508.1 - Advanced Incident Response and Threat Hunting

[Incident Response and Threat Hunting](#_Toc122964506) 19-34

[Incident Response](#_Toc122964507) 20-30

[Six-step process](#_Toc122964508) 20-21

[Eradicating too fast](#_Toc122964509) 22-23

[Containment and intel development](#_Toc122964510) 24-25

[Detection and intel loop](#_Toc122964511) 26

[Remediation](#_Toc122964512) 27-30

[Remediation events](#_Toc122964513) 28

[Critical remediation events](#_Toc122964514) 29

[Real-time remediation](#_Toc122964515) 30

[Organization maturity](#_Toc122964516) 30

[Threat hunting](#_Toc122964517) 31-34

[Reactive response vs. Threat hunting](#_Toc122964518) 31

[Threat hunting process](#_Toc122964519) 32-34

[Team roles](#_Toc122964520) 32-34

[What to look for](#_Toc122964521) 32-34

[Threat Intel](#_Toc122964522) 36-51

[Attack lifecycle](#_Toc122964523) 37-38

[Kill Chain](#_Toc122964524) 39-43

[Indicator types (atomic, behavioral, computed)](#_Toc122964525) 39

[Adversary behavior/Attribution](#_Toc122964526) 40

[Mitre ATT&CK](#_Toc122964527) 44-48

[IOCs](#_Toc122964528) 49-51

[Host-based & Network-based](#_Toc122964529) 49

[Tools & languages](#_Toc122964530) 50

[YARA](#_Toc122964531) 51

[Malware-ology](#_Toc122964532) 54-66

[Malware paradox](#_Toc122964533) 54

[Types of compromise](#_Toc122964534) 56

[‘Analysis funnel’](#_Toc122964535) 57-58

[Detecting endpoints without active malware](#_Toc122964536) 59

[Hiding in plain sight](#_Toc122964537) 60

[Living off the land (LOLBins)](#_Toc122964538) 61

[LOLBAS project](#_Toc122964539) 61

[Common defense evasion](#_Toc122964540) 62

[Code signing](#_Toc122964541) 63-66

[Overview](#_Toc122964542) 63-64

[Signed vs. unsigned malware](#_Toc122964543) 65-66

[Malware persistence](#_Toc122964544) 69-87

[Malware persistence options](#_Toc122964545) 69

[Autostart locations (ASEPs)](#_Toc122964546) 70-71

[Windows services](#_Toc122964547) 72-73

[Scheduled tasks](#_Toc122964548) 74-75

[DLL Hijacking attacks](#_Toc122964549) 76-78

[Search order hijacking](#_Toc122964550) 76

[Phantom DLL hijacking](#_Toc122964551) 77

[DLL side-loading (SxS)](#_Toc122964552) 77

[Relative path DLL hijacking](#_Toc122964553) 77

[Hunting notes](#_Toc122964554) 78

[WMI backdoors](#_Toc122964555) 79-84

[Filter/consumer/binding](#_Toc122964556) 79-80

[Managed Object Format (MOF)](#_Toc122964557) 79-80

[Finding suspicious WMI](#_Toc122964558) 81

[Scaling collection](#_Toc122964559) 82

[Hunting notes](#_Toc122964560) 83-84

[autorunsc.exe](#_Toc122965734) 85-87

[Overview](#_Toc122965735) 85

[Usage](#_Toc122965736) 86-87

[IR: Hunting across network](#_Toc122965737) 92-110

[IR scripting evolution](#_Toc122965738) 92

[Hunting with WMIC](#_Toc122965739) 93

[Powershell](#_Toc122965740) 94-99

[Capabilities](#_Toc122965741) 94

[Basics](#_Toc122965742) 95-96

[Remoting](#_Toc122965743) 97-98

[Authentication](#_Toc122965744) 99

[Kerberos vs. CredSSP](#_Toc122965745) 99

[Kansa – Powershell IR Framework](#_Toc122965746) 100-110

[Overview](#_Toc122965747) 100-101

[Modules](#_Toc122965748) 102

[Usage](#_Toc122965749) 104-110

[Kansa with other tools](#_Toc122965750) 106

[Analysis scripts](#_Toc122965751) 107-108

[Fire & forget modules](#_Toc122965752) 110

[Credential Theft](#_Toc122965753) 114-149

[Lateral movement overview](#_Toc122965754) 114

[Credential theft overview](#_Toc122965755) 115-116

[Credential attack mitigation](#_Toc122965756) 117-118

[Windows 7/Vista](#_Toc122965757) 117

[Windows 8.1](#_Toc122965758) 117

[Windows 10](#_Toc122965759) 118

[Credential guard / Remote credential guard](#_Toc122965760) 118

[Device guard](#_Toc122965761) 118

[Password hashes](#_Toc122965762) 119-127

[Overview](#_Toc122965763) 119

[Pass-the-hash attacks](#_Toc122965764) 119-120

[Credential availability](#_Toc122965765) 121

[Hash dump example](#_Toc122965766) 122

[Pass-the-hash example (Mimikatz)](#_Toc122965767) 124

[Defending hashes](#_Toc122965768) 126-127

