



BloodHound/Framework // Active Directory //
Database Neo4j



\$ Red Teamer

@matt-homjxi0e

السلام عليكم ورحمت الله وبركاته انا جهاد ملقب بي

@homjxi0e

17/ع

Security/Researcher MSF Powershell .NET
/Rerverse/E-G And etc

مطور

Empire/Empyre/ //

بخصوص الاشهر الماضية انضميت لفريق الاحمر

البحث اكتشاف اتجاهات العدو بحوث

Dll inject /VBA-Macro // Analysis //

ووراء البحوث للوجود علل

And etc //

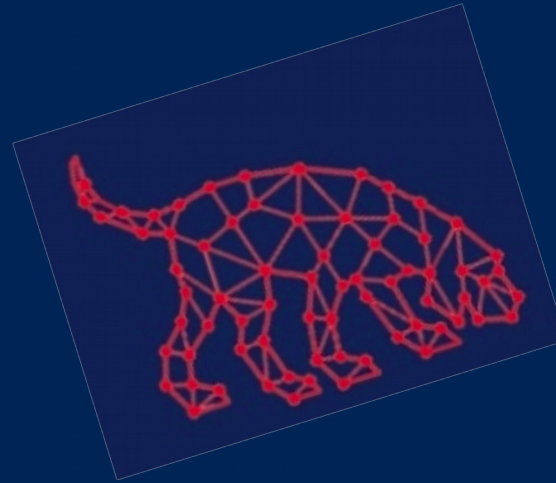
لم تذكر في هذا الوصف



#Red Team

بادن الله وبعد ادنة وبعد الصلاة
والسلام على اشرف الخلق
والمرسلين سيدنا محمد وعلى اهله
وصحبة اجمعين سوف اقدم شريط
متواصل على
(BloodHound/Active Directory
/Database-Neo4j)

What is BloodHound/Framework



اول شي هيا عبارة عن تحلل بيئة اکتيف
ديريکتوري بصورة رسم بياني وبالالاخص
تفهمك كيفية عمل بيئة اکتيف ديريکتوري
وينسبة لها تدعمها
قاعدة بيانات للرسم البياني
Database Neo4j
وتغذيها
Powershell

What is BloodHound // 2

مثل مقلت انها تدعمها قاعدة الرسم
البياني نيو فور دجي يعني انها في لحظة
التحليل لمه تخرج بصورة الرسم البياني
هدأ بفضل قاعدة البيانات نيو فور دجي هدة
القاعدة

البيانات للرسم البياني تدعم اطار بلودهوند

في العروض لي تحليلات بي واسطة
عروضها
الجميلة بالرسم البياني

وكذلك التسجيل الدخول لي اطار
البلودهوند

What is **BloodHound** / 3

مثل مقلت انها تغديها

Powershell

يعني انة التحليل نفسة

على شان يضرلك في

اطار البلودهوند لازم تكون

الملفات وترفعها في

البلودهوند والملفات هادي

هيا داخلها التحليلات لبيئة

اكتيف ديريكتر ومين

هيكون الملفات هادي مثل

مقلت تغديها

Powershell /Generation

this Files Via powershell

- What is database Neo4j

- هيا عبارة عن اطار للرسم
- البياني يعني بمعنى ادق
- وواضح
- انها تعطيك رسم بياني على
- المعلومات الي تقدمها ليها
- انت بتعطيك معلوماتك
- بتنسيق مرتب وبصيورة
- رسم بياني

What Is Active Directory //

اول شي اكتيف ديركتوري هيا بيئة لي عملها
وسياستها ولكن بالاخص هوا تطبيق المغزى منه
توفير الخدمات المركزية وتوفير تقنيات تحديد الهوية
للمتصلين او اي من اتصالات التحقق من هوياتهم
وكذلك توفير امن وامان لي موارد الشبكة

EX/

التحقق من التسجيلات الدخول وبالاخص تحديد هوية
الداخل المتصل

معرفة الاشخاص الامتيازين من الاشخاص العاديين

What is Active Directory // 2

وبنسبة لي بيئة اكتيف ديريكتوري لها العديد من
الاشياء لتوثيق موارد الشبكة وتسير الامور في
نظام التشغيل ويندوز

ادارة الشبكة ومن تحت ادارة الشبكة الي هيا
توثيق موارد الشبكة مثل
موارد الاتصالات المصادقة

