# Aa

**accounts *[****b3****/p28]***

**Active Directory *[****b3****/p80, p81, p82, p99, p102, p110]***

**Active Directory Authentication Protocols *[****b3****/p102]***

**AD Explorer (Active Directory Explorer) *[****b3****/p46]***

**administrator access token *[****b3****/p70]***

**AES *[****b3****/p66]***

**"AlwaysInstallElevated" registry key *[****b3****/p63]***

**arp -a *[****b3****/p26]***

**Assumed Breach *[****b3****/p15, p74]***

**Assumed Breach Testing** *[b3/****p5, p7, p9****]*

**Assumed Breach Phases** *[b3/****p10****]*

**Authentication Protocols *[****b3****/p102]***

**Autologon Credentials *[****b3****/p74]***

# Bb

**base64 *[****b3****/p33, p65]***

**BeRoot *[****b3****/p73]***

**BloodHoundAD *[****b3****/p79, p80, p81, p82, p83, p84]***

**BloodHound Graph Interface *[****b3****/p83]***

**BloodHound Queries *[****b3****/p82]***

**Blowfish-based *[****b3****/p108]***

**BSDi Extended DES *[****b3****/p108]***

**bypassuac module *[****b3****/p72]***

# Cc

**CAC and Smartcards *[****b3****/p107]***

**Cain *[****b3****/p142]***

**Ceded Access *[****b3****/p15]***

**Certificates *[****b3****/p54]***

**Cewl *[****b3****/p91]***

**Chameleon *[****b3****/p45]***

**Client Challenge Blob (Binary Large Object) *[****b3****/p106]***

**Collection *[****b3****/p18]***

**cpassword *[****b3****/p66, p67]***

**Crackstation *[****b3****/p91]***

**Cracking Sniffed Credentials *[****b3****/p142]***

**Credential Access *[****b3****/p18]***

**CredentialDump-Session.log *[****b3****/p144]***

**Creds *[****b3****/p114]***

**crypt (1) *[****b3****/p108]***

**crypt (3) *[****b3****/p108]***

**Crypto Keys *[****b3****/p32]***

**csscript *[****b3****/p115]***

**CUDA *[****b3****/p128]***

# Dd

**Data Exfiltration *[****b3****/p10]***

**DCSync *[****b3****/p82]***

**Defense Evasion *[****b3****/p18]***

**degraded sensors** *[b3/****p7****]*

**Deleting Windows Users and Accounts** *[b3/****p41****]*

**DES** *[b3/****p100, p103, p104, p108****]*

**Determining Windows Firewall Settings** *[b3/****p42****]*

**Dictionaries *[****b3****/p90, p92]***

**DirtyCow (Dirty copy-on-write)*****[****b3****/p57]***

**Discovery** *[b3/****p18****]*

**Displaying and Scraping Through Files** *[b3/****p43****]*

**Distributed Cracking *[****b3****/p93] [Old b4/p11]***

**DLL Hijacking *[****b3****/p74]***

**DLL search order hijacking *[****b3****/p63, p72]***

**Domain Admins** *[b3/****p40****]*

**Domain Groups** *[b3/****p40****]*

**Domain User** *[b3/****p38****]*

**Dumping Creds** *[b3/****p114****]*

**Dumping Hashes with Meterpreter** *[b3/****p113****]*

# Ee

**Empire *[****b3****/p72, p73]***

**Environment Variables *[****b3****/p35]***

**Exfiltration** *[b3/****p18****]*

**/etc/group *[****b3****/p29]***

**/etc/passwd *[****b3****/p28, p32, p95, p108, p109, p110, p111]***

**/etc/shadow *[****b3****/p32, p95, p108, p109, p110, p111, p129]***

**extract password hashes *[****b3****/p99, p113, p116, p117, p142, p143]***

**Extracting Hashes with PCredz *[****b3****/p143]***

# Ff

**File Transfer Services** *[b3/****p20, p21****]*

**File Pilfering** *[b3/****p25, p26, p32****]*

**Find Interesting Files *[****b3****/p30, p31]***

**FTP *[****b3****/p20]***

# Gg

**GECOS *[****b3****/p111, p122, p131]***

**Getting the Hashes from PCredz’ Log File *[****b3****/p144]***

**GhostPack *[****b3****/p48]***

**GnuPG (Gnu Privacy Guard) *[****b3****/p32]***

**Group Policy Preferences (GPP) *[****b3****/p63, p66, p67]***

**groups *[****b3****/p29]***

**GTFOBins *[****b3****/p61, p75]***

# Hh

**Hash Types *[****b3****/p108, p109, p129]***

**Hashcat *[****b3****/p126, p128, p129, p130, p131, p132, p133, p134, p135, p142, p144, p150]***

**Hashcat Dictionaries, and Word Mangling Rules *[****b3****/p131]***

**Hashcat Masks *[****b3****/p132, p133]***

**hashcat.potfile *[****b3****/p130]***

**Hashcat: Specifying Hash Types *[****b3****/p129]***

**Hashcat Status and Temp Sensor *[****b3****/p134]***

**hashdump *[****b3****/p112, p113, p119]***

**High Value Target *[****b3****/p84]***

**HMAC-MD5 *[****b3****/p105, p106]***

**HTTrack** *[b3/****p20****]*

**Hybrid Guessing *[****b3****/p92]***

# Ii

**IFM (Install From Media) *[****b3****/p117]***

**Impacket *[****b3****/p99, p116]***

**Impersonation *[****b3****/p54]***

**Improving Speed *[****b3****/p93] [Old b4/p11]***

**Improving Speed for cracking passwords *[****b3****/p93]***

**Initial Access** *[b3/****p8****]*

**Interesting Files** *[b3/****p30, p31****]*

**ipconfig /displaydns *[****b3****/p26]***

# Jj

**john --test *[****b3****/p125]***

**john the ripper (jtr) *[****b3****/p93, p111, p121, p126, p142, p144]***

**john the Ripper vs. Hashcat *[****b3****/p126]***

**John.conf *[****b3****/p122]***

**John.ini *[****b3****/p122]***

**John.pot file *[****b3****/p123, p124]***

**John Distributed Cracking *[****b3****/p93] [Old b4/p11]***

**John and Speed *[****b3****/p93, p125]***

**John's Configuration File and Cracking Modes *[****b3****/p122]***

**John Cracking Modes *[****b3****/p122]***

**John's Output *[****b3****/p124]***

**JSON *[****b3****/p49]***

**Jumbo Patch *[****b3****/p121]***

# Kk

**Kerberos *[****b3****/p102, p112, p139, p141]***

**Kerberos and NTLMv2 *[****b3****/p139]***

**Kernel Exploits** ***[****b3****/p57]***

**Keystroke logging *[****b3****/p94]***

**Kiwi *[****b3****/p114]***

# Ll

**LANMAN *[****b3****/p98, p99, p100, p102, p105, p129]***

**LANMAN and NTLMv1 Challenge/Response *[****b3****/p104]***

**LANMAN Challenge/Response *[****b3****/p102, p103, p104, p105, p112, p141]***

**LANMAN Hash Algorithm *[****b3****/p100, p101, p103, p104]***

**LANMAN OWF *[****b3****/p100]***

**Lateral Movement** *[b3/****p10, p18****]*

**linux-exploit-suggester** *[b3/****p57****]*

**Linux and UNIX Password Representations *[****b3****/p108, p111]***

**Linux/UNIX MD5-Based Password Scheme *[****b3****/p109]***

**Linux Privilege Escalation** *[b3/****p56, p57, p58, p59, p60, p61****]*

**LLMNR (Link-Local Multicast Name Resolution)*****[****b3****/p146, p148, p152, p153]***

**Local File Pilfering** *[b3/****p32****]*

**Local groups** *[b3/****p39****]*

**logon script location** *[b3/****p38****]*

**LOLBAS (Living Off The Land Binaries, Scripts and Libraries) *[****b3****/p75]***

**List.Rules: *[****b3****/p122]***

**LSASS *[****b3****/p107, p112, p114]***

**lsof *[****b3/****p26]***

**Lynx** *[b3/****p20****]*

# Mm

**Mangling Rules *[****b3****/p91]***

**MD4 *[****b3****/p101]***

**MD5 *[****b3****/p108, p109, p129]***

**md5crypt *[****b3****/p129]***

**Mimikatz *[****b3****/p48, p80, p112, p114, p119]***

**MMX (MultiMedia eXtension) instructions *[****b3****/p125]***

**Modifiable Service Binaries *[****b3****/p74]***

**Moving Files** *[b3/****p19, p20, p21, p22, p33****]*

**MS14-025** *[b3/****p66****]*

# Nn

**neo4j database *[****b3****/p83]***

**net1.exe / net.exe *[b3/p37]***

