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]* Overviewof DCShadow, a follow-up on DCSync

Active Directory - DCSync *[b5/p75]* Overview ofthe 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 fora 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 trollsploit

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

Gg

Hh

Ii

Jj

Kk

encrypted. Also PAC is discussed (Privilege Attribute Certificate)

Ll

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

LANMAN Challenge/Repsonse *[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 hases are salted using DES

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

Mm

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 piecesof 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 - Pivotting *[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, msfcli 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 priviliges

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

Nn

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

Oo

Pp

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 throught 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 Forwardingusing SSH

Pivoting - SSH Local Port Forwarding *[b4/p72]* Describes SSH Local Port Forwarding using SSH

Pivoting - SSH Reverse Port Forwarding *[b4/p73]* Describes 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

Powershel - 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 organizatoin 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 ofthe 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 toperform 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 oftend 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

Ss

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