# 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

**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]***

**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]***

**UDPBehavior 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****]*