essential Things To Remember

[b2/p136] Five Essential Things/Commands to remember about Powershell

Powershell - ForEach-Object

[b2/p126] Describes the uses of the ForEach-Object cmdlet to run commands for each object in a command

Powershell - Ping Sweep

[b2/p133] How to perform a ping sweep using Powershell

Powershell - Searching for Files or Directories

[b2/p129] How to use powershell to search for files on a system as a pentester

Powershell - Select-String [b2/p131] Use the select-string cmdlet to search for words in a file

Powershell - The Pipeline [b2/p124] Describes how to use pipes in Powershell and what they do

Powershell - Useful Cmdlets [b2/p119] Overview of the most useful Powershell Cmdlets

Powershell - WhatIf [b2/p123] Describes the -WhatIf option in Powershell

Powershell - Where-Object [b2/p127] Describes the uses of the Where-Object cmdlet

Preparation phase [b1/p61] Sign NDA, discuss nature of the test with target personnel, sign off on permission to test, assign a team to test

Product Security test [b1/p23] Test to look for security flaws in software products that can be installed in a lab environment of the tester. Flaws may include buffer overflow, privilege escalation and unencrypted sensitive data.

Purple Teaming [b1/p15] Cross-functional teams consisting of Red Team and Blue Team members to allow for better collaboration. ACE minded.

Rr

Reasons for Ethical Hacking and Penetration Testing

[b1/p19] To help find vulnerabilities before the bad guys do, to help an organization better understand and manage risks, to make a point to decision makers

Recon-ng - Introduction [b1/p157] What is Recon-ng

Recon-ng - Module Groups [b1/p158] Overview of the module groups that exist within Recon-ng

Recon-ng - Recon Module [b1/p159] Overview of the Recon module of Recon-ng

Reconnaissance [b1/p25] The process of investigating the target organization to gather information about it from public available resources

Reconnaissance - Additional Search Databases [b1/p124] Other examples of search databases like GHDB

Reconnaissance - Dig [b1/p108] How to use dig to perform recursive and no-recursive lookups including zone transfers

Reconnaissance - DNS Lookups [b1/p107] How to get useful information from DNS lookups

Reconnaissance - Intro [b1/p117] What is reconnaissance, why is it important and how long should it take

Reconnaissance - Job Requisitions [b1/p101] How to retrieve informations about the target environment from job requisitions

Reconnaissance - Samples from the GHDB [b1/p125] Some interesting searches from the Google Hack DataBase

Reconnaissance - SearchDiggity [b1/p154] Description of the SearchDiggity Suite

Reconnaissance - Social Media [b1/p92] What and where to look for on social media to learn more about employees of the target

Reconnaissance - Website Searches [b1/p122] What to look for on, for example, Google

Reconnaissance - Whois Lookups [b1/p112] Regional Internet Registries and ASN lookups

Reconnaissance - Whois Searches [b1/p115] What is whois and how can we look information up from various databases

Red Teaming [b1/p15] Focussing on vulnerabilities, helping to measure and improve the Blue Team's capabilities to detect the attack and respond to it effectively

Remote dial-up war dial test [b1/p23] Test that looks for modems in an environment and often involve password guessing to log in to systems connected to discovered modems. Not really common test at the moment.

Reporting - Executive Summary [b1/p98] Explains how to format and write a good executive summary

Reporting - Executive Summary II [b1/p98] Explains how to format and write a good executive summary

Reporting - Findings [b1/p98] How to report on findings from a pen-test

Reporting - Introduction [b1/p99] What to include in the introduction section of the report

Reporting - Methodology [b1/p108] Describe the test process; what did you do to gain access and gather findings?