خدمات // directory الدليل

هي عبارة عن خدمة قائمة على بتروكول إل داب حيث تستخدم لتحقيق إدارة مركزية للشبكات ومواردها عن طريق تمكين المستخدمين من الوصول لكل المعطيات والمعلومات الموجودة على الشبكة. فيمكننا إدارة شركة عن طريق شبكة بها عدد قليل من المستخدمين حوالي 10 و 5 طابعات وعدد محدود من أجهزة الكمبيوتر دون الحاجة لاستعمال الدليل لكن يصعب علينا إدارة شبكة كبيرة موجودة بشركة بها الاف المستخدمين ومئات الطابعات وعدد كبير من أجهزة الكمبيوتر من دون استعمال الدليل

فوائد اكتيف ديريكثوري

يسمح الدليل النشط ببناء وتنظيم ومراقبة موارد الشبكة في نظام التشغيل ويندوز كما يقوم تخزين معلومات حول المستخدمين وأجهزة الكمبيوتر والأجهزة الأخرى على الشبكة, ويسمح ايضا للمسؤولين بإدارة هذه المعلومات بشكل آمن ويسهل تقاسم الموارد والتعاون بين المستخدمين, كما نقوم بتثبيت الدليل على الشبكة من اجل تثبيت التطبيقات التي تدعم الدليل (مثل مايكروسوفت ® عليه تبادل الخادم) وتكنولوجيايات نظام التشغيل الويندوز الخادم أخرى مثل نهج المجموعة وتثبيته على الجهاز يعطيك صلاحية التحكم المركزي باجزاء الشبكة, كما يمكن تعديل وإضافة أي بيانات من أي جهاز وحدات تحكم المجال, بالإضافة إلى هذا توجد خاصية تسمى النسخ المتماثل هدفها الإبقاء والحفاظ على كل وحدات تحكم المجال محدثة وموزعة في نفس الوقت هذا بالنسبة للدور اما الفوائد فتتمثل في

مكونات الدليل النشط

تعريف الكائن

اي مدخل موجود داخل الدليل النشط له خصائص معينة مثل حسابات المستخدم, الاجهزة, الطابعات الخ... كما ان الدليل النشط يتكون من كائنات حيث كل كائن يمثل كيان الشبكة مثل المستخدمين, الطابعات, أو الخدمات البريدية, بحيث يتم تصنيف الكائنات إلى 3 مجموعات

وصف لي مثال الكائن

كما ان الكائنات تمتلك كل الصفات التي تميزها فعلى سبيل المثال سيتم تعريف المستخدم بلقب, اسم وعنوان حيث ان بعض الكائنات هي حاويات بحيث يمكن لحاوية تخزين الكائنات ولكن أيضا غيرها من الحاويات, كما أن لديها سمات خاصة بها

شجرة اكتيف ديركتوري

.هي مجموعة من النطاقات المرتبطة فيما بينها و التي تتكون من النطاق الاب والنطاق الطفل

مكونات اكتيف ديريكتوري 2

تعريف مسمى الشجرة

هي مجموعة من النطاقات المرتبطة فيما بينها و التي تتكون من النطاق الاب والنطاق الطفل

تعريف مسمى الغابة

مجموعة من الاشجار و النطاق التي لها نفس المميزات و الخصائص في بيئة الويندوز كما تعتبر أكبر محتوى في الدليل, كما ان الغابة هي عبارة عن مجموعة من النطاقات ذات الصلة معا عن طريق علاقة ثقة ثنائية الاتجاه بحيث ان الغابة تتكون من الاشجار التي لها نفس النمط, نفس التكوين ونفس الكتالوج العمومي

امن اكتيف ديركتوري

حماية الكائنات

ان جميع الكائنات الموجودة في الدليل النشط تكون محمية بواسطة قوائم كما ان قوائم تحكم الوصول تقوم (Access Control Lists) تحكم الوصول بتحديد من يمكنه رؤية كائن وما هي الإجراءات المسموحة لكل مستخدم بتنفيذها على الكائن بحيث ان وجود الكائن لا يتم كشفه ابدا لمستخدم لا يملك (SID), حق الاطلاع كما ان كل قوائم تحكم الوصول تحتوي على معرف أمان الذي يحدد مبدأ (مستخدم أو مجموعة) التي تنطبق عليها قوائم تحكم الوصول وتتضمن معلومات عن نوع الوصول لقوائم تحكم الوصول (مسموح أو مرفوض).

