

Index

access logs	504.1 – 72
ASEPs	504.W – 20
Berkeley Packet Filters	504.1 – 70
CIM	504.1 – 42
COMSPEC	504.1 – 55
containment	504.1 – 29
continuous recording	504.1 – 93
detection	504.1 – 26
differential analysis	504.W – 25-31, 504.1 – 57
encoding	504.1 – 45
eradication	504.1 – 30
event of interest	504.1 – 83
gold image	504.1 – 57
HKCU	504.W – 20
HKLM	504.W – 20
logs	
access	504.1 – 72
LSASS	504.1 – 42-3
malware analysis	
online	504.1 – 89
post-incident	504.1 – 33
prefetch files	504.1 – 95
preparation	504.1 – 25
proxies	
web	504.1 – 71
recovery	504.1 – 31
registry keys	504.W – 20
remediation	504.1 – 32
scoping	504.1 – 28
snapshot	504.1 – 93
static analysis	504.1 – 88
web proxies	504.1 – 71
Windows Event Log	504.1 – 55
WMI	504.1 – 42

SEC504– Hacker Tools, Techniques, and Incident Handling

Commands

Linux

sha256sum	504.1 – 91
strings	504.1 – 91
tcpdump	504.1 – 68-9

Windows

Export-ScheduledTask	504.1 – 54
Format-List	504.1 – 50
Get-ChildItem	504.1 – 51
Get-CimInstance	504.1 – 40
Get-FileHash	504.1 – 91
Get-ItemProperty	504.1 – 51
Get-LocalGroupMember	504.1 – 53
Get-LocalGroup	504.1 – 53
Get-LocalUser	504.1 – 53
Get-NetTCPConnection	504.1 – 46
Get-Process	504.W – 14-6, 504.1 – 40
Get-ScheduledTaskInfo	504.1 – 54
Get-ScheduledTask	504.1 – 54
Get-Service	504.1 – 50
Get-WinEvent	504.1 – 55
Remove-ItemProperty	504.W – 23, 24
Select-Object	504.W – 15-7, 504.1 – 40
Stop-Process	504.1 – 40
Where-Object	504.W – 15-7, 504.1 – 53

Modules

Incident Response

DAIR Dynamic Approach	504.1 – 25-34
PICERL Six-Step Process	504.1 – 21-2
summary of	504.1 – 35-6

Live Examination

lab	L1.1
of accounts	504.1 – 53
of encoded data	504.1 – 45
of logs	504.1 – 55
of network activity	504.1 – 46-9
of processes	504.1 – 40-5

of registry keys	504.1 – 51-2
of scheduled tasks	504.1 – 54
of services	504.1 – 50
summary of	504.1 – 62

Malware Examination

lab	L1.4
-----------	------

Malware Investigations

monitoring the environment	504.1 – 92
----------------------------------	------------

Memory Examination

lab	L1.3
-----------	------

Memory Investigations

summary of	504.1 – 99
------------------	------------

Network Examination

lab	L1.2
-----------	------

Network Investigations

summary of	504.1 – 73
------------------	------------

Tools

Blue Coat	504.1 – 71
CyberChef	504.1 – 45
Forefront TMG	504.1 – 71
Ghidra	504.1 – 98
Hybrid Analysis	504.1 – 89
IDA Pro	504.1 – 98
Powershell	504.1 – 39
Regshot	504.1 – 94-5
Squid	504.1 – 71
Sysinternals	504.1 – 61
Autoruns	504.1 – 61
Procdump	504.1 – 61
Process Explorer	504.1 – 61
Process Monitor	504.1 – 61, 504.1 – 96-7
Sysmon	504.1 – 61
TCPView	504.1 – 61
VirusTotal	504.1 – 89
Volatility	504.1 – 77-82
WinPmem	504.1 – 77-82