**NetBIOS** *[b3/****p21, p112, p113****]*

**NetBIOS Name Server (NBT-NS)*****[****b3****/p146, p148, p152, p153]***

**Netcat** *[b3/****p21****]*

**netsh *[****b3****/p42]***

**netstat** *[b3/****p26****]*

**net group** *[b3/****p40****]*

**net localgroup** *[b3/****p37, p39, p41****]*

**NetNTLMv2 *[****b3****/p150]***

**NetNTLMv2 Challenge/Response *[****b3****/p147, p149]***

**net user** *[b3/****p37, p38, p41****]*

**NFS (Network File System) mounts** *[b3/****p21****]*

**NPK *[****b3****/p93] [Old b4/p11]***

**Ntds.dit *[****b3****/p95, p99, p112, p113, p115, p116, p117, p135]***

**NTDSUtil *[****b3****/p117]***

**NT Hash *[****b3****/p98, p99, p100, p101, p102, p103, p104, p105, p106, p107, p140]***

**NT Hash Algorithm *[****b3****/p101]***

**NTLMv1 *[****b3****/p102, p103, p104, p112, p141]***

**NTLMv1 Challenge/Response *[****b3****/p104]***

**NTLMv2 *[****b3****/p102, p105, p106, p112, p139, p140, p141, p144, p146, p147, p150, p151]***

**NTLM Attack Strategy # 1: Offline Brute Force *[****b3****/p150]***

**NTLM Attack Strategy # 2: SMB Relaying *[****b3****/p151]***

**NTLM Attack Strategy # 2: SMB Relaying with responder *[****b3****/p152]***

**NTLMv2 Attack Strategies *[****b3****/p140]***

**NTLMv2 Challenge/Response *[****b3****/p105, p106, p140, p146, p147, p150]***

**NTLMv2 OWF (One-Way Function) *[****b3****/p105, p106]***

# Oö

**OpenCL (Open Computing Language) *[****b3****/p128]***

**Owned Principal *[****b3****/p84]***

# Pp

**Pass-the-Hash *[****b3****/p94]***

**Password.lst *[****b3****/p122]***

**Password Cracking *[****b3****/p88, p91, p95, p96]***

**Password Guessing *[****b3****/p88, p91, p92, p95, p96, p111]***

**Password Hashes *[****b3****/p54, p99, p108, p114, p117]***

**Password Representations *[****b3****/p32, p98, p108]***

**Passwords without Cracking *[****b3****/p94]***

**Pcredz *[****b3****/p142, p143, p144]***

**PE Loader *[****b3****/p48]***

**Penetration Testing** *[b3/****p5****]*

**Persistence** *[b3/****p18****]*

**PGP (Pretty Good Privacy) *[****b3****/p32]***

**PHI** *[b3/****p25****]*

**Phishing** *[b3/****p12****]*

**PII** *[b3/****p25****]*

**Pilfer** *[b3/****p26, p32****]*

**Pipal and reporting on cracked password** *[b3/****p135****]*

**Privilege Escalation** *[b3/****p18, p54, p56, p63****]*

**Post-Exploitation** *[b3/****p15, p17, p18****]*

**Post-Exploitation Tactics** *[b3/****p18****]*

**PowerShell WebClient *[****b3****/p20]***

**PowerSploit *[****b3****/p45, p48]***

**PowerSploit Out-Minidump.ps1 *[****b3****/p48]***

**PowerSploit PowerUp *[****b3****/p73, p74]***

**PowerUp *[****b3****/p48, p73, p74]***

**PowerView *[****b3****/p45]***

**Privilege Escalation** *[b3/****p10****]*

**ps aux | grep root *[****b3****/p58]***

**pw-inspector *[****b3****/p90]***

**pwdump file *[****b3****/p129]***

# Qq

-

# Rr

**reg *[****b3****/p44]***

**reg add *[****b3****/p44]***

**reg export *[****b3****/p44]***

**reg import *[****b3****/p44]***

**reg query *[****b3****/p44]***

**Registry *[****b3****/p44, p116]***

**Responder *[****b3****/p146, p147, p148, p149, p150, p151, p152, p153]***

**Responder Attacks: Understanding the Defenses *[****b3****/p153]***

**Rockyou *[****b3****/p91]***

**Rubeus *[****b3****/p48]***

# Ss

**SafetyKatz *[****b3****/p48]***

**Salt *[****b3****/p101, p108, p109]***

**SAM (Security Account Manager) *[****b3****/p32, p95, p98, p99, p100, p102, p104, p105, p106, p110, p113, p116, p141]***

