560.1 Comprehensive Pen Test Planning, Scoping, and Recon

Aa

ACE (Automation, Coverage, Effectiveness) *[b1/p19]*

Admin Hunting *[b1/p87]*

AfriNIC *[b1/p111]*

Announced vs. Unannounced Tests *[b1/p76]*

APNIC *[b1/p111]*

ARIN *[b1/p111, p112]*

ASNs (Autonomous System Numbers) *[b1/p108, p109, p110, p111]*

Assumed breach test *[b1/p24]*

Attack Phases *[b1/p26]*

Attack System *[b1/p30]*

AXFR *[b1/p105]*

Bb

Building Infrastructure *[b1/p28]*

Building a Lab *[b1/p31]*

BuiltWith *[b1/p115, p116]*

Cc

C2 *[b1/p39]*

CIDR (Classless Inter-Domain Routing) *[b1/p111]*

Cloud services *[b1/p73]*

Commercial Tools *[b1/p39]*

Common Signed Paperwork *[b1/p79]*

Competitive Intelligence *[b1/p98]*

Credentials *[b1/p131, p132]*

crystal-box testing *[b1/p77]*

Dd

Data Breach *[b1/p131, p132]*

Dates and Time of Day *[b1/p75]*

debriefing calls *[b1/p80]*

deconfliction *[b1/p80]*

Dedicated Test Systems *[b1/p33]*

Dehashed.com *[b1/p132]*

DIA-NZ *[b1/p125]*

Dig Command *[b1/p105]*

DNS Records *[b1/p104]*

DNSDumpster *[b1/p108, p109, p110]*

DNSRecon *[b1/p106, p107]*

DNSSEC *[b1/p107]*

Document Metadata *[b1/p124]*

Documented Permission *[b1/p66]*

Drop / Drop Box *[b1/p34, p36]*

Ee

Employee Data *[b1/p87]*

ExifTool *[b1/p125, p126]*

Exploit *[b1/p13]*

Exploits *[b1/p37]*

Exploitation Toolkits *[b1/p39]*

External Testing Systems *[b1/p36]*

Ff

FOCA *[b1/p125]*

Follow the Law *[b1/p67]*

Free Software Tools *[b1/p38]*

Free Tools and Exploits *[b1/p37]*

FQDN (fully qualified domain name) *[b1/p85]*

Gg

GatherContacts *[b1/p135, p136]*

GDPR *[b1/p78]*

Get Out of Jail Free Card *[b1/p66]*

GHDB *[b1/p119, p120]*

GLBA *[b1/p78]*

Google Dork *[b1/p117, p118, p119, p120]*

Google Search *[b1/p117, p118]*

Hh

Harden Testing Systems *[b1/p35]*

HaveIBeenPwned.com ***[b1/p132]***

HIPAA ***[b1/p78]***

Hostname Information ***[b1/p103]***

Hunter.io ***[b1/p128, p129]***

Ii

infrastructure Data ***[b1/p87]***

Infrastructure Recon ***[b1/p102]***

Intellectual Property ***[b1/p78, p79]***

intelx.io ***[b1/p132]***

Intentional Sharing ***[b1/p88]***

Interesting DNS Records ***[b1/p104]***

Internal Permission memo ***[b1/p66]***

Internal Testing Systems ***[b1/p34, p36]***

Inventory of Discoverable Flaws via Google ***[b1/p119]***

IP Address Assignment WHOIS Databases ***[b1/p111]***

Jj

-

Kk

Kickoff Call ***[b1/p69, p80]***

Ll

Lab Systems ***[b1/p32]***

LACNIC ***[b1/p111]***

Law ***[b1/p67]***

Leave Behind ***[b1/p34]***

Light Touch ***[b1/p90]***

Liability ***[b1/p66, p79]***

Limitation of Liability ***[b1/p66, p79]***

LinkedIn ***[b1/p133, p134, p135, p136]***

LinkedInt ***[b1/p134]***

Linux ***[b1/p43-p55]***

Linux: Commands ***[b1/p55]***

Linux: Escalation ***[b1/p53]***

Linux: Escalating with SETUID ***[b1/p52]***

Linux File System Structure ***[b1/p47]***

Linux: Listing Files ***[b1/p50]***

Linux: Navigating the Filesystem ***[b1/p49]***

Linux: Network Configs (ifconfig) ***[b1/p54]***

Linux: Permissions ***[b1/p51]***

Linux Shell Tips ***[b1/p44]***

Linux Users: Root and Non-root ***[b1/p45]***

Linux: Where Am I? ***[b1/p48]***

Linux: Who Am I? ***[b1/p46]***

Linux vs. Windows ***[b1/p29]***

Mm

Metadata ***[b1/p124, p125]***

Metadata Analysis ***[b1/p125]***

Methodology ***[b1/p79]***

MSA (Master Service Agreement) ***[b1/p79]***

Mindset of Penetration Testers and Ethical Hackers ***[b1/p9]***

MITRE ATT&CK ***[b1/p65]***

Nn

NDA (Non-Disclosure Agreement) ***[b1/p63, p79]***

Network services test ***[b1/p24]***

nslookup ***[b1/p85, p105]***

Oö

Organization(al) Data/Information ***[b1/p87]***

Organizational Recon ***[b1/p93-p98]***

Overall Penetration Testing Process ***[b1/p63-p67]***

OWASP Testing Guide ***[b1/p64]***

Pp

Penetration Test ***[b1/p68]***

Penetration Testing ***[b1/p16, p17, p21]***

Penetration Testing Goals ***[b1/p23]***

Penetration Testing Process ***[b1/p63-p67]***

560.1 Comprehensive Pen Test Planning, Scoping, and Recon

Penetration Testing Types *[b1/p24]*

Permission ***[b1/p63, p66]***

PHI ***[b1/p78]***

phonebook.cz ***[b1/p130]***

Physical security test ***[b1/p24]***

PII ***[b1/p78]***

PowerMeta ***[b1/p125, p126]***

Pre-Engagement *[b1/p68-p82]*

Pre-Engagement: Announced vs. Unannounced Tests ***[b1/p76]***

Pre-Engagement: Be Careful Viewing Data on Compromised Systems ***[b1/p78]***

Pre-Engagement: Common Signed Paperwork ***[b1/p79]***

Pre-Engagement: Dates and Time of Day ***[b1/p75]***

Pre-Engagement: Finalizing Pen Test Planning ***[b1/p82]***

Pre-Engagement: Goals *[b1/p70]*

Pre-Engagement: Kickoff Call *[b1/p80]*

Pre-Engagement: Rules of Engagement *[b1/p74]*

Pre-Engagement: Scope *[b1/p72]*

Pre-Engagement: Scope: Third Parties ***[b1/p73]***

Pre-Engagement Steps *[b1/p69]*

Pre-Engagement: Types of Tests and Allowed Actions *[b1/p71]*

Pre-Engagement: Zero-Knowledge vs. Full-Knowledge Testing *[b1/p77]*

Product security test *[b1/p24]*

Public Breach Data of Credentials ***[b1/p131]***

Purple Teaming *[b1/p16, p19]*

PwnDb ***[b1/p132]***

Qq

-

Rr

Recon – Infrastructure ***[b1/p101-p120]***

Recon – Infrastructure ***[b1/p101, p102]***

Recon – Infrastructure: BuiltWith ***[b1/p115, p116]***

Recon – Infrastructure: Dig Command ***[b1/p105]***

Recon – Infrastructure: DNSDumpster ***[b1/p108, p109, p110]***

Recon – Infrastructure: DNSRecon ***[b1/p106, p107]***

Recon – Infrastructure: Google Search Directives: Sites and Links ***[b1/p117, p118]***

