# Dd

**Domain Domination** *[b5/****p28****]* - Domain Domination and AD Persistence

**Domain Domination** *[b5/****p29****]* - Obtaining Access to Back-Up NTDS.dit File

**Domain Domination** *[b5/****p31****]* - Creating a Domain Admin Account

**Domain Domination** *[b5/****p32****]* – Skeleton Key

**Domain Domination** *[b5/****p33****]* – Skeleton Key in Action

**Domain Domination** *[b5/****p34****]* – Replicating the Domain: DCSync

**Domain Domination** *[b5/****p35****]* – Replicating the Domain: DCSync Example

**Domain Domination** *[b5/****p36****]* – Becoming a Domain Controller: DCShadow

**Domain Domination** *[b5/****p37****]* – Becoming a Domain Controller: DCShadow in Action

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Domain PrivEsc** *[b5/****p59****]* - PowerView Find-InterestingDomainShareFile

**Domain PrivEsc** *[b5/****p60****]* - PowerView Find-LocalAdminAccess

**Domain PrivEsc** *[b5/****p61, p62****]* - Privilege Escalation

# Gg

**Golden Ticket** *[b5/****p52****]*

**Golden Ticket** *[b5/****p53****]* - Kerberos Flow with Golden Ticket

**Golden Ticket** *[b5/****p54****] -* Golden Ticket Properties

**Golden Ticket** *[b5/****p55****] -* Golden Ticket Tools

# Kk

**Kerberos** *[b5/****p5, p12, p53, p54****]*

**Kerberos** *[b5/****p6****]* - How it works

**Kerberos** *[b5/****p7****]* - Pre-Authentication and TGT

**Kerberos** *[b5/****p8, p9****]* - Authenticating to a Service

**Kerberos** *[b5/****p10****]* - Overall Flow

**Kerberos** *[b5/****p11****]* - AS-REQ with Pre-Authentication and AS-REP

**Kerberos** *[b5/****p12****]* - TGT (Ticket Granting Ticket) and PAC

**Kerberos** *[b5/****p13****]* - Requesting a Service Ticket (ST)

**Kerberos** *[b5/****p14****]* - Service Principal Name

**Kerberos** *[b5/****p15****]* - Using a Service Ticket (ST)

**Kerberos** *[b5/****p16****]* - Service Ticket

**Kerberos** *[b5/****p17****]* - Kerberos: Three Long-Term Keys

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Kerberoast** *[b5/****p19****]* - Requesting a Service Ticket (ST) Revisited

**Kerberoast** *[b5/****p20****]* - Requesting a Ticket

**Kerberoast** *[b5/****p21****]* - Kerberos Attack

**Kerberoast** *[b5/****p22****]* - Obtaining Tickets

**Kerberoast** *[b5/****p23****]* - Kerberoast Attack Steps

**Kerberoast** *[b5/****p24****]* - What Service Accounts are Good Targets?

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**More Kerberos Attacks** *[b5/****p41****] –* Pass-the-Ticket