**Samba *[****b3****/p21]***

**SCP (Secure Copy) *[****b3****/p20]***

**Searching the File System *[****b3****/p36]***

**Seatbelt *[****b3****/p48, p49, p50]***

**Seatbelt Command Groups *[****b3****/p50]***

**secretsdump.py *[****b3****/p99, p116]***

**Services Running as root *[****b3****/p58]***

**SETGUID (2000) *[****b3****/p30, p60]***

**SETUID (4000) *[****b3****/p30, p60]***

**SHA-256 *[****b3****/p108, p109]***

**SHA-512 *[****b3****/p108, p109, p129]***

**sha512crypt *[****b3****/p129]***

**SharpDump *[****b3****/p48]***

**SharpHound *[****b3****/p81]***

**SharpRoast *[****b3****/p48]***

**SharpUp *[****b3****/p48]***

**SharpWMI *[****b3****/p48]***

**Situational Awareness** *[b3/****p10, p24, p25****]*

**smart card *[****b3****/p107]***

**SMB** *[b3/****p21, p112, p113, p140, p149, p151****]*

**SMB Relay Attack** *[b3/****p151, p152****]*

**SMB Signing** *[b3/****p153****]*

**smbclient *[****b3****/p21]***

**smbd (Samba Daemon) *[****b3****/p21]***

**smbmount *[****b3****/p21]***

**Sniffing *[****b3****/p54, p94, p141, p142]***

**SPNs (Service Principal Names) *[****b3****/p139]***

**ss *[****b3****/p26]***

**SSE2 (Streaming Single SIMD Extensions 2) instructions *[****b3****/p125]***

**ssh *[****b3****/p20, p32]***

**sshd *[****b3****/p32]***

**standard user access token *[****b3****/p70]***

**Streaming Single SIMD Extensions 2 (SSE2) instructions *[****b3****/p125]***

**sudo *[****b3****/p29]***

**Synced Passwords *[****b3****/p89]***

**Sysinternals *[****b3****/p46]***

**Syskey *[****b3****/p113]***

**sysprep.exe *[****b3****/p72]***

**sysprep.inf *[****b3****/p64]***

**sysprep.xml *[****b3****/p64]***

**SYSVOL *[****b3****/p38, p66, p67]***

**System Key *[****b3****/p113]***

# Tt

**Test Assumptions** *[b3/****p11****]*

**Token Attacks *[****b3****/p54]***

**TCP\_20 (data) *[****b3****/p20]***

**TCP\_20 (control) *[****b3****/p20]***

**TCP\_135-139 *[****b3****/p21, p112]***

**TCP\_204 *[****b3****/p21]***

**TCP/UDP\_445 *[****b3****/p21, p112]***

**TFTP (Trivial File Transfer Protocol) *[****b3****/p20]***

**Traditional DES-based schemes *[****b3****/p108]***

**Traditional Test** *[b3/****p11****]*

# Uü

**UDP\_69 *[****b3****/p20]***

**UDP\_204 *[****b3****/p21]***

**Unattended.xml *[****b3****/p64, p65]***

**Unattended install files *[****b3****/p63, p64, p65]***

**Underlying Assumption** *[b3/****p11****]*

**Unquoted paths with spaces *[****b3****/p63, p68, p69]***

**unshadow *[****b3****/p111]***

**UAC (User Account Control) *[****b3****/p70, p71, p72]***

**UAC Levels *[****b3****/p71]***

**UAC Bypass Techniques *[****b3****/p72]***

# Vv

**Vulnerability assessments** *[b3/****p5****]*

**VSS (Volume Shadow Copy Service)** *[b3/****p112, p115, p116****]*

**VSSOwn tool** *[b3/****p115****]*

# Ww

**Watson *[****b3****/p73]***

**WebClient *[****b3****/p20]***

**Web Proxy Autodiscovery Protocol (WPAD) *[****b3****/p148]***

**wget** *[b3/****p20****]*

**Windows Accounts and Groups** *[b3/****p37****]*

**Windows Challenge/Response Authentication** *[b3/****p141****]*

**Windows Challenge/Response on the Network** *[b3/****p102****]*

**Windows File Sharing** *[b3/****p21****]*

**Windows Firewall *[****b3****/p42]***

**Windows Password Representations *[****b3****/p98, p99, p112]***

**Windows Password Representations in AD *[****b3****/p99]***

**Windows Privilege Escalation *[****b3****/p63, p64, p65, p66, p67, p68, p69, p72, p73, p74, p75]***

**Windows Privilege Escalation Tools *[****b3****/p73]***

**WMI *[****b3****/p48]***

**wmic*[****b3****/p69]***

**World Readable *[****b3****/p111]***

**World Writeable Files *[****b3****/p59]***

**WPAD (Web Proxy Autodiscovery Protocol) *[****b3****/p148, p153]***

**wpad.internaldomain *[****b3****/p148]***

**Writeable Registry Keys *[****b3****/p74]***

**Writable Windows Service executables *[****b3****/p63]***

# Xx

-

# Yy

-

# Zz

**0-Day** *[b3/****p14****]*