Recon – Infrastructure: Hostname Information ***[b1/p103]***

Recon – Infrastructure: Interesting DNS Records ***[b1/p104]***

Recon – Infrastructure: Inventory of Discoverable Flaws via Google ***[b1/p119]***

Recon – Infrastructure: IP Address Assignment WHOIS Databases ***[b1/p111]***

Recon – Infrastructure: Sample ARIN Lookups: Network ***[b1/p112]***

Recon – Infrastructure: Searching for File Types ***[b1/p118]***

Recon – Infrastructure: Shodan ***[b1/p113, p114]***

Recon – Infrastructure: Some Interesting Samples from the GHDB ***[b1/p120]***

Recon – Organization ***[b1/p93-p98]***

Recon – Organization: Gather Competitive Intelligence ***[b1/p98]***

Recon – Organization: Information on the Organization ***[b1/p94]***

Recon – Organization: Look for Open Job Requisitions ***[b1/p97]***

Recon – Organization: Press Releases and Annual Reports ***[b1/p96]***

Recon – Organization: Where to Start? ***[b1/p95]***

Recon Overview ***[b1/p85-p92]***

Recon – Overview: Motivation ***[b1/p86]***

Recon – Overview: Social Engineering and Recon Ethics ***[b1/p91]***

Recon – Overview: Targets ***[b1/p87]***

Recon – Overview: Timing ***[b1/p89]***

Recon – Overview: Traffic ***[b1/p90]***

Recon – Overview: Types of Shared Data ***[b1/p88]***

Recon – User: ***[b1/p123-p136]***

Recon – User: Document Metadata ***[b1/p124]***

Recon – User: Employee Roles ***[b1/p133]***

Recon – User: ExifTool ***[b1/p126]***

Recon – User: GatherContacts ***[b1/p135, p136]***

Recon – User: Hunter.io ***[b1/p128, p129]***

Recon – User: LinkedInt ***[b1/p134]***

Recon – User: phonebook.cz ***[b1/p130]***

Recon – User: Public Breach Data ***[b1/p132]***

Recon – User: Public Breach Data of Credentials ***[b1/p131]***

Recon – User: Retrieving Documents for Metadata Analysis *[b1/p125]*

Recon – User: Strings Command Details *[b1/p127]*

Red Team *[b1/p16, p18, p21]*

RFP (Request for Proposal) *[b1/p83]*

RIPE NCC *[b1/p111]*

RIRs (Regional Internet Registries) *[b1/p111]*

Risk *[b1/p14]*

Risk Reduction *[b1/p15]*

RoE (Rules of Engagement) *[b1/p63, p69, p74, p79, p80, p82, P83]*

Ss

Scope *[b1/p63, p69, p72, p73, p79, p80, p82, P83]*

Scope Creep *[b1/p72]*

Searching for File Types *[b1/p118]*

Security Audits *[b1/p16, p20]*

SEGUID *[b1/p51, p52]*

Server *[b1/p30]*

SETUID *[b1/p51, p52]*

Shodan *[b1/p113, p114]*

SOA *[b1/p104, p105]*

Social engineering test *[b1/p24, p91]*

Social Engineering and Recon Ethics *[b1/p91]*

SOW (Statement of Work) *[b1/p79]*

SPF (Sender Policy Framework) *[b1/p110]*

SpiderFoot *[b1/p140, p141,]*

SpiderFoot HX *[b1/p140]*

Strings Command Details *[b1/p127]*

subdomain *[b1/p106, p108]*

System Stability *[b1/p68]*

Tt

Target *[b1/p30, p87]*

Testing Machines/System *[b1/p30]*

Third Parties *[b1/p73]*

Threat *[b1/p12]*

Tools *[b1/p37, p38, p39, p40]*

Tools and Exploits *[b1/p37]*

Tools for Penetration Testing Teams *[b1/p40]*

TTPs (Tactics, Techniques, and Procedures) *[b1/p18]*

Types of Shared Data *[b1/p88]*

Uü

Unintentional Sharing *[b1/p88]*

User *[b1/p30]*

User Information *[b1/p87]*

Vv

Victim *[b1/p30]*

Vulnerability *[b1/p11]*

Vulnerability Assessments *[b1/p16, p21]*

Vulnerability Scanners *[b1/p39]*

Ww

Web application test *[b1/p24]*

WHOIS *[b1/p111]*

Wireless security test *[b1/p24]*

Xx

-

Yy

-

Zz

Zero-Knowledge vs. Full-Knowledge Testing *[b1/p77]*

Zero Touch *[b1/p90]*

Zone Transfer *[b1/p105]*

560.2 In-Depth Scanning and Initial Access

Aa

Account Lockout *[b2/p96]*

Account Lockout on Windows *[b2/p97]*

ACK (Acknowledgment Number) *[b2/p14, p15, p16]*

Actual Port Scanning (Phase 2) *[b2/p29]*

Agent-based Scan *[b2/p81, p82]*

ALockout.dll *[b2/p96]*

Authenticated Scan *[b2/p81, p82]*

Bb

blocked *[b2/p18, p19, p23]*

Cc

Client-side exploits *[b2/p110, p112, p113, p114, p115, p116, p117]*

Client-side exploits: Deliver Payloads to a test system *[b2/p116]*

Client-side exploits and Guardrails *[b2/p115]*

Client-side exploits: Commonly Vulnerable Software *[b2/p113]*

Client-side exploits: Mounting a Client-Side Exploitation Campaign *[b2/p114]*

Client-side exploits: Use Appropriate, Representative Client Machines *[b2/p117]*

