

508.1 - Advanced Incident Response and Threat Hunting

Incident Response and Threat Hunting 19-34

Incident Response.....	20-30
Six-step process.....	20-21
Eradicating too fast.....	22-23
Containment and intel development.....	24-25
Detection and intel loop.....	26
Remediation	27-30
Remediation events.....	28
Critical remediation events.....	29
Real-time remediation.....	30
Organization maturity.....	30
Threat hunting.....	31-34
Reactive response vs. Threat hunting.....	31
Threat hunting process.....	32-34
Team roles.....	32-34
What to look for.....	32-34

Threat Intel..... 36-51

Attack lifecycle	37-38
Kill Chain.....	39-43
Indicator types (atomic, behavioral, computed).....	39
Adversary behavior/Attribution	40
Mitre ATT&CK	44-48
IOCs	49-51
Host-based & Network-based.....	49
Tools & languages.....	50
YARA.....	51

Malware-ology..... 54-66

Malware paradox.....	54
Types of compromise.....	56
'Analysis funnel'.....	57-58
Detecting endpoints without active malware	59
Hiding in plain sight.....	60
Living off the land (LOLBins)	61

LOLBAS project.....	61
Common defense evasion.....	62
Code signing.....	63-66
Overview.....	63-64
Signed vs. unsigned malware	65-66

Malware persistence 69-87

Malware persistence options	69
Autostart locations (ASEPs).....	70-71
Windows services	72-73
Scheduled tasks.....	74-75
DLL Hijacking attacks	76-78
Search order hijacking.....	76
Phantom DLL hijacking.....	77
DLL side-loading (SxS).....	77
Relative path DLL hijacking.....	77
Hunting notes	78
WMI backdoors	79-84
Filter/consumer/binding	79-80
Managed Object Format (MOF).....	79-80
Finding suspicious WMI.....	81
Scaling collection	82
Hunting notes	83-84
autorunsc.exe	85-87
Overview.....	85
Usage.....	86-87

IR: Hunting across network 92-110

IR scripting evolution.....	92
Hunting with WMIC.....	93
Powershell.....	94-99
Capabilities	94
Basics.....	95-96
Remoting	97-98
Authentication.....	99
Kerberos vs. CredSSP.....	99

Kansa – Powershell IR Framework	100-110	Kerberos attacks.....	143-144
Overview.....	100-101	Pass/Overpass the ticket	143-144
Modules.....	102	Kerberoasting.....	143-144
Usage	104-110	Golden ticket.....	143-144
Kansa with other tools.....	106	Silver ticket	143-144
Analysis scripts.....	107-108	Skeleton key.....	143-144
Fire & forget modules	110	DCSync	143-144
Credential Theft.....	114-149	Defending tickets.....	145-146
Lateral movement overview	114	Kerberos attack mitigations	147
Credential theft overview	115-116	NTDS.DIT	148-149
Credential attack mitigation	117-118	Overview.....	148
Windows 7/Vista	117	Bloodhound.....	149
Windows 8.1.....	117		
Windows 10.....	118		
Credential guard / Remote credential guard.....	118		
Device guard.....	118		
Password hashes	119-127		
Overview.....	119		
Pass-the-hash attacks.....	119-120		
Credential availability.....	121		
Hash dump example.....	122		
Pass-the-hash example (Mimikatz).....	124		
Defending hashes	126-127		
Tokens	128-132		
Overview.....	128		
Token stealing	128		
Token stealing example (Mimikatz)	129		
Defending tokens	131		
Cached credentials	133-136		
Overview.....	133		
Mscash2 hashes.....	133		
Extracting cached credentials (credump)	134		
Defending cached credentials.....	136		
LSA secrets	137-139		
Decrypting LSA secrets (Nishang).....	138		
Defending LSA secrets	139		
Tickets	140-147		
Pass-the-ticket example	141		