Reporting - Proper reporting vulnerabilities [b1/p95] How to report the results of a vulnerability scan properly

Reporting - Reasons to Report [b1/p94] Why reporting is important for your client

Reporting - Recommendations I [b1/p106] How to report on recommended actions to take after reporting findings

Reporting - Recommendations II [b1/p107] Make multiple recommendations when you can and recommend for different budgets

Reporting - Recommended Report Format [b1/p96] Recommended elements to include in a report

Reporting - Redaction and Transparency [b1/p105] How to properly use redaction and transparency in screenshots in your report

Reporting - Screenshots [b1/p102] How to use screenshots in a report

Repository Tools and Collaboration - Additional Tools [b1/p115] Describes EtherPad, Lair and Metasploit for collaboration

Repository Tools and Collaboration - How Discovered [b1/p113] Report on how you discovered a target server for the first time

Repository Tools and Collaboration - Maintain Inventory [b1/p112] How to keep track of your findings during a test

Repository Tools and Collaboration - Other tools [b1/p114] Explains other tools for building a repository like Dradis and MediaWiki

Risk [b1/p9] The point where threat and vulnerability overlap

Rules of Engagement [b1/p66] Rules that both target and testing organization must agree upon and comply to during the test

Rules of Engagement - Announced vs. Unannounced Testing [b1/p73] Discusses announced testing versus unannounced testing

Rules of Engagement - Black-Box vs. Crystal-Box Testing [b1/p75] Discusses the differences and recommended approaches on black-box and crystal-box testing

Rules of Engagement - Dates and Time of Day [b1/p72] Defines allowed dates and time of day for testing

Rules of Engagement - Debriefing Conference Calls [b1/p85] Defines the usage of debriefing conference calls with the client in a useful way during a test

Rules of Engagement - Encrypted Communication [b1/p70,80] Defines techniques to securely exchange vulnerability details and the final report

Rules of Engagement - How to approach [b1/p66] Rules of Engagement vs Project Scope

Rules of Engagement - Shunning of Pen Test Traffic [b1/p74] How to deal with shunning of traffic by the target organization

Rules of Engagement - Viewing Data on Compromised Systems [b1/p76] How to handle sensitive data once you gained access to a target system

Rules of Engagement - What should not be included [b1/p68] Items that should not be included in a Rules of Engagement document

Ss

Scanning [b1/p24] The process of finding openings in the target organization

Scanning - Dealing with large scopes [b2/p10] How to scan large scopes efficiently

Scanning - Discovering Vulnerabilities [b2/p72] Methods how to discover vulnerabilities (continues on page 73)

Scanning - Discovering Vulnerabilities (2) [b/p] More methods how to discover vulnerabilities

Scanning - Goals of Scanning [b2/p5] Goals of the Scanning Phase

Scanning - Hyperfast port scanning [b2/p13] Speed up scanning by hyperfast scanning methods

Scanning - IP address vs domain name scanning [b2/p8] Why it's better to use IP addresses for scanning instead of domain names (load balancers!)

Scanning - IPv4 Header and TTL Field [b2/p23] Important fields in IPv4 headers for scanning and the usage of the TTL field

Scanning - IPv6 Header and Hop Limit field [b2/p24] Important fields in IPv6 headers for scanning and the usage of the Hop Limit field

Scanning - Masscan [b2/p14] Describes the masscan tool and the difference with nmap

Scanning - Netcat Command Flags [b2/p103] The most important netcat command flags to use

Scanning - Other Vulnerability Scanning Tools [b2/p100] Overview of some other commercial scanning tools

Scanning - Scan Types [b2/p6] The different types of scans during a test

Scanning - Slow UDP Port Scanning [b2/p34] Why UDP scanning is slower than TCP (no control bits)

Scanning - Sniffer usage [b2/p17] Reasons to use a sniffer while scanning

Scanning - Speeding up scans [b2/p12] Speeding up scans by altering firewall rules

Scanning - TCP Behavior While Scanning [b2/p30] How to use results from scanning when you receive SYN-ACK or RST-ACK responses

Scanning - TCP Behavior While Scanning II [b2/p31] How to use results from scanning when you receive ICMP Port Unreachable or nothing at all

Scanning - TCP Control Bits [b2/p27] TCP Controls bits and their meaning/usage (SYN/ACK/RST/FIN/PSH/URG/CWR/ECE)

Scanning - TCP Header [b2/p26] The TCP header overview and TCP handling of packets

Scanning - TCP Ports [b2/p29] Describes why scanning TCP ports is a reliable method of port scanning