Client-side exploits: Using Payloads on Target Systems *[b2/p116]*

closed *[b2/p18, p23, p33]*

closed | filtered *[b2/p34]*

compromising a machine *[b2/p106]*

Connect Scan *[b2/p33]*

Control Bits *[b2/p14, p15]*

Credential Databases *[b2/p92]*

Credential Stuffing *[b2/p91]*

Custom Dictionary *[b2/p94]*

CWR *[b2/p15]*

Dd

Dealing with Very Large Scans *[b2/p7]*

dehashed.com *[b2/p92]*

DomainPasswordSpray *[b2/p98]*

Ee

ECE *[b2/p15]*

echo "" command *[b2/p56]*

exploit/multi/handler *[b2/p126]*

/etc/services *[b2/p49]*

Exploit *[b2/p106]*

Exploit Categories*[b2/p109, p110]*

Exploit Rankings *[b2/p128]*

Exploitation *[b2/p106, p107, p108]*

Exploitation: What Is Exploitation? *[b2/p106]*

Exploitation: Why Exploitation? *[b2/p107]*

Exploitation: Risks of Exploitation *[b2/p108]*

ext_server_priv.dll *[b2/p142]*

ext_server_stdapi.dll *[b2/p142]*

EyeWitness *[b2/p60, p61, p62, p63, p64]*

EyeWitness: Report Content *[b2/p63]*

EyeWitness: Specifying Targets *[b2/p62]*

EyeWitness: What to Look For *[b2/p64]*

Ff

Faster Scanning *[b2/p41]*

filtered *[b2/p19, p23, p33]*

FIN *[b2/p15]*

Firewall Filtering *[b2/p111]*

Gg

560.2 In-Depth Scanning and Initial Access

Goals of Scanning Phase *[b2/p5]*

Guardrails *[b2/p115]*

Hh

half-open scan *[b2/p19, p33]*

Handling Large Scans by Limiting Scope *[b2/p8]*

Handling Large Scans by Speeding Up *[b2/p9]*

Handshake *[b2/p16, p17]*

Hop Limit *[b2/p12]*

Host Detection *[b2/p31]*

Hydra / xHydra / THC-Hydra *[b2/p95, p99, p100, p101, p102]*

Hydra Examples *[b2/p101]*

Hydra's pw-inspector *[b2/p95]*

Hydra with the Domain *[b2/p102]*

Ii

IANA (Internet Assigned Numbers Authority) *[b2/p49]*

ICMP message types *[b2/p19, p23]*

ICMP Port Unreachable *[b2/p19, p20, p23, p34]*

Important TCP Ports/Services *[b2/p31]*

Important UDP Ports/Services *[b2/p34]*

inaccessible *[b2/p19, p24]*

Initial Access *[b2/p87, p88]*

Initial Access: Where Does Access Come From *[b2/p88]*

IPv4 Header *[b2/p11]*

IPv6 *[b2/p35, p36]*

IPv6 Header *[b2/p12]*

Important IPv6 Addresses *[b2/p36]*

ISNA (initial sequence number) *[b2/p16]*

Jj

-

Kk

-

Ll

leakcheck.net *[b2/p92]*

Linux Exploit Suggester *[b2/p119]*

Local Privilege Escalation Exploits *[b2/p110, p118, p119]*

Local Privilege Escalation Attack Categories and Suites *[b2/p119]*

Lockout duration *[b2/p97]*

Lockout observation window *[b2/p97]*

Lockout threshold *[b2/p97]*

LockoutStatus.exe *[b2/p96]*

Mm

Masscan *[b2/p9, p41, p42, p43, p44]*

Masscan: Extracting Live Hosts and Open Ports *[b2/p44]*

Masscan Output *[b2/p43]*

Metasploit *[b2/p121, p122, p123, p124, p125, p126, p127, p128, p129, p130, p131, p132, p141]*

Metasploit Arsenal *[b2/p122]*

Metasploit Exploit Arsenal *[b2/p126]*

Metasploit: Exploit Rankings *[b2/p128]*

Metasploit Full Payload *[b2/p129]*

Metasploit Modules *[b2/p125]*

Metasploit Modules: Payloads *[b2/p129]*

Metasploit Payloads: Windows Singles *[b2/p130]*

Metasploit Payloads: Windows Stagers *[b2/p131]*

Metasploit Payloads: Windows Stages *[b2/p132]*

Metasploit: Pivoting Using Metasploit's route Command *[b2/p141]*

metasploit route *[b2/p141]*

Metasploit User Interfaces *[b2/p124]*

Metasploit: Windows Exploits *[b2/p127]*

Meterpreter *[b2/p133, p134, p135, p136, p137, p138, p139, p140, p141, p142]*

Meterpreter: Additional Modules *[b2/p142]*

Meterpreter Base Commands *[b2/p134]*

Meterpreter File System Commands *[b2/p136]*

Meterpreter Keystroke Logger *[b2/p140]*

Meterpreter Networking Commands *[b2/p137]*

Meterpreter: Pivoting Using Metasploit's route Command *[b2/p141]*

Meterpreter Process Commands *[b2/p135]*

meterpreter route *[b2/p137, p141]*

Meterpreter Target Machine Console Interface and Screenshot *[b2/p138]*

Meterpreter Webcam and Mic Commands *[b2/p139]*

metsrv.dll *[b2/p142]*

.msf4 *[b2/p139]*

msfconsole*[b2/p124]*

msfd*[b2/p124]*

msfrpcd*[b2/p124]*

msfvenom*[b2/p124]*

Nn

ncat *[b2/p52]*

Ncrack *[b2/p99]*

net accounts *[b2/p97]*

Netcat *[b2/p52, p53, p54, p55, p56, p57, p58, p59]*

Netcat: Automating Service String Information Gathering *[b2/p56]*

Netcat Client Grabbing Service Info *[b2/p55]*

Netcat Command Flags *[b2/p53]*

Netcat Listener Grabbing Client Info *[b2/p58]*

Netcat: Moving Files *[b2/p59]*

Netcat Uses for PenTesters and Ethical Hackers *[b2/p54, p55, p56, p57, p58, p59]*

Network Sweep *[b2/p6]*

Nmap *[b2/p26, p27, p28, p29, p30, p31, p32, p33, p34, p35, p36]*

Nmap Active OS Fingerprinting *[b2/p48]*

Nmap Address Probing *[b2/p29]*

Nmap Host Detection *[b2/p31]*

Nmap Input/Output Options *[b2/p28]*

Nmap Limitations and Host Groups *[b2/p40, p41]*

Nmap Network Probe/Sweeping Options *[b2/p30]*

Nmap Optimizing Host Detection *[b2/p31]*

Nmap Port Scanning *[b2/p32]*

Nmap Scan Speeds with Timing Options *[b2/p27]*

Nmap Scripting Engine (NSE) *[b2/p26]*

Nmap Support for IPv6 *[b2/p35, p36]*

Nmap SYN Stealth Scan *[b2/p33]*

Nmap TCP Port Scan Types: Connect Scan *[b2/p33]*

Nmap Timing Options *[b2/p27]*

Nmap UDP Scans *[b2/p34]*

***Nmap* Version Scanning** *[b2/p49, p50, p70]*

no response *[b2/p24]*

NSE (Nmap Scripting Engine) *[b2/p26, p72, p73, p78]*

NSE Scripts *[b2/p73]*

NSE Script Categories *[b2/p74]*

NSE Scripts: Some Examples *[b2/p75]*

Null RPC *[b2/p50]*

Oö

Online Password Attacks Types *[b2/p93]*

open *[b2/p18, p23, p33]*

open | filtered *[b2/p24]*

OS Fingerprinting *[b2/p48]*

Pp

P0f2 *[b2/p48]*

Password Attacks Types: Online *[b2/p93]*

Password complexity requirements *[b2/p94]*

Password Guessing *[b2/p89, p90, p91, p92, p93, p94, p95, p96, p97, p98, p99, p100, p101, p102]*

