SEC660- Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

\mathbf{Index}	group policy objects	B2–66
802.1	hash extension	D9 55
Q/ISLB1–78	padding algorithms	
shadow		
supplicant	hot standby router protocol	
AMSI	hsrp	
arp spoofing	http	D1 169
ASLR B4–138-46	redirection	
assembly language	strict transport security	
basic blocks	tampering	L169
bgpB1–137	impersonation	D4 00 0
	browser	
bit flipping B2–31, L131	MAC	
border gateway protocolB1–137	operating system	
browser	user-agent	B1–63
caching	inter-switch	
canaries	LAN	
captive portalB1–52-69	IPv6	*
cdecl	anycast	
ciphers	enumeration	B1–149
blockB2–12	multicast	B1–144
streamB2-9	neighbor discovery	B1–151
IV reuse B2–48	prefixes	B1–144
cisco	remote discovery	B1–156
discovery protocolB1–88	router advertisement	B1–153
dtpB1–78	router solicitation	B1–153
port status codesB1-79	unicast	B1–144
client-side exploitB2-90-100, L1150	IV collision	
designated router B1–134	jop	B4–117
dll hijacking B2–111	juniper	
DTPB1–78	lldep-med	B1–78
VLAN hopping attackB1-79-86	kernel pool	
dynamic trunking protocolB1–78	kernel32.dll	
EAP	kiosk mode	
MD5 B1–71	krack attack	
TLSB1–71	library loading	
wired shadow attackB1–74	link-state advertisements	
ELF B4–40	linkers	
environment variable pointerB4–119	loaders	
exploit suggesters	lsa	
export address table	mmap	
fastcall	multicast	
filter	NAC	
ettercapB1–105	clientless	
manipulation		
fuzzing	dissolvable agent	
block coverage	neighbor discovery	
grammar	network admission control	
instrumented	object files	
	open shortest path first protocol	
intelligent mutation	oracle padding	
source-assisted	ospf	
Sulley	dictionary attack	
agents B3–136	enumeration	
analysis	route injection	
grammar	state tree	
gadgets B4–113	OUI	
ghostwriting B1–27	padding	B2–35
global offset tableB4-42	pae	
GPOs B2-66		

SEC660- Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

paging	B4–17
pairwise	B2–53
peb	B4–81
physical memory	B4–5
PIE	
PKCS	
port	
access	B1–78
trunk	
port access entity	
position independent executable	
powershell	
autoruns	B2–86
command order	
command precedence	
persistent modules	
procedure	
calling conventions	B4-31
epilogue	
prologue	
procedure linkage	
process environment block	
processors	
RADIUS	
registers	b1-/1
general	B4_7 14
segments	
relative virtual addresses	
relocation	
return2libcB4	
risk analysis	
rop	
routing traffic	
seh	
setuid	B4-97
shellcode	D4 50 74
linux	
multistage return-oriented	
windows	
signature detection	B1-27
smb	D1 100
capture	
relay	
signing	
software restriction policies	
sslstrip	B1–113
stack	D . 0.
operations	
overflows	
pointer	
protection	
tweaks	
stateless	
stdcall	
stripped programs	
structured exception handling	
supplicant	$R1_{-71}$

symbol resolution	B4–39
system calls	
test case splicing	
tlb	
tracing	,
linux	B2-102
windows	
translation lookaside buffers	
UAC	
user account control	
virtual memory	
virtual router redundancy protocol	
virtual routers	
virtualization	
VLAN	22 00
hopping	B1–85
trunking	
voice hopping	
vrrp	
WDAC	
wdac	
windows	
AMSI	B2-126
defender application control	
defenses	
EMET	
kernel resources	
Windows Defender	
App Control	B1-26
wired shadow attack	
wpa2	
ws2_32.dll	

SEC660- Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Invoke-MSIRypass	Tools/Commands	jackelope
Invoke-Obrluscation		· -
Table Tabl		
Agric Cuircorn B1-20		
debug.exe B2-73 metasploit dritrace B2-105 smb capture B1-106 httphijack.py B1-119 Mimikittenz L1158 iptables B1-66 miredo B1-155 ldd B4-149 mitumproxy B1-117, 120, 171 underprobe B1-84 mefwenom B2-74 objame B4-44 mefwenom B2-74 objame B4-44 Netwide Assmebler B4-65 ping6 B1-149 map B1-152 ping6 B1-149 map B1-152 ping6 B1-149 map B1-152 ping6 B1-149 map B1-152 ping6 B1-144 Not Powershell B2-72 sysct1 B1-84 Of Successed B1-65 xad B4-66 PacketFence B1-153 AFL B3-165, 13259 panopticilek B1-53 amsi fall B1-13 parasite6 B1-53 amsi fall B1-17 <td>•</td> <td></td>	•	