[Tokens](#_Toc122965769) 128-132

[Overview](#_Toc122965770) 128

[Token stealing](#_Toc122965771) 128

[Token stealing example (Mimikatz)](#_Toc122965772) 129

[Defending tokens](#_Toc122965773) 131

[Cached credentials](#_Toc122965774) 133-136

[Overview](#_Toc122965775) 133

[Mscash2 hashes](#_Toc122965776) 133

[Extracting cached credentials (creddump)](#_Toc122965777) 134

[Defending cached credentials](#_Toc122965778) 136

[LSA secrets](#_Toc122965779) 137-139

[Decrypting LSA secrets (Nishang)](#_Toc122965780) 138

[Defending LSA secrets](#_Toc122965781) 139

[Tickets](#_Toc122965782) 140-147

[Pass-the-ticket example](#_Toc122965783) 141

[Kerberos attacks](#_Toc122965784) 143-144

[Pass/Overpass the ticket](#_Toc122965785) 143-144

[Kerberoasting](#_Toc122965786) 143-144

[Golden ticket](#_Toc122965787) 143-144

[Silver ticket](#_Toc122965788) 143-144

[Skeleton key](#_Toc122965789) 143-144

[DCSync](#_Toc122965790) 143-144

[Defending tickets](#_Toc122965791) 145-146

[Kerberos attack mitigations](#_Toc122965792) 147

[NTDS.DIT](#_Toc122965793) 148-149

[Overview](#_Toc122965794) 148

[Bloodhound](#_Toc122965795) 149

# Incident Response and Threat Hunting

## Incident Response

### Six-step process

### Eradicating too fast

### Containment and intel development

### Detection and intel loop

### Remediation

#### Remediation events

#### Critical remediation events

#### Real-time remediation

#### Organization maturity

## Threat hunting

### Reactive response vs. Threat hunting

### Threat hunting process

#### Team roles

#### What to look for

# Threat Intel

## Attack lifecycle

## Kill Chain

### Indicator types (atomic, behavioral, computed)

### Adversary behavior/Attribution

## Mitre ATT&CK

## IOCs

### Host-based & Network-based

### Tools & languages

### YARA

# Malware-ology

## Malware paradox

## Types of compromise

## ‘Analysis funnel’

## Detecting endpoints without active malware

## Hiding in plain sight

## Living off the land (LOLBins)

### LOLBAS project

## Common defense evasion

## Code signing

### Overview

### Signed vs. unsigned malware

# Malware persistence

## Malware persistence options

## Autostart locations (ASEPs)

## Windows services

## Scheduled tasks

## DLL Hijacking attacks

### Search order hijacking

### Phantom DLL hijacking

### DLL side-loading (SxS)

### Relative path DLL hijacking

### Hunting notes

## WMI backdoors

### Filter/consumer/binding

### Managed Object Format (MOF)

### Finding suspicious WMI

### Scaling collection

### Hunting notes

## ‘autorunsc.exe’ – Detecting malware persistence

### Overview

### Usage

# IR: Hunting across network

## IR scripting evolution

## Hunting with WMIC

## Powershell

### Capabilities

### Basics

### Remoting

### Authentication

#### Kerberos vs. CredSSP

## Kansa – Powershell IR Framework

### Overview

### Modules

### Usage

#### Kansa with other tools

#### Analysis scripts

#### Fire & forget modules

# Credential Theft

## Lateral movement overview

## Credential theft overview

## Credential attack mitigation

### Windows 7/Vista

### Windows 8.1

### Windows 10

#### Credential guard / Remote credential guard

#### Device guard

## Password hashes

### Overview

### Pass-the-hash attacks

### Credential availability

### Hash dump example

### Pass-the-hash example (Mimikatz)

### Defending hashes

## Tokens

### Overview

### Token stealing

### Token stealing example (Mimikatz)

### Defending tokens

## Cached credentials

### Overview

### Mscash2 hashes

### Extracting cached credentials (creddump)

### Defending cached credentials

## LSA secrets

### Decrypting LSA secrets (Nishang)

### Defending LSA secrets

## Tickets

### Pass-the-ticket example

### Kerberos attacks

#### Pass/Overpass the ticket

#### Kerberoasting

#### Golden ticket

#### Silver ticket

#### Skeleton key

#### DCSync

### Defending tickets

### Kerberos attack mitigations

## NTDS.DIT

### Overview

### Bloodhound