Password Guessing (Traditional) *[b2/p93]*

Password Guessing: Account Lockout *[b2/p96]*

Password Guessing: Account Lockout on Windows *[b2/p97]*

Password Guessing: Credential Databases *[b2/p92]*

Password Guessing: Credential Stuffing *[b2/p91]*

Password Guessing: Hydra Examples *[b2/p101]*

Password Guessing: Hydra with the Domain *[b2/p102]*

Password Guessing: Making Good Guesses with a Custom Dictionary *[b2/p94]*

Password Guessing: Suggested Spray Technique *[b2/p98]*

560.2 In-Depth Scanning and Initial Access

Password Guessing: THC-Hydra *[b2/p100]*

Password Guessing Tools *[b2/p99]*

Password Guessing: Trimming Word Lists with Hydra's pw-inspector *[b2/p95]*

Password Guessing: Types of Online Password Attacks *[b2/p93]*

Password Guessing: Primacy of Passwords *[b2/p90]*

Password Spray *[b2/p93, p98]*

Password Spray Technique *[b2/p98]*

Patator *[b2/p99]*

Payloads *[b2/p129]*

ping6 *[b2/p36]*

pivoting *[b2/p137, p141]*

Pivoting Using Metasploit's route Command *[b2/p141]*

portfwd *[b2/p137]*

Port Scanning *[b2/p18, p19, p22, p23, p24, p32]*

Ports/Services: TCP *[b2/p31]*

Ports/Services: UDP *[b2/p34]*

Probe (Phase 1) *[b2/p29]*

Probe (Phase 2) *[b2/p29]*

Protocol Layers *[b2/p13]*

PSH *[b2/p15]*

pw-inspector *[b2/p95]*

Qq

-

Rr

representative sample *[b2/p117]*

RST *[b2/p15, p19, p20, p33]*

RST-ACK *[b2/p18, p19, p20]*

Ss

scada *[b2/p127]*

Scanning Phase *[b2/p5]*

Scan Types *[b2/p6]*

ScanRand *[b2/p9]*

script.db *[b2/p75]*

scylla.sh *[b2/p92]*

sequence numbers *[b2/p14, p16]*

Service-side exploits *[b2/p110, p111]*

singles *[b2/p129]*

smb *[b2/127]*

Socat *[b2/52]*

stagers *[b2/p129]*

stages *[b2/p129]*

stdapi *[b2/p137, p142]*

SuperScan *[b2/p9]*

SYN *[b2/p15, p16]*

SYN-ACK *[b2/p16, p18, p19, p33]*

SYN Scan *[b2/p33]*

SYN Stealth Scan *[b2/p33]*

Tt

TCP *[b2/p13]*

TCP_55553/TCP_55554 *[b2/p124]*

TCP Behavior While Port Scanning *[b2/p18, p19]*

TCP Connect Scan *[b2/p33]*

TCP Control/Communication Bits/Flags *[b2/p14, p15]*

TCP Header *[b2/p14]*

Three-Way Handshake *[b2/p16, p33]*

traceroute *[b2/p50]*

Traditional Password Guessing *[b2/p93]*

Trimming Word Lists with Hydra's pw-inspector *[b2/p95]*

TTL (Time To Live) *[b2/p11]*

Uü

Unauthenticated Scan *[b2/p81, p82]*

UDP *[b2/p13]*

UDP Behavior While Port Scanning *[b2/p23, p24]*

UDP Checksum *[b2/p21]*

UDP Header *[b2/p21]*

UDP Message Length *[b2/p21]*

UDP Port Scanning *[b2/p22, p23, p24]*

Unicornscan *[b2/p9]*

URG *[b2/p15]*

Vv

Version Scanning *[b2/p49, p50, p70]*

VNC (Virtual Network Computing) *[b2/p127]*

vncinject *[b2/p132]*

Vulnerability Scanners *[b2/p78, p79, p80, p81, p82, p83, p84]*

Vulnerability Scanners: Scan Results *[b2/p84]*

Vulnerability Scanners: Safe Checks and Dangerous Plugins *[b2/p83]*

Vulnerability Scanners: Scan Types *[b2/p81]*

Vulnerability Scanners: Scanner Goals *[b2/p79]*

Vulnerability Scanners: Scanner Types *[b2/p80]*

Vulnerability Scanning: Methods for Discovering Vulnerabilities *[b2/p68]*

Vulnerability Scanning: Nmap Version Scan as Vulnerability Scanner? *[b2/p70]*

Vulnerability Scanning Tools (General Purpose) *[b2/p82]*

Ww

well-known ports *[b2/p49]*

Windows Exploits *[b2/p127]*

Xx

-

Yy

-

Zz

Zmap *[b2/p9]*

560.3 Assumed Breach, Post-Exploitation, and Passwords

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]*

560.3 Assumed Breach, Post-Exploitation, and Passwords

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]*

560.3 Assumed Breach, Post-Exploitation, and Passwords

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]*

560.3 Assumed Breach, Post-Exploitation, and Passwords

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]*

560.4 Lateral Movement and Command and Control (C2)

Aa

3gstudent template *[b4/p106]*

AC/DC Thunderstruck *[b4/p73]*

accepteula *[b4/p20]*

AMSI (Anti-Malware Scanning Interface) *[b4/p81, p82, p83, p84, p85, p89]*

AMSI DLL *[b4/p83, p84, p89]*

amsiInitFailed *[b4/p84]*

AmsiScanBuffer *[b4/p83, p84]*

AMSI ScanContent() *[b4/p83, p84]*

amsiutils *[b4/p85, p86]*

Application Control *[b4/p97]*

Application Control ***Bypass [b4/p98, p99, p100, p101, p102, p103, p104, p105, p106]***

