Aa

Bb

Cc

Dd

Ee

Ff

Gg

Hh

Ii

Jj

Kk

Kerberos *[b5/**p5**]* Introduction to Kerberos.

Kerberos and NTLMv2 *[b5/**p116**]*

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/**p29**]* Introduction to the Golden Ticket of Kerberos and how to obtain it.

Kerberos - Golden Ticket Creation *[b5/**p32**]* Explains how you can create a Golden Ticket with the necessary inputs using Mimikatz.

Kerberos - Golden Ticket Creation (2) *[b5/**p33**]* How to use a Golden Ticket with Kerberos after creation.

Kerberos - Golden Ticket Properties *[b5/**p31**]* 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 futher 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/**p116**]* 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).

Ll

LANMAN and NTLMv1 Challenge/Response *[b4/**p23**]* Describes how LANMAN Challenge/Response is used in 3 pieces vs NTLMv1 usage.

LANMAN Challenge/Repsonse *[b4/**p22**]* Describes the usage of LANMAN Challenge/Response.

LANMAN Hashes *[b4/p19]* Description of the LANMAN hash algorithm.

Legacy Authentication Example *[b5/p168]*

Linux/Unix DES Password Scheme *[b4/**p27**]* Describes how Linux hases are salted using DES.

Linux/Unix MD5 Password Scheme *[b4/**p28**]* Describes how Linux hases are salted using MD5.

LLMNR (Link-Local Multicast Name Resolution) *[b5/p118]* Howto Obtain NetNTLMv2 Challenge/Response? (I)

Logging in Azure AD *[b5/**p165**]*

Mm

MDSec O365 toolkit [b5/**p109] -** Illicit Consent Attack - Abusing App Permissions.

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.

MDSec 0365 toolkit [b5/**p109] -** Illicit Consent Attack - Abusing App Permissions.

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

Metadata - Useful entries *[b1/p129]* Useful piecesof metadata for reconnaissance.

Metasploit - Components *[b3/**p24**]* Describes the components of Metasploit (documentation, user interfaces, modules, exploit creation tools & other items).

Metasploit Explatation Framework *[b3/p20]*

Metasploit - Exploit Rankings *[b3/**p29**]*

Metasploit - Exploits and Payloads *[b3/**p21**]* Describes how Metasploit is built up from exploits and payloads.

Metasploit - Modules *[b3/**p26**]* Describes the modules in Metasploit (auxiliary, encodes, exploits, nops, payloads & post).

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

Nn

Oo

Pp

Passwords - Admin Account Lockout on Windows *[b4/**p120**]* Describes the possibilities on account lockout for admin accounts on Windows.

Passwords - Credential Databases [b2/p115]

Passwords - Cracking Sniffed Credentials *[b4/**p68**]* How to crack sniffed credentials using tcpdump, PCredz and John/Hashcat.

Passwords - Credential Stuffing *[b2/**p114**]* Describes credential stuffing attacks and password less authentication.

Passwords - Custom Dictionaries *[b4/**p9**]* Describes the usefullness of custom dictionaries to use for password cracking.

Passwords - Dictionary Attacks *[b4/**p8**]* Describes the usage of dictionaries to crack passwords.

Passwords - Extracting Audio from an RTP stream -

*[b4/**p72, p73**]*

Passwords - Getting hashes from the PCredz Log File *[b4/**p70**]* How to grep useful hashes from the PCredz log file to use with John or Hashcat.

Passwords - How to report *[b4/**p15**]* How to report on cracked passwords to make the result effective.

Passwords - Improving Cracking Speed *[b4/**p11**]* 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/**p81**]* Overview of what Microsoft has done to migitate pass-the-hash attacks over time.

Passwords - More Account Lockout Approaches *[b4/**p118**]* Two more methods of account lockout detection.

Passwords - Obtain hashes and passwords using VSS *[b4/**p34**]* Describes how to obtain hashes and passwords using the VSS service on Windows boxes.