Satitrace B2-105 Simb capture B1-106 http.hijack.py B1-119 Mimikittenz L1158 https://dx.py B1-119 Mimikittenz L1158 https://dx.py B1-119 Mimikittenz L1158 https://dx.py B1-150 mitmodump B1-115 https://dx.py B1-117 micro B1-117 modprobe B1-84 mitmodump B1-117 https://dx.py B1-117 micro B1-117 https://dx.py B1-149 micro B1-150 https://dx.py B1-149 micro B1-150 https://dx.py B1-149 micro B1-150 https://dx.py B1-150		e e e e e e e e e e e e e e e e e e e
http.hijack.py	•	•
Iptables Bl		•
Name		
htrace	-	
modprobe		•
Description		
Ping6 B1-149 nmap B1-150 reade1f	-	
Packer P		
sysct1 BI-152, 154 NPK BI-23 veonfig BI-84 OSfuscate BI-65 xxd B4-66 PacketFence B1-65 AFL B3-165, L3259 panopticlick B1-68 amsi.fail B1-31 parasite6 B1-152 APIMonitor B2-104 pcaphistogram B2-24 arpspoof B1-117 PDFSharp B2-81 Bettercap B1-111 PEDA B4-98, 151 autopwn B1-115 POODLE B2-43 caplets B1-112 Probable Password List B1-23 sslstrip B1-168 ProcessMonitor B2-103 Bofuzz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chimera B1-30 pwnie express B1-75 chimera B1-33 Responder B1-75 chimera B1-125 pwntools B4-122 Coalfire NPK B1-23 Responder B1-07		
vconfig B1-84 OSfuscate B1-65 xxd B4-66 PacketFence B1-53 AFL B3-165, 13259 panopticlick B1-68 amsi fail B1-31 parasite6 B1-152 APIMonitor B2-104 peaphistogram B2-24 arpspoof B1-117 PDFSharp B2-81 Bettercap B1-111 PEDA B4-98, 151 autopwn B1-115 POODLE B2-43 caplets B1-112 Probable Password List B1-23 solvizz B3-145-7 PSAttack B2-213 solvizrip B1-168 ProcessMonitor B2-103 Boofuzz B3-145-7 PSAttack B2-27 Cain B1-55 pwn plug B1-75 chinera B1-30 pwntools B4-122 chiron B1-35 pwntools B4-122 chiron B1-35 pwntools B4-122 chiron B1-60 scapy B2-29, B1-67		
R4-66	•	
AFL B3-165, L3259 panopticlick B1-68 amsi.fall B1-31 parasite6 B1-152 APIMonitor B2-104 pcaphistogram B2-24 arpspoof B1-117 PDFSharp B2-81 Bettercap B1-111 PEDA B4-98, 151 autopwn B1-115 POODLE B2-43 caplets B1-115 POODLE B2-43 salstrip B1-68 ProcessMonitor B2-103 sslstrip B1-168 ProcessMonitor B2-103 sslstrip B1-55 pwn plug B1-75 chimera B1-30 pwnic express B1-75 chiiron B1-155 pwn plug B4-122 Coalfire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 Dr. Memory B2-105 SharpHook B2-114		
amsi.fail B1-31 parasite6 B1-152 APIMonitor B2-104 pcaphistogram B2-24 arpspoof B1-117 PDFSharp B2-24 Bettercap B1-111 PDFSharp B2-83 Bettercap B1-111 PEDA B4-98, 151 autopwn B1-155 PODDLE B2-93 salets B1-112 Probable Password List B1-23 salstrip B1-68 ProcessMonitor B2-103 Boofuzz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chinera B1-30 pwnie express B1-75 chinen B1-35 pwntools B4-122 Coalfire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpseam B1-60 scapy B2-92, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt-exe L1150 <td></td> <td></td>		
APIMonitor B2-04 arpspoof B1-117 PDFSharp B2-84 Bettercap B1-111 PEDA B4-98, 151 autopwn B1-115 POODLE B2-43 caplets B1-112 Probable Password List B1-23 sslstrip B1-168 ProcessMonitor B2-103 sslstrip B1-168 ProcessMonitor B2-103 softuz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chinera B1-30 pwnie express B1-75 chinen B1-155 pwntools B4-122 Coalfire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-99, B1-27 gescam B1-60 scapy B2-99, B1-27 b1-101 B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-157 Drov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 scoat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-13, B3-112, L3251 filters B1-98 Sulley B1-73, B3-112, L3251 filters B1-168 unicorn B2-13 filters B1-168 unicorn B2-14 Frewalker B2-13 UnmangedPowershell B2-74 Frewalker B2-13 UnmangedPowershell B2-93 H0-105 UnmangedPowershell B2-93 H0-105 Un	,	• •
Bettercap B1-117 PDFSharp B2-81		-