at *[b4/p19, p23, p24]*

atexec.py *[b4/p37]*

AV/EDR Evasion *[b4/p78, p79, p80, p81, p82, p88, p89, p95, p98]*

Bb

BC Security *[b4/p69]*

Beacon *[b4/p54]*

Behavioral analytics *[b4/p81]*

binpath *[b4/p25, p26]*

Bypassing AMSI *[b4/p84, p85, p86]*

Bypassing AMSI - Downgrade Attacks *[b4/p85]*

Bypassing AMSI - String Modification *[b4/p86]*

Bypass Hooks *[b4/p89]*

Bypassing Signature-Based Detections *[b4/p90]*

Bypassing Windows Defender *[b4/p91, p92, p93, p94]*

Cc

C2 Matrix *[b4/p55, p56]*

Carbon Black (CB) Protection *[b4/p97]*

Cobalt Strike *[b4/p54]*

Command and Control (C2 or C&C) *[b4/p47, p54, p58, p59]*

Client Challenge Blob *[b4/p45]*

Command Line Kung Fu *[b4/p9]*

Covenant *[b4/p54]*

cmd.exe *[b4/p13, p26]*

commands on a remote windows machine *[b4/p19]*

Dd

DCOM *[b4/p37]*

dcomexec.py *[b4/p37]*

DefenderCheck *[b4/p91, p92]*

DNS Canary *[b4/p60]*

DRSUAPI *[b4/p36]*

Dump Hash *[b4/p36, p48]*

Dynamic Analysis *[b4/p81]*

Ee

Empire *[b4/p69, p70, p71, p72]*

Empire Modules *[b4/p72, p73, p74]*

Executable *[b4/p26]*

Extracting Hashes *[b4/p36]*

Evade *[b4/p78]*

Evasion *[b4/p78]*

Ff

-

Gg

GatewayPorts *[b4/p112]*

Get-Credential *[b4/p11]*

GetUserSPNs.py *[b4/p35]*

Golden ticket *[b4/p35]*

Grunt *[b4/p54]*

Guard Rails *[b4/p62, p65]*

Hh

Hashes *[b4/p36, p43]*

HMAC-MD5 key *[b4/p45]*

Ii

Impacket *[b4/p29, p34, p35, p36, p37]*

Invoke a Program *[b4/p27]*

Invoke-Command *[b4/p11]*

IPC$ *[b4/p14]*

Implant *[b4/p54]*

iptables *[b4/p5]*

Jj

JBoss *[b4/p73]*

Jenkins *[b4/p73]*

jitter *[b4/p54]*

Kk

Kerberos *[b4/p35]*

Kerberoasting attack *[b4/p35]*

Kerberos Ticket Reuse *[b4/p12]*

Ll

LANMAN Challenge/Response *[b4/p49]*

Lateral Movement *[b4/p5]*

Live off the Land *[b4/p8]*

LM-NT *[b4/p48]*

Local Security Authority Subsystem Service (LSASS) *[b4/p43, p46, p74]*

Mm

Making an Executable *[b4/p26]*

Metasploit PsExec *[b4/p22, p48, p49]*

Metasploit Route *[b4/p116]*

Microsoft AppLocker *[b4/p97]*

mknod *[b4/p5]*

MMC20.Application *[b4/37]*

mount a share *[b4/p14]*

MSBuild.exe *[b4/p98, p99, p100, p101, p102, p103, p104, p105, p106]*

multiplayer *[b4/p64]*

Nn

nc.exe *[b4/p26, p30]*

.NET Assemblies *[b4/p60, p98, p99]*

NETBIOS *[b4/p14]*

netcat *[b4/p26, p30]*

netsh *[b4/p5]*

net time *[b4/p23]*

net use *[b4/p14, p21, p23, p25]*

/node@[filename] *[b4/p27]*

NTDS.dit *[b4/p36]*

NT Hash *[b4/p45, p49]*

NTLMv1 *[b4/p49]*

NTLMv2 *[b4/p45, p49]*

Null session *[b4/p14]*

Oö

-

Pp

Pass-the-Hash *[b4/p22, p43, p44, p45, p46, p47, p48, p49]*

Password Attacks *[b4/p49]*

Pivoting *[b4/p110, p111, p112, p113, p114]*

Port Forwarding *[b4/p5,p111, p112, p113, p114]*

Port Forwarding through a Meterpreter Session

560.4 Lateral Movement and Command and Control (C2)

[b4/p114]

Posh-SecMod *[b4/p69, p72]*

PowerBreach *[b4/p72]*

powershell *[b4/p11, p69]*

PowerStripper *[b4/p88]*

PowerSploit *[b4/p69, p72, p88]*

PowerUp *[b4/p72]*

PowerView *[b4/p72]*

process *[b4/p28]*

process call *[b4/p27]*

process list brief *[b4/p28]*

process where *[b4/p28]*

proxychains *[b4/p113]*

PsExec *[b4/p8, p19, p20, p21, p22]*

psexec.py [b4/p37]

Qq

-

Rr

relative identifier / RID 500 *[b4/p46]*

RemComSvc *[b4/p37]*

RSA *[b4/p59]*

Rubeus *[b4/p12]*

Runtime analysis *[b4/p81]*

Ss

SAM *[b4/p36, p43]*

sc *[b4/p16, p19, p25]*

sc config *[b4/p17]*

schtasks *[b4/p19, p23, p24]*

schtasksabuse *[b4/p24]*

sc query *[b4/p16, p18, p23]*

sc qc *[b4/p16, p17]*

sc start *[b4/p17]*

sc stop *[b4/p17]*

Scheduling a job *[b4/p23]*

secretsdump.py *[b4/p36]*

Security Advisory 2871997 *[b4/p46]*

Server Challenge *[b4/p45]*

Server Message Block (SMB) *[b4/p14, p29, p49]*

Service Name *[b4/p18]*

Service Principal Names (SPNs) *[b4/p35]*

services.msc *[b4/p17, p18]*

Service Controller (sc) *[b4/p16, p25]*

SharpBlock *[b4/p89]*

ShellWindows *[b4/p37]*

ShellBrowserWindow *[b4/p37]*

Signature-based *[b4/p81, p87, p90]*

Silver ticket *[b4/p35]*

Sliver *[b4/p54, p58, p59, p60, p61, p62, p63, p64, p65]*

Sliver Implant Commands *[b4/p63]*

Sliver Payload *[b4/p61, p62, p65]*

smb session *[b4/p14, p15, p21, p22, p23]*

smbexec *[b4/p36]*

smbexec.py *[b4/p37, p39]*

SOCKS *[b4/p113, p114, p117]*

ssh *[b4/p5]*

sshd_config *[b4/p112]*

SSH Dynamic Port Forwarding *[b4/p113, p117]*

SSH Local Port Forwarding *[b4/p111, p117]*

SSH Remote Port Forwarding *[b4/p112]*

Sysinternals PsExec *[b4/p20, p21]*

Static Analysis *[b4/p81]*

Static Analysis Evasion *[b4/p87]*

Stripping PowerShell Comments [b4/p88]

Tt

Task Scheduler *[b4/p37]*

tcp 135-139 *[b4/p14, p39]*

tcp 445 *[b4/p14, p39]*

tcp 5985/5986 *[b4/p10]*

Test-NetConnection *[b4/p11]*

Test-WSMan *[b4/p11]*

Ticket Reuse *[b4/p12]*

ticketer.py *[b4/p35]*

Trollsploit [b4/p74]

Uü

-

Vv

Virustotal ***[b4/80]***

VSSADMIN ***[b4/p36]***

Ww

Windows Defender Credential Guard ***[b4/p46]***

Windows Lateral Movement *[b4/**p8**]*

Windows Remote Management (WinRM) *[b4/**p8, p10**]*

winrs tool ***[b4/p10]***

WMI/WMIC *[b4/**p8**]*

WMIC (Windows Management Instrumentation) *[b4/**p18, p19**, p27, **p28, p29**, p37]*

wmic service *[b4/**p18**]*

wmiexec ***[b4/p36]***

wmiexec.py ***[b4/p37, p39]***

Xx

-

Yy

-

Zz

-

[1] 560.5 Domain Domination, Azure Annihilation, and Reporting

Dd

Domain Domination *[b5/**p28**]* - Domain Domination and AD Persistence

Domain Domination *[b5/**p29**]* - Obtaining Access to Back-Up NTDS.dit File

Domain Domination *[b5/**p31**]* - Creating a Domain Admin Account

Domain Domination *[b5/**p32**]* – Skeleton Key

Domain Domination *[b5/**p33**]* – Skeleton Key in Action

Domain Domination *[b5/**p34**]* – Replicating the Domain: DCSync

Domain Domination *[b5/**p35**]* – Replicating the Domain: DCSync Example

Domain Domination *[b5/**p36**]* – Becoming a Domain Controller: DCShadow

Domain Domination *[b5/**p37**]* – Becoming a Domain Controller: DCShadow in Action

****

Domain PrivEsc *[b5/**p59**]* - PowerView Find-InterestingDomainShareFile

Domain PrivEsc *[b5/**p60**]* - PowerView Find-LocalAdminAccess

Domain PrivEsc *[b5/**p61, p62**]* - Privilege Escalation

Gg

Golden Ticket *[b5/**p52**]*

Golden Ticket *[b5/**p53**]* - Kerberos Flow with Golden Ticket

Golden Ticket *[b5/**p54**]* - Golden Ticket Properties

Golden Ticket *[b5/**p55**]* - Golden Ticket Tools

Kk

Kerberos *[b5/**p5, p12, p53, p54**]*

Kerberos *[b5/**p6**]* - How it works

Kerberos *[b5/**p7**]* - Pre-Authentication and TGT

Kerberos *[b5/**p8, p9**]* - Authenticating to a Service

Kerberos *[b5/**p10**]* - Overall Flow

Kerberos *[b5/**p11**]* - AS-REQ with Pre-Authentication and AS-REP

Kerberos *[b5/**p12**]* - TGT (Ticket Granting Ticket) and PAC

Kerberos *[b5/**p13**]* - Requesting a Service Ticket (ST)

Kerberos *[b5/**p14**]* - Service Principal Name

Kerberos *[b5/**p15**]* - Using a Service Ticket (ST)

Kerberos *[b5/**p16**]* - Service Ticket

Kerberos *[b5/**p17**]* - Kerberos: Three Long-Term Keys

****

Kerberoast *[b5/**p19**]* - Requesting a Service Ticket (ST) Revisited

Kerberoast *[b5/**p20**]* - Requesting a Ticket

Kerberoast *[b5/**p21**]* - Kerberos Attack

Kerberoast *[b5/**p22**]* - Obtaining Tickets

Kerberoast *[b5/**p23**]* - Kerberoast Attack Steps

Kerberoast *[b5/**p24**]* - What Service Accounts are Good Targets?

