



ERNW  
**SECTOOLS**  
building on knowledge.

## How to efficiently assess Active Directories of Any Scale with Directory Ranger, BloodHound and CypherDog

JD & Michael Thumann

1

ERNW  
**SECTOOLS**  
building on knowledge.

### #whoami

Security Consultant & Windows Automation Engineer

Contact:

ERNW GmbH

JD

Carl-Bosch-Str. 4

69115 Heidelberg





## #whoami

Lead Architect @ERNW SecTools

Contact:

ERNW SecTools GmbH

Michael Thumann

Carl-Bosch-Str. 4

69115 Heidelberg

Email: [mthumann@ernw.de](mailto:mthumann@ernw.de)



## Introduction



## Microsoft Active Directory

- A directory service
- Introduced with Windows 2000 Server in 2000 ☺
- Authenticates and authorizes all users and computers
- A kind of database that contains
  - Users
  - Groups
  - Computers
  - Services
  - Corresponding attributes
- **The key to the crown jewels of a corporate network**



## Worst case Hack

- A complete compromise of your directory service
- Consequences:
  - The attacker can impersonate **every** user
  - The attacker can access **every** server/system/resource integrated into the directory service
  - The attacker can access/modify **any** unencrypted data stored in that environment
  - The attacker can even access/modify encrypted data in that environment, if Microsoft's Data Protection API (DPAPI) is used





## What is required

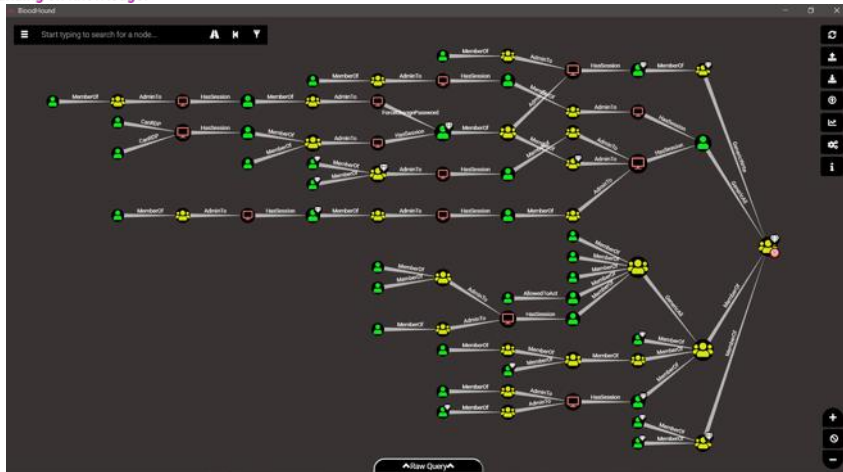
- An initial attack vector like
  - Executed email attachment
  - Drive-by-download from malicious website
  - Exploited vulnerability
- Access to a client/workstation
- Hijacking the user of the client
- Elevated privileges e.g. local admin
- A path to domain admin privileges
- Vulnerabilities/Misconfiguration