Scanning - TCP Three-Way Handshake [b2/p28] Describes the TCP Three-Way Handshake to initiate a session over TCP

Scanning - TCP vs UDP [b2/p25] The differences between the TCP and UDP protocols

Scanning - tcpdump expressions [b2/p20] Useful tcpdump expressions to use while scanning

Scanning - tcpdump options [b2/p19] Describes useful options to configure a tcpdump sniffer

Scanning - tcpdump usage examples [b2/p21] Examples of combinations of primitives and expressions to sniff targets

Scanning - UDP Behavior While Scanning I [b2/p35] Describes why UDP scanning is less reliable and often slower than TCP scanning.

Scanning - UDP Header [b2/p33] Overview of the UDP header

Scanning - Workflow of Scanning [b2/p7] The typical workflow of the scanning phase

Scoping - Cloud Pen Testing [b1/p83] How to deal with cloud providers that host target servers/services

Scoping - Concerns [b1/p79] Discusses the concerns that the target organization may have about their security

Scoping - Dangerous Exploits [b1/p90]

Determine if you want to run so called dangerous exploits or not during a test and reasons why to do

Scoping - Internal and Pseudo-Internal Access

[b1/p86] Methods for testing from the inside

Scoping - Scope Creep [b1/p80]

How to avoid scope creep and how to calculate the amount of time needed for a test

Scoping - Testing FROM the cloud [b1/p84]

How to and why should we use cloud resources for pentesting

Scoping - Third Parties [b1/p82]

How to handle third parties in your penetration testing

Scoping - What to Test? [b1/p81]

Setting the scope for a pen test

Security Audit [b1/p17] Measuring things against a fixed, predetermined, rigorous set of standards

Social Engineering Test [b1/p22] Test attempting to dupe a user into revealing sensitive information such as passwords or letting them click a link in an email.

SQL Injection - Blind Injection to pull data

[b5/p127] Describes how to use blind injection to gather information when you can't see output

SQL Injection - Discovering the database structure

[b5/p124] How to query different platforms to obtain the database structure (MS SQL, Oracle and MySQL)

SQL Injection - Finding SQL injection flaws

[b5/p119] How to manually find SQL injection flaws

SQL Injection - How it happens [b5/p117]

Explains how SQL injection can potentially take place

SQL Injection - Overview [b5/p116]

Overview of Structured Query Language and relational databases

SQL Injection - SQL Elements [b5/p122]

Overview of useful SQL elements to create a useful query

SQL Injection - Structured Query Language

[b5/p120] Overview of the differences between SQL spoken by several vendors and differences in metadata

SQL Injection - The Penetration Process

[b5/p118] Explains the proces of penetrating a web application for SQL flaws

SQL Injection - Use SQL Injection to perform command injection

[b5/p125] Describes how to use SQL injection to obtain command injection on a web server

SQL Injection - Useful SQL Elements (2)

[b5/p123] More useful SQL elements like the semicolon and union element

SQL Injection - Useful SQL Statements

[b5/p121] Useful SQL statements like select, update, substring, drop, delete and shutdown

Stolen Equipment Test [b1/p23]

Test that involves obtaining a piece of equipment such as a laptop and trying to extract sensitive information from it in a lab environment

Tt

Target Machines [b1/p41]

Systems whose security stance is being evaluated. Also called vicitim machines.

Testing Machines [b1/p41]

Systems used by the penetration tester or ethical hacker to evaluate the security of other machines. Also called attack machines.

Testing phase [b1/p61]

Conduct the actual pen test

Threat [b1/p9]

An actor or agent that may want to or actually can cause harm to the target organization

Title [bBook/pPage] Description

Uu

UAC - Bypass Techniques [b5/p59]

Three ways how UAC typically can be bypassed

UAC - Levels [b5/p58]

Description of the four different levels UAC can run on

UAC - Overview [b5/p57]

Description of User Account Control in Windows

Vv

Vulnerability [b1/p9] A flaw in the environment that an attacker can use to cause damage

Vulnerability Assessments [b1/p16]

Assessment focused on finding vulnerabilities without regard to exploiting them and getting into a system