****

More Kerberos Attacks *[b5/**p41**]* – Pass-the-Ticket

More Kerberos Attacks *[b5/**p42**]* – Pass-the-Ticket: Mimikatz Example

More Kerberos Attacks *[b5/**p43**]* – Overpass-the-Hash

More Kerberos Attacks *[b5/**p44**]* – Golden Ticket Overview

Ss

Silver Ticket *[b5/**p46**]*

Silver Ticket *[b5/**p47**]* - Generating a Silver Ticket with Impacket Silver Ticket

Silver Ticket *[b5/**p48**]* - Silver Ticket Use

AD replication *[b5/**p34**]*

AES *[b5/**p43, p52**]*

AGPMServer *[b5/**p24**]*

AS-REP *[b5/**p10, p11, p17, p19, p43, p53**]*

AS-REP Roasting *[b5/**p62**]*

AS-REQ *[b5/**p10, p11, p15, p17, p19, p32, p43, p53**]*

Authentication Server (AS) *[b5/**p7, p10, p11, p15**]*

brute force attacks *[b5/**p23**]*

Client long-term secret key *[b5/**p17**]*

Comsvcs.dll *[b5/**p61**]*

DCSync *[b5/**p28, p34, p35, p36**]*

DCSync attack *[b5/**p34**]*

DCShadow *[b5/**p28, p36, p37**]*

560.5 Domain Domination, Azure Annihilation, and Reporting

Directory Replication Service Remote (DRSR) *[b5/p35, p36]*

Domain Admin *[b5/p31, p34]*

Domain Administrator *[b5/p44]* – RID 512

Domain Controller *[b5/p34, p36]*

Domain replication protocol *[b5/p34]*

Domain SID *[b5/p55]* – (S-1-5-21-XXX…….)

empire *[b5/p22]*

FIMService *[b5/p24]*

FQDN (fully qualified domain name) *[b5/p14]*

GetUserSPNs.py *[b5/p22]*

Golden Ticket *[b5/p28, p34, p35, p44, p52, p53, p54, p55]*

hashcat *[b5/p22]*

impacket *[b5/p22, p29, p47, p48, p62]*

Install from Media (IFM) *[b5/p29, p30]*

Invoke-Kerberoast *[b5/p22]*

jtr (john the ripper) *[b5/p22]*

KDC LT key (krbtgt NT hash) *[b5/p12, p46, p52]*

KDC long-term secret key *[b5/p17]*

Kerberoasting *[b5/p16, p62]*

Kerberos server *[b5/p5]*

Key Distribution Center (KDC) *[b5/p7, p8, p11, p17, p19, p20, p46]*

krbtgt *[b5/p11, p15, p17]*

krbtgt hash *[b5/p35, p44, p46, p52, p54, p55]*

krbtgt NT hash (KDC LT key) *[b5/p12]*

KRB5CCNAME *[b5/p48]*

lsadump *[b5/p35, p37]*

lsass.exe *[b5/p561]*

mimikatz *[b5/p22, p32, p33, p34, p35, p36, p37, p41, p42, p48, p55]*

MS-DRSR *[b5/p36]*

MSSQL/MSSQLSvc *[b5/p24]*

NT hash *[b5/p52]*

NTDS.dit *[b5/p28, p29, p34]*

ntdsutil.exe *[b5/p29]*

Overpass-the-Hash *[b5/p43]*

PAC (rivilege Attribute Certificate) *[b5/p8, p9, p12, p17, p44, p46, p52]*

PAC Validation *[b5/p46] [Old b5/p12, p17]*

Pass-the-Hash attack (PtH) *[b5/p43]*

pass-the-ticket (ptt) *[b5/p48]*

PowerSploit *[b5/p22]*

PowerSploit Out-MiniDump *[b5/p61]*

PowerView *[b5/p59, p60]*

Privilege Attribute Certificate (PAC) *[b5/p8, p9, p12, p17, p44, p46, p52]*

Procdump *[b5/p61]*

Process Explorer *[b5/p61]*

PsExec *[b5/p42]*

RC4 encryption *[b5/p32, p52]*

RC4_HMAC_MD5 *[b5/p21, p43]*

RC4 service tickets *[b5/p23]*

registry *[b5/p29, p30]*

Responder style attacks *[b5/p62]*

RID 512 *[b5/p44]* - Domain Administrator

Rubeus *[b5/p41, p48, p62]*

RunDLL32 *[b5/p61]*

secretsdump.py *[b5/p29]*

Security Token Service (STS) *[b5/p24]*

Service Principal Name (SPN) *[b5/p12, p14, p20, p21, p22, p23, p62]*

setspn.exe *[b5/p14]*

Service Ticket (ST) *[b5/p10, p13, p15, p16, p19, p21, p23, p41, p46, p53]*

Silver Ticket *[b5/p46, p47, p48]*

Skeleton Key *[b5/p28, p32, p33]*

Skeleton Key Attack *[b5/p32]*

SMBClient *[b5/p62]*

Sysinternals *[b5/p42, p61]*

System Key *[b5/p29]*

SYSTEM registry hive *[b5/p29, p30]*

Target LT Key *[b5/p12, p52]*

Target long-term secret key *[b5/p17, p19]*

Task Manager *[b5/p61]*

TGS-REP *[b5/p10, p13, p17, p19, p53]*

TGS-REQ *[b5/p10, p12, p13, p19, p53]*

Ticket Granting Service (TGS) *[b5/p10, p11, p15]*

Ticket Granting Ticket (TGT) *[b5/p7, p8, p10, p11, p12, p15, p19, p41, p43, p44, p52, p54]*

ticketer.py *[b5/p47, p55]*

Volume Shadow Copy Service *[b5/p29]*

wmiexec.py *[b5/p48]*

1 560.5 Domain Domination, Azure Annihilation, and Reporting

Aa

Azure *[b5/**p64**]*

Azure *[b5/**p65**]* - Azure Services

Azure *[b5/**p66**]* - Interacting with Online Services

Azure *[b5/**p67**]* - Azure in relation to Azure

****

Azure AD *[b5/**p69**]* – Microsoft Azure AD

Azure AD *[b5/**p70, p71, p72, p73**]* – Azure AD Authentication Flow

Azure AD *[b5/**p74**]* – Microsoft Authentication Systems

Azure AD *[b5/**p75**]* – Identity Architectures in Microsoft

Azure AD *[b5/**p76**]* – Synchronization and Federation

Azure AD *[b5/**p77**]* – Cloud Identity Models

Azure AD *[b5/**p77**]* – Authentication for Hybrid Indentity

****

Azure Recon *[b5/**p78**]* – Introduction to AADInternals

Azure Recon *[b5/**p79**]* – AADInternals Recon

Azure Recon *[b5/**p80**]* – Username Enumeration Endpoints

Azure Recon *[b5/**p81**]* – Username Enumeration: GetCredentialType Endpoint

Azure Recon *[b5/**p83**]* – Detecting Throttling: GetCredentialType Endpoint

Azure Recon *[b5/**p84, p85**]* – Username Enumeration: OAuth Token Endpoint

Azure Recon *[b5/**p86**]* – Legacy Authentication and Protocols

****

Azure Password Attacks *[b5/**p89**]* – Password Spraying in Azure

Azure Password Attacks *[b5/**p90**]* – Password Spraying Tool: TrevorSpray

Azure Password Attacks *[b5/**p92**]* – Password Spraying Tool: Spray365

Azure Password Attacks *[b5/**p94**]* – Azure Smart Lockout

Azure Password Attacks *[b5/**p96**]* – Bypass Strategies for Avoiding Lockout

Azure Password Attacks *[b5/**p97, p98**]* – Bypassing Technique: Rotating IP Addresses