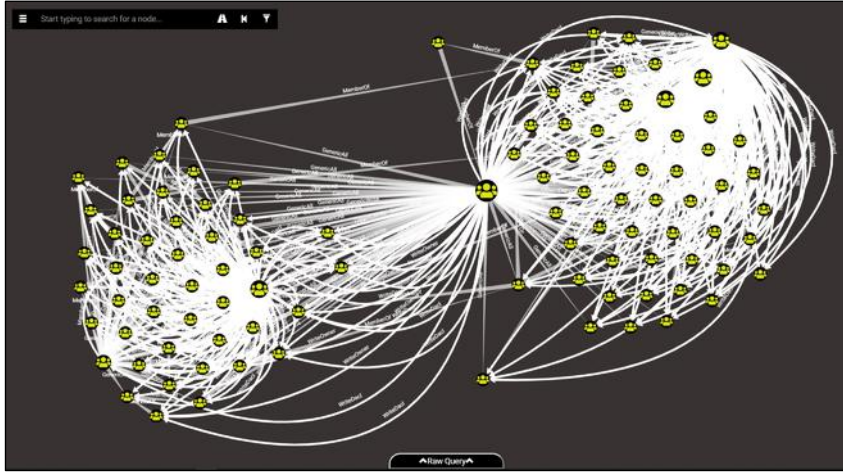
## Bloodhound – Path to Domain Admin



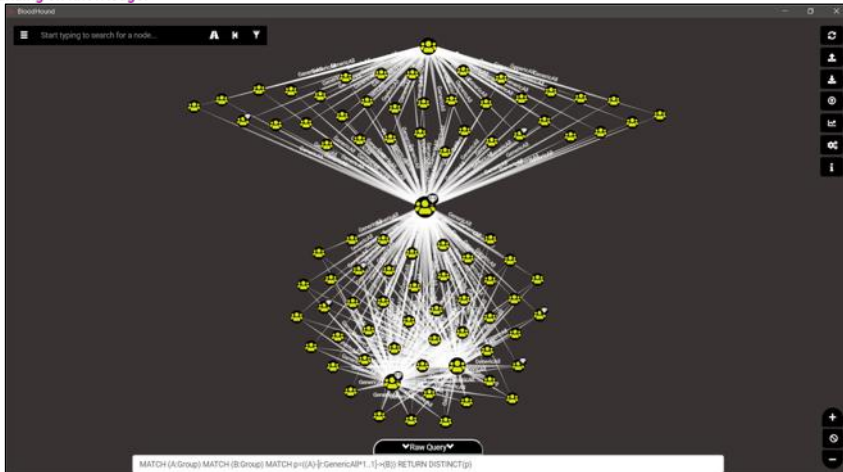
# An Active Directory Attack Paths Graphing tool



ERNW  
**SECTOOLS**  
building on knowledge.



ERNW  
**SECTOOLS**  
building on knowledge.





# BloodHound

## Why?

---



## Attackers think in Graphs, Defenders think in lists...

[John Lambert - MS Threat Intel]