Bettercap B1-111 PEDA B4-98, 151 autopwn B1-115 POODLE B2-43 caplets B1-112 Probable Password List B1-23 sslstrip B1-68 ProcessMonitor B2-103 Boofuzz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chimera B1-30 pwnie express B1-75 chimera B1-35 pwn plug B1-75 chimera B1-30 pwnie express B1-75 chimera B1-30 pwnie express B1-75 chimera B1-32 Responder B1-122 Coalfire NPK B1-23 Responder B1-122 COMB B1-23 Responder B1-122 COMB B1-23 Responder B1-122 Coalfire NPK B1-23 Responder B1-122 Coalfire NPK B1-23 Responder B1-122 Coalfire NPK B1-23 Responder B1-122		
autopwn B1-115 POODLE B2-43 caplets B1-112 Probable Password List B1-23 sslstrip B1-168 ProcessMonitor B2-103 Boofuzz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chimera B1-30 pwnie express B1-75 chimera B1-155 pwn plug B1-75 chimera B1-155 pwn plug B1-75 chimera B1-160 pwnie express B1-75 chimera B1-163 pwnie express B1-75 chimera B1-163 pwnie express B1-75 chimera B1-162 scapy B2-122 chimera B1-123 Responder B1-122 cpscam B1-149 fuzzing B3-70-89, L3245 <td></td> <td>•</td>		•
caplets B1-112 Probable Password List B1-23 sslstrip B1-168 ProcessMonitor B2-103 Boofuzz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chimera B1-30 pwnie express B1-75 chiron B1-155 pwntools B4-122 Colafire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 slstrip B1-163-6 <td>•</td> <td>,</td>	•	,
sslstrip B1-168 ProcessMonitor B2-103 Boofuzz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chimera B1-30 pwnie express B1-75 chiron B1-155 pwntools B4-122 Coalfire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-49 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynapmoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-155 eapmdforuzies B2-117 SprayWMI B1-20 ent B2-27 slstrip B1-63-6 <td></td> <td></td>		
Boofuzz B3-145-7 PSAttack B2-72 Cain B1-55 pwn plug B1-75 chimera B1-30 pwnie express B1-75 chiron B1-155 pwntools B4-122 Coalfire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5ftzzies B1-73 socat B1-155 emi B2-88, L1171 SprayWMI B1-20 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-02 tcpick B2-27 <	•	
Cain B1-55 chimera pwn plug B1-75 chimera B1-75 chimera B1-30 pwnie express B1-75 chiron B1-155 pwntools B4-122 pwntools	-	
chimera B1-30 pwnie express B1-75 chiron B1-155 pwntools B4-122 Coalfire NPK B1-23 Responder B1-07 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-9, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt-exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Droov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-155 eapmdefuzzies B1-173 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-63-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27		
chiron B1-155 pwntools B4-122 Coalfire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-87 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-154 TinyInst <t< td=""><td></td><td></td></t<>		
Coalfire NPK B1-23 Responder B1-107 COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Droov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-157 eapmd5fuzzies B1-33 socat B1-157 Empire B2-8k, L1171 SprayWMI B1-20 ent B2-8x, L1171 SprayWMI B1-20 ettercap B1-98 Sulley B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-154 TinyInst		-
COMB B1-23 Ropper B4-122 cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-155 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-63-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-177 theC2Matrix B1-19 fingerbank B1-68 unicorn B2-74 Firewalker B2-113 UnmanagedPowershell		•
cpscam B1-60 scapy B2-29, B1-67 detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-155 empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-74 Firewalker B2-113 UnmanagedPowershell B2-72 GDB B4-32-5 User Agent S		•
detect-new-ip6 B1-149 fuzzing B3-70-89, L3245 DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-27 ent B2-88, L1171 SprayWMI B1-63-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-74 Firewalker B2-13 UnmanagedPowershell B2-72 GDB B4-32-5 <		
