# 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]***

**.NETAssemblies *[****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 *[****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]***

**processcall *[****b4****/p27]***

**processlist brief *[****b4****/p28]***

**processwhere *[****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

-