# BloodHound

## By who?

---



@Harmj0y  
@\_Wald0  
@CptJesus



---

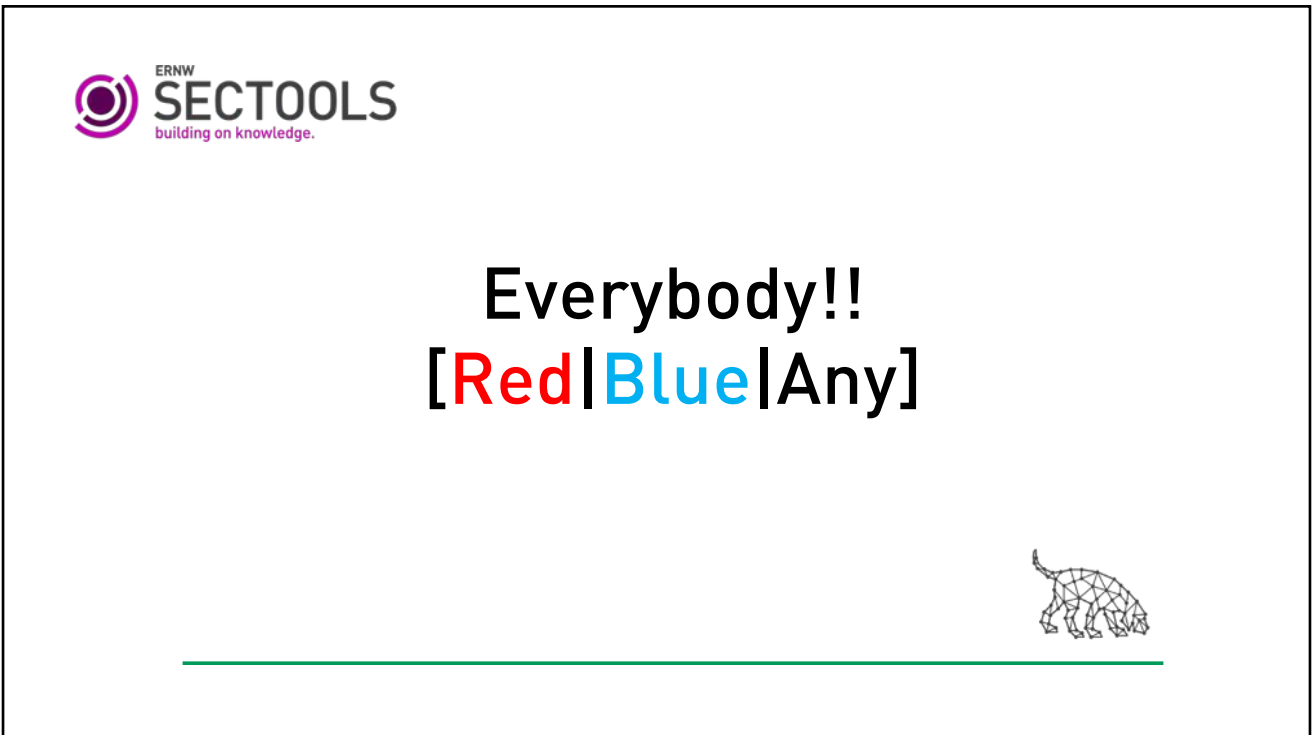




# BloodHound

## For who?

---



Everybody!!  
[Red|Blue|Any]

---





# BloodHound

## When?

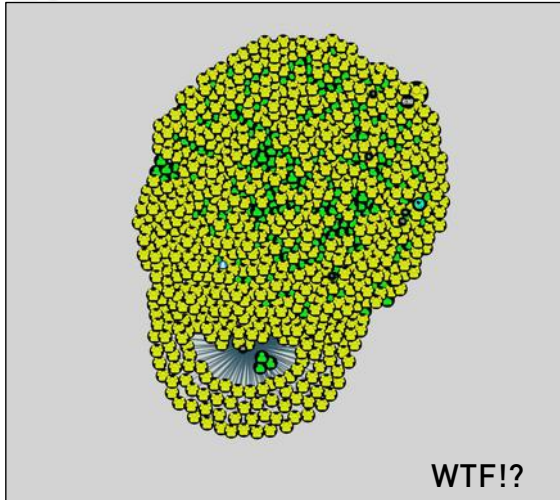
---



**Do not run BloodHound in your environment if your AD security isn't "mature" yet...  
[unless if you like pain]**

---





# BloodHound

## How?





- Data Collection with **Sharphound**
- Stored in **Neo4j** Database
- Displayed in **Web UI**



**Cypher**

**What?**





# Cypher is the Neo4j DB query language



```
MATCH (x) RETURN x  
// Return All Nodes
```






```
MATCH (x:User) RETURN x
// Return All User Nodes
```



```
MATCH (x:User {name: 'Bob'})
MATCH (y:Group
{name: 'GROUPX@ERNW.LAB'})
MATCH p=shortestPath((x)-[*1..]->(y))
RETURN p
// Return shortest Path from Bob to GroupX
```







ERNW  
**SECTOOLS**  
building on knowledge.

# CypherDog

# Wow!




---

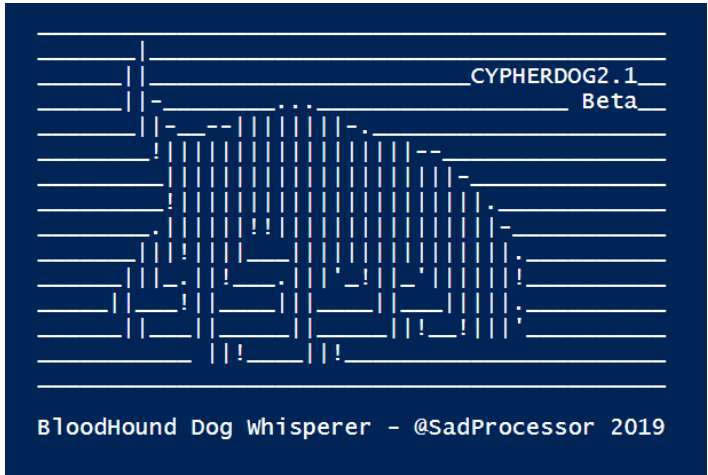


ERNW  
**SECTOOLS**  
building on knowledge.