Passwords - Obtaining Password Representations on Linux/Unix *[b4/**p30**]* Describes where hashes and representations of passwords are stored on Linux/Unix machines.

Passwords - Obtaining Password Representations on Windows *[b4/**p31**]* Describes where hashes and representations of passwords are stored on Windows machines.

Passwords - Pass-The-Hash Advantages *[b4/**p78**]* Advantages of Pass-The-Hash over password guessing/cracking.

Passwords - Pass-The-Hash Technique *[b4/**p77**]* Overview of Pass-The-Hash.

Passwords - Pass-The-Hash with Windows Credentials Editor *[b4/**p79**]* Overview of the WCE tool for pass-the-hash attacks on Windows.

Passwords - Password leakage *[b4/**p13**]* Describes how to prevent password leaking as a pen-tester.

Passwords - Passwords without cracking *[b4/**p12**]* Describes obtaining passwords without cracking.

Password protection *[b5/**p150**]* - Fundamentals- Password protection.

Passwords - Safe Account Lockout Approaches *[b2/**p119**]* Approaches to avoid account lockout.

Passwords - Secure Copying and Transfering *[b4/**p14**]* How to handle passwords files securely when using them.

Passwords - Sniffing and Cracking Windows Challenge/Response *[b4/**p67, p68**]* Describes two ways to sniff Windows Challenge/Response authentications.

Passwords - Synced Password *[b4/**p7**]* The importance of compromising and saving every password we can get and how synced passwords are used.

Passwords - VSS Extract from NTDS.dit *[b4/**p35**]* How to obtain hashes from the NTDS.dit file after compromising the file using VSS.

Passwords (Attacks) - When to Use Each Technique *[b4/**p85**]* Describes in which case you may want to use a certain technique to crack passwords.

Passwords - Windows Challenge/Response on the network *[b4/**p21**]* Describes differences between LANMAN and LANMAN challenge/response as well as NT hash and NTLMv1/v2.

Passwords - Windows Passwords in the SAM *[b4/**p17**]* Overview of hashes used in the SAM databases on Windows.

PCredz *[b4/**p68**]*

Penetration Testing *[b1/**p16**]* 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/**p40**]* What is pivoting and how can you use it on Linux and Windows.

Pivoting - Port Forwarding through Meterpreter *[b4/**p45**]* Explains how to set up port forwarding through a meterpreter session.

Pivoting - SSH Dynamic Port Forwarding *[b4/**p44**]* Describes SSH Dynamic Port Forwardingusing SSH.

Pivoting - SSH Local Port Forwarding *[b4/**p42**]* Describes SSH Local Port Forwarding using SSH.

Pivoting - SSH Remote/Reverse Port Forwarding *[b4/**p43**]* Describes Describes SSH Remote Port Forwarding using SSH.

Post-exploitation - Local files *[b3/**p62**]* Discusses useful local files to get after compromise (passwd/shadow files, SAM database, PGP/GPG keys).

Post-exploitation - Local Files (2) *[b3/**p63**]* More useful files to gather from a system (PHP/Perl and other web code, scripts, WLAN profiles).

Post-exploitation - Local Files (3) *[b3/**p63**]* More files to gather including ARP cache, DNS cache, Routing table, DNS zone files, e-mail inventory.

Powershell - Cmdlets *[b4/**p88**]* Overview of foundational cmdlets in Powershell (how they are constructed).

Powershell - Complete Ping Sweep Syntax/Port Scan *[b4/**p106**]* A complete port scanner command string to use in Powershell.

Powershell - Essential Things To Remember *[b4/**p107**]* Five Essential Things/Commands to remember about Powershell.

Powershell - ForEach-Object *[b4/**p97**]* Describes the uses of the ForEach-Object cmdlet to run commands for each object in a command.

Powershell - Format-List *[b4/**p96**]*

Powershell - Ping Sweep : Counting Loops *[b4/**p104**]* How to perform a ping sweep using Powershell.

