# 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****]*

**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]***