## A PoSh Client for Bloodhound [Become a Dog Whisperer]



---



Cmdlet	Synopsis	Alias	RTFM
Get-BloodHoundCmdlet	BloodHound RTFM - Get Cmdlet	BloodHound	Help BloodHound
Send-BloodHoundPost	BloodHound POST - Cypher to REST API	DogPost	Help DogPost
Get-BloodHoundNode	BloodHound Node - Get Node	Node	Help Node
Search-BloodHoundNode	BloodHound Node - Search Node	NodeSearch	Help NodeSearch
New-BloodHoundNode	BloodHound Node - Create Node	NodeCreate	Help NodeCreate
Set-BloodHoundNode	BloodHound Node - Update Node	NodeUpdate	Help NodeUpdate
Remove-BloodHoundNode	BloodHound Node - Delete Node	NodeDelete	Help NodeDelete
Get-BloodHoundNodeList	BloodHound Node - Get List	List	Help List
Get-BloodHoundNodeHighValue	BloodHound Node - Get HighValue	HighValue	Help HighValue
Get-BloodHoundNodeOwned	BloodHound Node - Get Owned	Owned	Help Owned
Get-BloodHoundNodeNote	BloodHound Node - Get Notes	Note	Help Note
Set-BloodHoundNodeNote	BloodHound Node - Set Notes	NoteUpdate	Help NoteUpdate
Get-BloodHoundBlacklist	BloodHound Node - Get Blacklist	Blacklist	Help Blacklist
Set-BloodHoundBlacklist	BloodHound Node - Set Blacklist	BlacklistAdd	Help BlacklistAdd
Remove-BloodHoundBlacklist	BloodHound Node - Remove Blacklist	BlacklistDelete	Help BlacklistDelete
Get-BloodHoundEdge	BloodHound Edge - Get Target	Edge	Help Edge
Get-BloodHoundEdgeReverse	BloodHound Edge - Get Source	EdgeR	Help EdgeR
Get-BloodHoundEdgeCrossDomain	BloodHound Edge - Get CrossDomain	CrossDomain	Help CrossDomain
Get-BloodHoundEdgeCount	BloodHound Edge - Get Count	EdgeCount	Help EdgeCount
Get-BloodHoundEdgeInfo	BloodHound Edge - Get Info	EdgeInfo	Help EdgeInfo
New-BloodHoundEdge	BloodHound Edge - Create Edge	EdgeCreate	Help EdgeCreate
Remove-BloodHoundEdge	BloodHound Edge - Delete Edge	EdgeDelete	Help EdgeDelete
Get-BloodHoundPathShort	BloodHound Path - Get Shortest	Path	Help Path
Get-BloodHoundPathAny	BloodHound Path - Get Any	PathAny	Help PathAny
Get-BloodHoundPathCost	BloodHound Path - Get Cost	PathCost	Help PathCost
Get-BloodHoundPathCheap	BloodHound Path - Get Cheapest	PathCheap	Help PathCheap
Get-BloodHoundWald0IO	BloodHound Path - wald0 Index	Wald0IO	Help wald0IO





```

PS @:\>
PS @:\> node user GARY_CATANIA@SUB.DOMAIN.LOCAL

highvalue           : True
sensitive           : False
enabled             : True
hasspn              : False
owned               : False
displayname         : GARY_CATANIA
pwdlastset          : 1469700023
domain              : SUB.DOMAIN.LOCAL
name                : GARY_CATANIA@SUB.DOMAIN.LOCAL
lastlogon           : 1469700023
objectsid           : S-1-5-21-2505991005-2303352498-2358670217-2123
admincount          : False
serviceprincipalnames : {}