Powershell - Searching for Files or Directories *[b4/**p100**]* How to use powershell to search for files on a system as a pentester.

Powershel - Select-Object *[b4/**p99**]* Describes the uses of the Select-Object cmdlet to select certain properties of an object.

Powershell - Select-String *[b4/**p102**]* Use the select-string cmdlet to search for words in a file.

Powershell - The Pipeline *[b4/**p95**]* Describes how to use pipes in Powershell and what they do.

Powershell - Useful Cmdlets *[b4/**p90**]* Overview of the most useful Powershell Cmdlets.

Powershell - WhatIf *[b4/**p94**]* Describes the - WhatIf option in Powershell.

Powershell - Where-Object *[b4/**p98**]* Describes the uses of the Where-Object cmdlet.

PowerUp *[b5/**p142**]* - Privilege EscalationTools.

Preparation phase *[b1/**p64**]* Sign NDA, discuss nature of the test with target personnel, sign off on permission to test, assign a team to test.

Privilege EscalationTools *[b5/**p142**]*

Privileged Identity Management (PIM) *[b5/**p164**]* **–** introduce.

Product Security test *[b1/**p24**]* 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/**p18**]* Cross-functional teams consisting of Red Team and Blue Team members to allow for better collaboration. ACE minded.

PwnAuth *[b5/**p109**]* **-** Illicit Consent Attack -Abusing App Permissions.

Rr

Reasons for Ethical Hacking and Penetration Testing *[b1/**p22**]* 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.

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

Reconnaissance - Additional Search Databases *[b1/**p39**, **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/**p25**]* 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 - 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/**p115**]* 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/**p17**]* 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 *[b4/**p114**]* Explains how to format and write a good executive summary.

Reporting - Executive Summary II *[b4/**p115**]* Explains how to format and write a good executive summary.

Reporting - Findings *[b4/**p117**]* How to report on findings from a pen-test.

Reporting - Introduction *[b4/**p116**]* What to include in the introduction section of the report.

Reporting - Methodology *[b4/**p125**]* Describe the test process; what did you do to gain access and gather findings?

Reporting - Proper reporting vulnerabilities *[b1/**p122**]* How to report the results of a vulnerability scan properly.

Reporting - Reasons to Report *[b1/**p111**]* Why reporting is important for your client.

Reporting - Recommendations I *[b1/**p123**]* How to report on recommended actions to take after reporting findings.

Reporting - Recommendations II *[b1/**p124**]* Make multiple recommendations when you can and recommend for different budgets.

Reporting - Recommended Report Format *[b4/**p113**]* Recommended elements to include in a report.

Ss

Scanning - TCP Control Bits *[b2/**p23**]* TCP Controls bits and there meaning/usage (SYN/ACK/RST/FIN/PSH/URG/CWR/ECE).

Scanning - TCP Header *[b2/**p22**]* The TCP header overview and TCP handling of packets.

Scanning - TCP Ports *[b2/**p32**]* Describes why scanning TCP ports is a reliable method of port scanning.

Scanning - TCP Three-Way Handshake *[b2/**p24**]* Describes the TCP Three-Way Handshake to initiate a session over TCP.

Scanning - TCP vs UDP *[b2/**p21**]* The differences between the TCP and UDP protocols.

Scanning - tcpdump expressions *[b2/**p16**]* Useful tcpdump expressions to use while scanning.

Scanning - tcpdump options *[b2/**p14**]* Describes useful options to configure a tcpdump sniffer.

Scanning - tcpdump usage examples *[b2/**p17**]* Examples of combinations of primitives and expressions to sniff targets.

Scanning - UDP Behavior While Scanning I *[b2/**p31**]* Describes why UDP scanning is less reliable and often slower than TCP scanning.

Scanning - UDP Header *[b2/**p29**]* Overview of the UDP header.