****

OpenID *[b5/**p102**]* – OpenIDConnect Flows

OpenID *[b5/**p103-p112**]* – Authentication Flows

OpenID *[b5/**p113**]* – OAuth Flow Types

****

Azure Infrastructure *[b5/**p115**]* – Infrastructure Components

Azure Infrastructure *[b5/**p116**]* – How Azure Organizes Items

Azure Infrastructure *[b5/**p117**]* – Control Plane and Data Plane

****

Running Commands on Azure *[b5/**p119**]* – Azure CLI Tools

Running Commands on Azure *[b5/**p120**]* – Azure CLI Basics

Running Commands on Azure *[b5/**p121**]* – Azure VM Operations

Running Commands on Azure *[b5/**p122**]* – Running Commands on Virtual Machines

****

ngrok *[b5/**p124**]* – Introduction to ngrok

ngrok *[b5/**p125**]* – How Does It Work?

ngrok *[b5/**p126**]* – Example ngrok Flow

ngrok *[b5/**p127**]* – Visualization of ngrok

****

Permissions on Azure *[b5/**p131**]* – What Is Better than Domain Admin (DA)? Global Administrator (GA)

Permissions on Azure *[b5/**p132**]* – Azure Permissions

Permissions on Azure *[b5/**p133**]* – Permissions IAM Document

Permissions on Azure *[b5/**p134**]* – Where Do Azure Permissions Get Applied?

Permissions on Azure *[b5/**p135**]* – Instance Metadata Services in Azure

Permissions on Azure *[b5/**p136**]* – Managed Identities in Azure

2 560.5 Domain Domination, Azure Annihilation, and Reporting

365Spray *[b5/p98]*

AADSTS *[b5/p85]*

AADInternals *[b5/p78, p79]*

AADIntPTASpy *[b5/p78]*

AADSTS 50053 (IdsLocked error code) *[b5/p94]*

Access Token *[b5/p107, p108, p109, p111, p112, p113, p136]*

Account Lockout *[b5/p94]*

Actions *[b5/p133]*

AD FS Federation *[b5/p76, p95]*

AD FS Extranet Lockout *[b5/p95]*

Assignable Scopes *[b5/p133]*

Authentication Flow *[b5/p70, p71, p72]*

authentication profiles *[b5/p136]*

autodiscover *[b5/p86]*

AWS API Gateway *[b5/p96, p98]*

AWS Terms of Service (ToS) *[b5/p98]*

az *[b5/p119]*

az vm *[b5/p120, p121, p122]*

Az Key Vault *[b5/p136]*

Az PowerShell 7 *[b5/p119]*

Azure Active Directory (Azure AD) *[b5/p65, p74, p75, p102, p104, p131]*

Azure Active Directory Domain Services (Azure AD DS) *[b5/ p74, p75]*

Azure AD Connect Agent *[b5/p76]*

Azure AD Connect Synchronization *[b5/p131]*

Azure AD Tenant *[b5/p70]*

Azure API Management *[b5/p115]*

Azure authentication library *[b5/p120]*

Azure Automation *[b5/p121]*

Azure Backup *[b5/p115]*

Azure Blobs *[b5/p115]*

Azure CLI *[b5/p66, p119, p120, P135]*

Azure Cloud Shell *[b5/p66, p119]*

Azure Compute *[b5/p115]*

Azure CosmosDB *[b5/p115]*

Azure DevOps *[b5/p115]*

Azure FrontDoor *[b5/p115]*

Azure Platform managed identity (System Assigned Managed Identity) *[b5/p136]*

Azure PowerShell Module(s) *[b5/p66]*

Azure Portal *[b5/p66, p70, p103,]*

Azure Smart Lockout *[b5/p84, p89, p90, p92, p94, p95, p96, p97, p98] [Old Book b5/p149]*