```



```

PS @:\> what user MemberOf Group 'SCHEMA_ADMINS@DOMAIN.LOCAL' -Degree * | select name,objectsid

name                objectsid
----                -
ADMINISTRATOR@DOMAIN.LOCAL S-1-5-21-2935009051-1024133711-517063756-500
ADMINISTRATOR@SUB.DOMAIN.LOCAL S-1-5-21-2505991005-2303352498-2358670217-500
ANNALEE_GARIBALDI@DOMAIN.LOCAL S-1-5-21-2935009051-1024133711-517063756-2648
DANILLE_FELL@SUB.DOMAIN.LOCAL S-1-5-21-2505991005-2303352498-2358670217-1634
EDELMIRA_LACY@DOMAIN.LOCAL S-1-5-21-2935009051-1024133711-517063756-2649
GARY_CATANIA@SUB.DOMAIN.LOCAL S-1-5-21-2505991005-2303352498-2358670217-2123
SANJUANA_DUSSAULT@SUB.DOMAIN.LOCAL S-1-5-21-2505991005-2303352498-2358670217-2125

```





```
PS @:\> list AdminBy GARY_CATANIA@SUB.DOMAIN.LOCAL | ft
```

highvalue	owned	pwdlastset	domain	lastlogon	name	operatingsystem
False	False	1535047674	DOMAIN.LOCAL	1536763480	DC_1.DOMAIN.LOCAL	Windows Server 2016 Standard Evaluation
False	False	146832084	SUB.DOMAIN.LOCAL	1469177131	DC_1.SUB.DOMAIN.LOCAL	Windows Server 2012 R2 Standard Evaluation
False	False	1535225427	DOMAIN.LOCAL	1536762108	DC_2.DOMAIN.LOCAL	Windows Server 2012 R2 Standard Evaluation
False	False	1535150285	SUB.DOMAIN.LOCAL	1536763425	DC_2.SUB.DOMAIN.LOCAL	Windows Server 2012 R2 Standard Evaluation
False	False	1534331977	DOMAIN.LOCAL	1534771359	DC_3.DOMAIN.LOCAL	Windows Server 2016 Standard Evaluation
False	False	1534752697	SUB.DOMAIN.LOCAL	1534752701	SRV_1.SUB.DOMAIN.LOCAL	Windows Server 2012 R2 Standard Evaluation
False	False	1524870586	DOMAIN.LOCAL	1529653485	SRV_2.DOMAIN.LOCAL	Windows Server 2016 Standard Evaluation
False	False	1506514307	DOMAIN.LOCAL	1507111547	SRV_3.DOMAIN.LOCAL	Windows Server 2003 Service Pack 2
False	False	1467202171	DOMAIN.LOCAL	1467203508	SRV_4.DOMAIN.LOCAL	Windows Server 2008 R2 Enterprise Service Pack 1
False	False	1476864916	DOMAIN.LOCAL	1476876879	SRV_5.DOMAIN.LOCAL	Windows Server 2012 R2 Standard Evaluation
False	False	1475220041	DOMAIN.LOCAL	1475221378	SRV_7.DOMAIN.LOCAL	Windows Server 2016 Standard Evaluation
False	False	1534144716	DOMAIN.LOCAL	1536560463	SRV_9.DOMAIN.LOCAL	Windows Server 2016 Standard Evaluation
False	False	1487233160	SUB.DOMAIN.LOCAL	1489048871	WS_1.SUB.DOMAIN.LOCAL	Windows 7 Enterprise Business Edition SP1
False	False	1486044415	SUB.DOMAIN.LOCAL	1486046468	WS_12.SUB.DOMAIN.LOCAL	Windows 10 Enterprise
False	False	1488653289	SUB.DOMAIN.LOCAL	1489048856	WS_17.SUB.DOMAIN.LOCAL	Windows 7 Enterprise Business Edition SP1
False	False	1488711717	SUB.DOMAIN.LOCAL	1489049212	WS_2.SUB.DOMAIN.LOCAL	Windows 10 Enterprise
False	False	1486044411	SUB.DOMAIN.LOCAL	1486046464	WS_3.SUB.DOMAIN.LOCAL	Windows 7 Enterprise Business Edition SP1
False	False	1505895637	DOMAIN.LOCAL	1510215305	WS_4.DOMAIN.LOCAL	Windows 8.1 Enterprise
False	False	1486044411	SUB.DOMAIN.LOCAL	1487251207	WS_4.SUB.DOMAIN.LOCAL	Windows 7 Enterprise Business Edition SP1
False	False	1532967914	DOMAIN.LOCAL	1533563312	WS_5.DOMAIN.LOCAL	Windows 10 Enterprise 2016 LTSB
False	False	1486044419	SUB.DOMAIN.LOCAL	1486046470	WS_6.SUB.DOMAIN.LOCAL	Windows 10 Enterprise
False	False	1512119750	DOMAIN.LOCAL	1516638054	WS_7.DOMAIN.LOCAL	Windows 10 Enterprise Evaluation
False	False	1486044419	SUB.DOMAIN.LOCAL	1486046470	WS_8.SUB.DOMAIN.LOCAL	Windows 7 Enterprise Business Edition SP1



```
PS @:\>
PS @:\>
PS @:\> highvalue group | wald0IO | wald0IOAvg | ft
```