DLHell B2-112 Seatbelt.exe L1150 Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-155 empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-63-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-177 theC2Matrix B1-19 fake_router6 B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-74 Firewalker B2-13 UnmanagedPowershell B2-72 GDB B4-32-5 User Agent Sw	-	,
Dr. Memory B2-105 SharpHook B2-114 DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-02 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-154 theC2Matrix B1-19 fake_router6 B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-72 GDB B4-32-5 User Agent Switcher B1-63 hash_extender B2-38 voiphopper B1-63 howDump B2-113 Watson B2-90 hurricane electric B1-85 Winpeas	*	,
DynamoRIO B3-154, L3237 Shelter B1-27 Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-02 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-177 theC2Matrix B1-19 fake_router6 B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-72 GDB B4-32-5 User Agent Switcher B1-63 hash_extender B2-13 Watson B2-90 HookDump B2-13 Watson B2-90 hurricane electric B1-55 Winpeas L1163 ida sploiter B4-122 yersinia		
Drcov B3-155 Sherlock B2-90 Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-177 theC2Matrix B1-19 fake_router6 B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-74 Firewalker B2-113 UnmanagedPowershell B2-72 GDB B4-32-5 User Agent Switcher B1-63 hash_extender B2-58 voiphopper B1-90 HookDump B2-113 Watson B2-90 hurricane electric B1-155 Winpeas L1163 ida sploiter B4-122 yersin	·	
Dynapstalker B3-157, L3237 sixxs B1-155 eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-177 theC2Matrix B1-19 fake_router6 B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-74 Firewalker B2-113 UnmanagedPowershell B2-72 GDB B4-32-5 User Agent Switcher B1-63 hash_extender B2-58 voiphopper B1-90 HookDump B2-113 Watson B2-90 hurricane electric B1-155 Winpeas L1163 ida sploiter B4-122 yersinia B1-80-3, 127		
eapmd5fuzzies B1-73 socat B1-157 Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-177 theC2Matrix B1-19 fake_router6 B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-74 Firewalker B2-113 UnmanagedPowershell B2-72 GDB B4-32-5 User Agent Switcher B1-63 hash_extender B2-58 voiphopper B1-90 HookDump B2-113 Watson B2-90 hurricane electric B1-155 Winpeas L1163 ida sploiter B4-122 yersinia B1-80-3, 127		
Empire B2-88, L1171 SprayWMI B1-20 ent B2-27 sslstrip B1-163-6 ettercap B1-98 Sulley B1-73, B3-112, L3251 filters B1-102 tcpick B2-27 Event Tracing For Windows B2-103 Teredo B1-155 evilginx B1-177 theC2Matrix B1-19 fake_router6 B1-154 TinyInst B3-178 fingerbank B1-68 unicorn B2-74 Firewalker B2-113 UnmanagedPowershell B2-72 GDB B4-32-5 User Agent Switcher B1-63 hash_extender B2-58 voiphopper B1-90 HookDump B2-113 Watson B2-90 hurricane electric B1-155 Winpeas L1163 ida sploiter B4-122 yersinia B1-80-3, 127	· -	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		- v
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	-	· · · · · · · · · · · · · · · · · · ·
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		-
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	~	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
Firewalker .B2-113 UnmanagedPowershell .B2-72 GDB .B4-32-5 User Agent Switcher .B1-63 hash_extender .B2-58 voiphopper .B1-90 HookDump .B2-113 Watson .B2-90 hurricane electric .B1-155 Winpeas .L1163 ida sploiter .B4-122 yersinia .B1-80-3, 127		v
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	· ·	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		~
HookDump .B2-113 Watson .B2-90 hurricane electric .B1-155 Winpeas .L1163 ida sploiter .B4-122 yersinia .B1-80-3, 127		
hurricane electric		
ida sploiter		
ı .		
$\operatorname{ImageMagick}$ $\operatorname{B2-16}$	ImageMagick B2–16	•

Lischke 3 01/2025