**More Kerberos Attacks** *[b5/****p42****] –* Pass-the-Ticket: Mimikatz Example

**More Kerberos Attacks** *[b5/****p43****] –* Overpass-the-Hash

**More Kerberos Attacks** *[b5/****p44****] –* Golden Ticket Overview

# Ss

**Silver Ticket** *[b5/****p46****]*

**Silver Ticket** *[b5/****p47****]* - Generating a Silver Ticket with Impacket Silver Ticket

**Silver Ticket** *[b5/****p48****]* - Silver Ticket Use

# 

**AD replication** *[b5/****p34****]*

**AES** *[b5/****p43,******p52****]*

**AGPMServer** *[b5/****p24****]*

**AS-REP** *[b5/****p10, p11, p17, p19, p43, p53****]*

**AS-REP Roasting** *[b5/****p62****]*

**AS-REQ** *[b5/****p10, p11, p15, p17, p19, p32, p43, p53****]*

**Authentication Server (AS)** *[b5/****p7****,* ***p10, p11, p15****]*

**brute force attacks** *[b5/****p23****]*

**Client long-term secret key** *[b5/****p17****]*

**Comsvcs.dll** *[b5/****p61****]*

**DCSync** *[b5/****p28, p34, p35, p36****]*

**DCSync attack** *[b5/****p34****]*

**DCShadow** *[b5/****p28, p36, p37****]*

**Directory Replication Service Remote (DRSR)** *[b5/****p35, p36****]*

**Domain Admin** *[b5/****p31, p34****]*

**Domain Administrator** *[b5/****p44****]* – RID 512

**Domain Controller** *[b5/****p34, p36****]*

**Domain replication protocol** *[b5/****p34****]*

**Domain SID** *[b5/****p55****]* – (S-1-5-21-XXX…….)

**empire** *[b5/****p22****]*

**FIMService** *[b5/****p24****]*

**FQDN (fully qualified domain name)** *[b5/****p14****]*

**GetUserSPNs.py** *[b5/****p22****]*

**Golden Ticket** *[b5/****p28, p34, p35, p44, p52, p53, p54, p55****]*

**hashcat** *[b5/****p22****]*

**impacket** *[b5/****p22, p29, p47, p48, p62****]*

**Install from Media (IFM)** *[b5/****p29, p30****]*

**Invoke-Kerberoast** *[b5/****p22****]*

**jtr (john the ripper)** *[b5/****p22****]*

**KDC LT key (krbtgt NT hash)** *[b5/****p12, p46, p52****]*

**KDC long-term secret key** *[b5/****p17****]*

**Kerberoasting** *[b5/****p16, p62****]*

**Kerberos server** *[b5/****p5****]*

**Key Distribution Center (KDC)** *[b5/****p7, p8, p11, p17, p19, p20, p46****]*

**krbtgt** *[b5/****p11, p15, p17****]*

**krbtgt hash** *[b5/****p35, p44, p46, p52, p54, p55****]*

**krbtgt NT hash (KDC LT key)** *[b5/****p12****]*

**KRB5CCNAME** *[b5/****p48****]*

**lsadump** *[b5/****p35, p37****]*

**lsass.exe** *[b5/****p561****]*

**mimikatz** *[b5/****p22, p32, p33, p34, p35, p36, p37, p41, p42, p48, p55****]*

**MS-DRSR** *[b5/****p36****]*

**MSSQL/MSSQLSvc** *[b5/****p24****]*

**NT hash** *[b5/****p52****]*

**NTDS.dit** *[b5/****p28, p29, p34****]*

**ntdsutil.exe** *[b5/****p29****]*

**Overpass-the-Hash** *[b5/****p43****]*

**PAC (rivilege Attribute Certificate)** *[b5/****p8, p9, p12, p17, p44, p46, p52****]*

**PAC Validation** *[b5/****p46****] [****Old b5/p12, p17****]*

**Pass-the-Hash attack (PtH)** *[b5/****p43****]*

**pass-the-ticket (ptt)** *[b5/****p48****]*

**PowerSploit** *[b5/****p22****]*

**PowerSploit Out-MiniDump** *[b5/****p61****]*

**PowerView** *[b5/****p59, p60****]*

**Privilege Attribute Certificate (PAC)** *[b5/****p8, p9, p12, p17, p44, p46, p52****]*

**Procdump** *[b5/****p61****]*

**Process Explorer** *[b5/****p61****]*

**PsExec** *[b5/****p42****]*

**RC4 encryption** *[b5/****p32, p52****]*

**RC4\_HMAC\_MD5** *[b5/****p21,******p43****]*

**RC4 service tickets** *[b5/****p23****]*

**registry** *[b5/****p29, p30****]*

**Responder style attacks** *[b5/****p62****]*

**RID 512** *[b5/****p44****] -* Domain Administrator

**Rubeus** *[b5/****p41, p48, p62****]*

**RunDLL32** *[b5/****p61****]*

**secretsdump.py** *[b5/****p29****]*

**Security Token Service (STS)** *[b5/****p24****]*

**Service Principal Name (SPN)** *[b5/****p12, p14, p20, p21, p22, p23, p62****]*

**setspn.exe** *[b5/****p14****]*

**Service Ticket (ST)** *[b5/****p10, p13, p15, p16, p19, p21, p23, p41, p46, p53****]*

**Silver Ticket** *[b5/****p46,******p47, p48****]*

**Skeleton Key** *[b5/****p28, p32, p33****]*

**Skeleton Key Attack** *[b5/****p32****]*

**SMBClient** *[b5/****p62****]*

**Sysinternals** *[b5/****p42, p61****]*

**System Key** *[b5/****p29****]*

**SYSTEM registry hive** *[b5/****p29, p30****]*

**Target LT Key** *[b5/****p12, p52****]*

**Target long-term secret key** *[b5/****p17, p19****]*

**Task Manager** *[b5/****p61****]*

**TGS-REP** *[b5/****p10, p13, p17, p19, p53****]*

**TGS-REQ** *[b5/****p10, p12, p13, p19, p53****]*

**Ticket Granting Service (TGS)** *[b5/****p10, p11, p15****]*

**Ticket Granting Ticket (TGT)** *[b5/****p7, p8, p10, p11, p12, p15, p19, p41, p43, p44, p52, p54****]*

**ticketer.py** *[b5/****p47, p55****]*

**Volume Shadow Copy Service** *[b5/****p29****]*

**wmiexec.py** *[b5/****p48****]*