Domain	Type	Total	Direction	Target	Count	Percent	Hop	Touch	Cost
*	User	64	Inbound	+	35	54.95	5.42	0.96	2.92
*	Computer	33	Outbound	+	22	66.92	2.25	0.96	1.81



## DirectoryRanger – Vulnerabilities/Misconfiguration

37

### Typical Use Cases

- Audit/Vulnerability Assessments for ADs
- Merger & Acquisition
- Trust Relationships in Supply Chains





## Audit/Vulnerability Assessments for ADs

- Self assessment due to compliance requirements like PCI, HIPAA, ...
- Like an audit interview with an integrated questionnaire
- Technical scan with standard user privileges and without agent installation
- Analyze collected data for security issues



## Merger & Acquisition

- Assessments of foreign Active Directory infrastructure
- Answer the question: "How secure is the other AD?" before establishing trust relationships
- Define tasks before integrating the other infrastructure





## Trust Relationships in Supply Chains

- Assessments of a Partner Active Directory infrastructure within a supply chain
- Answer the question: “How secure is the other AD?” before making a decision about establishing trust relationships
- Define tasks and requirements



DirectoryRanger

172.16.217.129 | https://172.16.217.129/Run

DirectoryRanger Runs mthumann

[New Run](#)

Status	Run Name	Run Policy	Start	Duration	Progress	
<input type="checkbox"/> DONE	mthumann.20-07-2018_09:48	AllTechScripts	07/20/2018 09:48 AM	16s	100 %	
<input type="checkbox"/> WAITING	mthumann.18-07-2018_11:48	SomeChecks			0 %	
<input type="checkbox"/> DONE	mthumann.18-07-2018_11:41	SomeChecks	07/18/2018 11:43 AM	07s	100 %	
<input type="checkbox"/> WAITING	mthumann.12-07-2018_14:16	AllTechScripts			0 %	
<input type="checkbox"/> DONE	mthumann.12-07-2018_09:29	SomeChecks	07/12/2018 09:32 AM	07s	100 %	
<input type="checkbox"/> DONE	mthumann.19-06-2018_16:29	SomeChecks	06/19/2018 16:34 PM	09s	100 %	
<input type="checkbox"/> DONE	mthumann.29-05-2018_11:48	AllQuest	05/29/2018 11:48 AM	07s	100 %	




## Follow Us

- On Twitter ;-)




Thank you for your attention!

 [customer@ernw-sectools.de](mailto:customer@ernw-sectools.de)

[www.ernw-sectools.de](http://www.ernw-sectools.de) 

 [@DirectoryRanger](https://twitter.com/DirectoryRanger)

[www.insinator.net](http://www.insinator.net) 



44