B2B (Business to Business) Federation *[b5/p74]*

B2C (Business to Customer) Federation *[b5/p74]*

base64 *[b5/p80]*

Basic Auth *[b5/p86, p96]*

Bearer Token *[b5/p107]*

BuiltIn Roles *[b5/p132, p133]*

BurpSuite *[b5/p92, p97, p98]*

BurpSuite IP Rotate *[b5/p96, p98]*

Central Authentication Server *[b5/p102]*

Client Credentials Flow *[b5/p113]*

Cloud Hosted Azure Active Directory Domain Services *[b5/p75]*

Cloud Identity *[b5/p77]*

Cloud Identity Models *[b5/p77] [Old b5/p70]*

Cloud-only Identity *[b5/p77] [Old b5/p70]*

Code Flow *[b5/p102, p104, p105, p113, p120]*

Conditional Access Policy *[b5/p72, p92, p105, p109, p112]*

Consent Screen *[b5/p106]*

Contributer *[b5/p132, p133, p134]*

Control Plane *[b5/p117]*

CSRF Code Flow *[b5/p113]*

curl *[b5/p80, p81, p83, p84, p135, p136]*

Custom Roles *[b5/p132]*

dataActions *[b5/p133]*

Data Plane *[b5/p117, p133]*

Device Code Flow *[b5/p113, p120]*

Device Code Flow Phishing *[b5/p113, p120]*

Domain Admin (DA) *[b5/p131]*

End user-managed identity (User Assigned Managed Identity) *[b5/p136]*

Enterprise Administrators *[b5/p131]*

error code response *[b5/p84, p85]*

error code response 50034 *[b5/p85]*

error code response 50126 *[b5/p85]*

Ews-Crack *[b5/p86]*

Exchange ActiveSync (EAS) *[b5/p86]*

exchange online powershell *[b5/p86]*

execution plan *[b5/p92]*

Extensions *[b5/p133]*

[3] 560.5 Domain Domination, Azure Annihilation, and Reporting

Extranet Smart Lockout *[b5/p95]*

fat clients *[b5/p70]*

Federated Identity *[b5/p77] [Old b5/p70]*

Federated Authentication *[b5/p77]*

FIDO2 *[b5/p102, p105]*

FireProx *[b5/p96, p98]*

flat structure *[b5/p74]*

GetCredentialType *[b5/p80, p81, p83]*

getuserrealm.srf *[b5/p81]*

Global Administrator (GA) *[b5/p131, p132]*

GUID *[b5/p132]*

high rate *[b5/p83, p84]*

Hosted Azure AD DS *[b5/p76]*

Hybrid Identity *[b5/p77]*

IAM (Identity Management System) *[b5/p66, p74, p75, p133, p134]*

Identity Models *[b5/p77]*

Identities *[b5/p136]*

IdP ***(Identity Provider)*** *[b5/p72, p76, p81, p82, p108, p110, p113]*

IfExistsResult *[b5/p81, p83]*

Instance Metadata Service (IMDS) *[b5/p135, p136]*

imap *[b5/p86]*

Invoke-AADIntUserEnumerationAsOutsider *[b5/p79]*

jitter *[b5/p90, p91, p97]*

jq *[b5/p81, p82, p83]*

JSON *[b5/p92, p122, p133]*

JSON Web Token (JWT) *[b5/p73, p107,p108]*

Kerberos *[b5/p74, p102]*

LDAP *[b5/p74, p75, p76, p102]*

IdsLocked (AADSTS 50053) *[b5/p94]*

legacy authentication *[b5/p86]*

legacy protocols *[b5/p86, p96, p102]*

Load Balancing *[b5/p96, p97]*

Log Analytics Contributor *[b5/p132]*

Management Groups *[b5/p116, p134]*

map4 *[b5/p86]*

MailSniper *[b5/p86]*

Managed Authentication *[b5/p77]*

Metadata *[b5/p135, p136]*

Metasploit Framework *[b5/p86]*

MFA *[b5/p86, p90, p102, p105, p108, p112]*

Microsoft Active Directory Domain Services (Microsoft AD DS) *[b5/p75]*

Microsoft Azure *[b5/p65]*

Microsoft Exchange Online *[b5/p86]*

MicrosoftOnline Login portal (MSOL) *[b5/p71, p104, p120]*

Microsoft Authentication Library (MSAL) *[b5/p120]*

MSOLSpray *[b5/p89]*

Modern authentication *[b5/p86, p102]*

NameSpaceType *[b5/p81]*

ngrok *[b5/p124]*

NT Hash *[b5/p76]*

NTLMv2 *[b5/p74]*

Oauth2 *[b5/p65, p74, p86, p87, p102, p104, p113, p120, p136]*

Oauth Token *[b5/p80, p84, p84, p89]*

Office 365 Portal *[b5/p66]*

Okta *[b5/p72, p74, p102]*

On Prem AD DS *[b5/p74]*

On Premise *[b5/p75]*

On Premise Active Directory *[b5/p76, p131]*

On-Premise Identity Provider *[b5/p77]*

OpenIDConnect Identity Provider (OIDC IdP) *[b5/p65, p74, p75, p102, p104, p107, p120, p131]*

Owner *[b5/p132]*

Pass-through Authentication (PTA) *[b5/p76, p77]*

Pass-Thru-Authentication agent *[b5/p78, p95]*

Password Guessing *[b5/p80, p84]*

Password Hash Synchronization (PHS) *[b5/p76, p77, p95]*

Password Protection *[Old Book b5/p150]*

Password Spraying *[b5/p89]*

PBKDF2 Hash *[b5/p76]*

Permissions *[b5/p132, p133, p134]*

Ping Federate *[b5/p72, p76]*

PKCE *[b5/p113]*

pop3 *[b5/p86]*

Powershell modules*[b5/p78, p119]*

Primary Refresh Token (PRT) *[b5/p107, p110, p111, p113]*

Prohibited Activities *[b5/p98]*

rate limit*[b5/p80]*

Reader *[b5/p132, p133]*

Refresh Token *[b5/p107, p110, p111, p113]*

Refresh Token Flow *[b5/p113]*

4 560.5 Domain Domination, Azure Annihilation, and Reporting

Resource Groups *[b5/p116, p134]*

Resources *[b5/p116, p134]*

Role Based Access Control (RBAC) *[b5/p66, p132]*

Role Name *[b5/p133]*

Roles *[b5/p132]*

Round-Robin *[b5/p96, p97]*

rst2.srf *[b5/p80]*

Runbooks *[b5/p121]*

S3-equivalent block storage *[b5/p115]*

SAML *[b5/p65, p74, p102]*

SCCM *[b5/p121]*

Secure Token Server (STS) *[b5/p108]*

SKU *[b5/p104]*

Smart Lockout *[b5/p84, p89, p90, p92, p94, p95, p96, p97, p98] [Old Book b5/p149]*

smtp *[b5/p86]*

smtp auth *[b5/p87]*

Spray365 *[b5/p89, p92, p94, p98]*

ssh *[b5/p97]*

SSO *[b5/p69]*

staging mode *[b5/p76]*

Subscriptions *[b5/p116, p134]*

Synchronized Identity *[b5/p77] [Old b5/p70]*

System Assigned Managed Identity (Azure Platform managed identity) *[b5/p136]*

Tenant *[b5/p72, p97]*

Terraform *[b5/p113]*

throttle *[b5/p83]*

ThrottleStatus *[b5/p83]*

Token Expiration *[b5/p110]*

TrevorProxy *[b5/p90, p97]*

TrevorSpray *[b5/p86, p89, p90, p94, p97]*

User Access Administrator Built-in role *[b5/p131]*

User Assigned Managed Identity (End user-managed identity) *[b5/p136]*

Username Enumeration *[b5/p80]*

User(name) Principal Name (UPN) *[b5/p70, p72, p73, p108]*

WS Federation *[b5/p74, p102]*

X.509 *[b5/p75]*

1 560.5 Domain Domination, Azure Annihilation, and Reporting

Rr

Reporting *[b5/p138]* - Always Create a Report

Reporting *[b5/p139]* - Don't Just Regurgitate Vuln Scan Results

Reporting *[b5/p140]* - Recommended Report Format

Reporting *[b5/p141, p142]* - Executive Summary

Reporting *[b5/p143]* - Introduction

Reporting *[b5/p144]* – Findings

Reporting *[b5/p145]* - Illustrating Findings with Screenshots

Reporting *[b5/p146]* - Screenshot Elements

Reporting *[b5/p147]* - Screenshot Tools

Reporting *[b5/p148]* - Redaction and Transparency

Reporting *[b5/p149, p150]* - Recommendations

Reporting *[b5/p151]* - Methodology

Reporting *[b5/p152]* - Appendices

Appendices *[b5/p140, p152]*

Appendix *[b5/p152]*

backup documentation *[b5/p152]*

Blackout *[b5/p148]*

Blur *[b5/p148]*

Brief Description *[b5/ p141]*

Brief Overview *[b5/ p141, p143]*

Business Impact *[b5/ p142]*

Business Risk *[b5/ p144]*

Conclusions and Future Considerations *[b5/p140]*

Date Range *[b5/p143]*

debriefings *[b5/ p143]*

detailed technical description *[b5/p140, p144]*

detailed technical results *[b5/p144]*

detailed vulnerability scan output *[b5/p52]*

Executive Summary *[b5/p140, p141, p142, p143, p144]*

Exploitation *[b5/ p144]*

Findings *[b5/p140, p141, p142, p144, p151]*

Flameshot *[b5/p147]*

Gimp *[b5/p147]*

Greenshot *[b5/p147]*

High Level *[b5/p140, p141, p142]*

Impact *[b5/ p144]*

In-house tests *[b5/p138]*

Introduction *[b5/p140]*

management level recommendations *[b5/p142]*

memos *[b5/p152]*

Methodology *[b5/p140, p151]*

Overview *[b5/ p143]*

Photoshop *[b5/p147]*

Pixilation *[b5/p148]*

Positive Findings *[b5/p141, p142]*

Recommendations *[b5/ p144, p149, p150]*

Redaction *[b5/p148]*

Risk *[b5/p141, p144, p150]*

Risk Level *[b5/p144]*

Root Causes *[b5/p142, p149]*

rules of engagement (RoE) *[b5/p152]*

Scope *[b5/p143, p152]*

Screenshots *[b5/p145]*

Snagit *[b5/p147]*

Snip & Sketch *[b5/p147]*

technical description *[b5/p144]*

Third-party testers *[b5/p138]*

Time Range *[b5/p143]*

Transparency *[b5/p148]*

Value Add *[b5/p150]*