Scanning - Workflow of Scanning *[b2/**p5**]* The typical workflow of the scanning phase.

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

Scoping - Concerns *[b4/**p124**]* Discusses the concerns that the target organization may have about their security.

Scoping - Dangerous Exploits *[b1/**p70**]* 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/**p33**]* Methods for testing from the inside.

Scoping - Scope Creep *[b1/**p74**]* How to avoid scope creep and how to calculate the amount of time needed for a test.

Scoping - Testing FROM the cloud *[b1/**p35**]* How to and why should we use cloud resources for pentesting.

Scoping - Third Parties *[b1/**p38**]* How to handle third parties in your penetration testing.

Scoping - What to Test? *[b1/**p74**]* Setting the scope for a pen test.

Seamless Single Sign-On On-PremAD Integration *[b5/**p77, p78**]*

Seatbelt *[b2/**p93**]*

Security Audit *[b1/**p19**]* Measuring things against a fixed, predetermined, rigorous set of standards.

Security Token Service (STS) *[b5/**p97**]* – MS AZURE AD Security Token Service (STS).

Service Principals for Backdoor Access *[b5/**p112**]*

Service Principal Hunting with ROADRecon *[b5/**p113**]*

Shodan *[b1/p117]*

SharpHound *[b5/**p130**]* - BloodHound in Action:Ingestion via SharpHound

SilverTicket-Attacking Seamless SSO *[b5/**p86**]*

Skeleton Key -Attacking PTA [b5/**p84**]

Smart Lockout - [b5/**p149**]

SNMP Simple Network Management Protocol [b2/p128]

snmpwalk – [b2/p135]

snmp-check - [b2/p136]

Social Engineering Test *[b1/**p23**]* Test attempting to dupe a user into revealing sensitive information such as passwords or letting them click a link in an email.

SpiderFoot [b1/p146]

SPNs (Service Principals Names) *[b5/**p116**]*

Synchronized Identity *[b5/**p70**]* Introduction -Azure AD Identity Models.

Tt

Target Machines *[b1/**p29**]* Systems whose security stance is being evaluated. Also called vicitim machines.

Tcpdump *[b2/p14]*

Testing Machines *[b1/**p29**]* Systems used by the penetration tester or ethical hacker to evaluate the security of other machines. Also called attack machines.

Testing phase *[b1/**p64**]* Conduct the actual pen test.

Threat *[b1/**p11**]* An actor or agent that may want to or actually can cause harm to the target organization.

Token Forging-Attacking ADFS *[b5/**p91**]*

Uu

UAC - Bypass Techniques *[b5/**p145**]* Three ways how UAC typically can be bypassed.

UAC - Levels *[b5/**p144**]* Description of the four different levels UAC can run on.

UAC - Overview *[b5/**p143**]* Description of User Account Control in Windows.

Unattended Install Files *[b5/**p139**]* - Windows Privilege Escalation Flaws.

Unquoted Paths with Spaces (I) (2) *[b5/**p137, p138**]* - Windows Privilege Escalation Flaws.

Vv

Vulnerability *[b1/**p10**]* A flaw in the environment that an attacker can use to cause damage.

Vulnerability Assessments *[b1/**p20**]* Assessment focused on finding vulnerabilities without regard to exploiting them and getting into a system.

Ww

Watson *[b5/**p142**]* - Privilege EscalationTools.

Web application test [b1/p23]

Windows Credentials Editor (WCE) *[b4/**p79**]*

Windows Privilege Escalation Flaws *[b5/**p136**]* - Common Windows Privilege Escalation Flaw.

Wireless security test *[b1/p23]*

WPAD (Web Proxy Autodiscovery Protocol) ***[b5/p120] -*** Responder AbusingWPAD

WS-Federation *[b5/**p95, p97**]* Azure AD:Enterprise Applications -Authentication Protocols.

Zz

(DNS) Zone Transfer *[b1/p108]*