نهج المجموعة

ان نهج و سياسات المجموعة هي عبارة عن اعدادات تطبيقية خاصة بالمستخدمين واجهزة الكمبيوتر على عكس ما قد يعني اسمهم, فإنها لا تطبق على مستوى المجموعة, ولكن في كائن الحاوية التي تحتوي على مجموعة من الكائنات مثل المستخدمين أو أجهزة الكمبيوتر التي تطبق الاستراتيجيات المشتركة, لذلك تم تعريفها على مستوى الموقع, النطاق, الوحدات التنظيمية, بحيث تطبق على جميع المستخدمين و أجهزة الكمبيوتر في الحاوية التي تم ربط سياسة الكائنات. نهج المجموعة توفر ميزات أساسية

Download Database neo4j //

<https://neo4j.com/download/other-releases/>

افضل تحميل اصدار
317

Neo4j 3.1.7

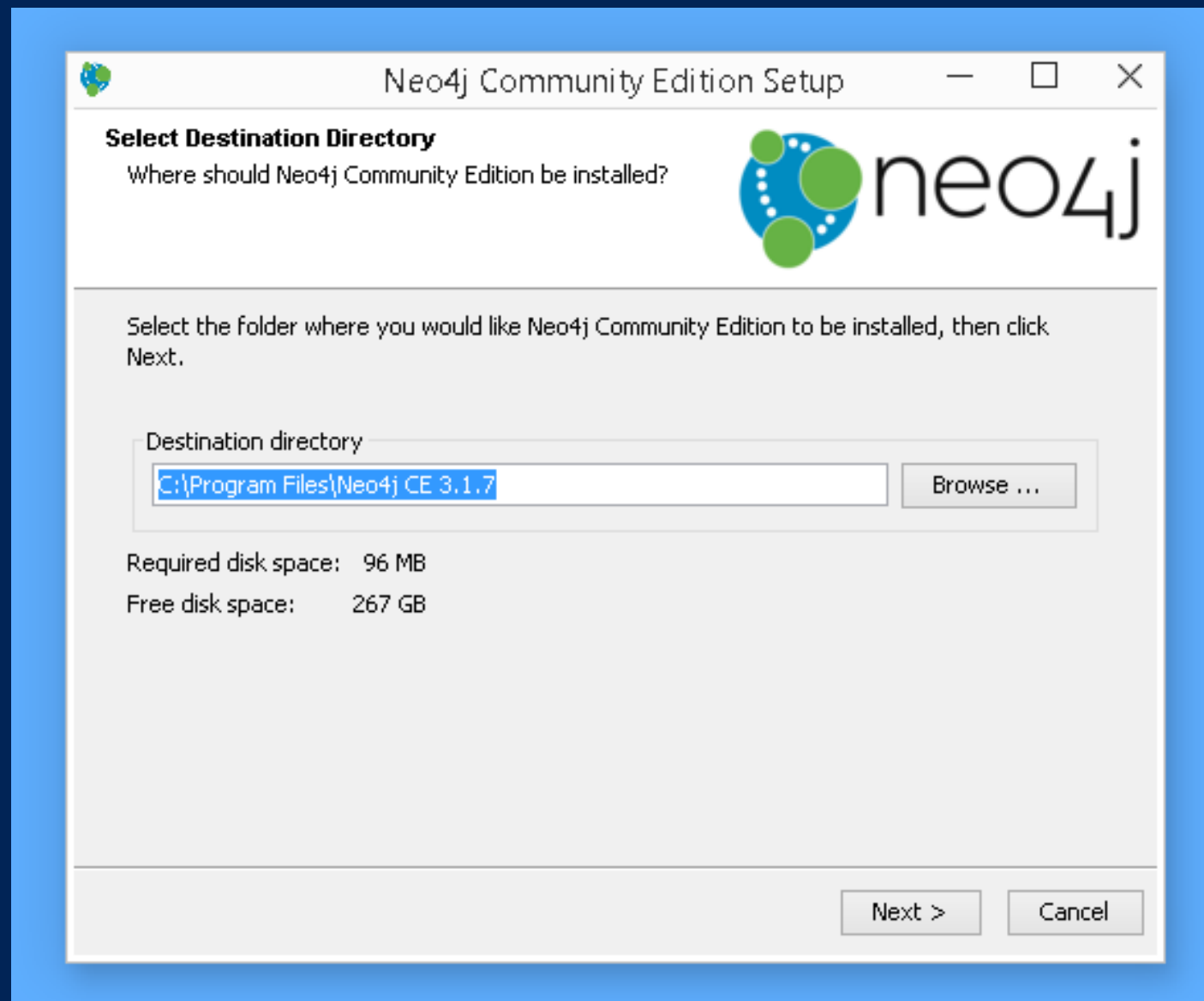
31 July 2017

[Release Notes](#) | [Read More](#)

Linux/Mac	Neo4j 3.1.7 (dmg) Neo4j 3.1.7 (tar)	Neo4j 3.1.7
Windows 64 bit	Neo4j 3.1.7 (exe) Neo4j 3.1.7 (zip)	Neo4j 3.1.7 (zip)
Windows 32 bit	Neo4j 3.1.7 (exe) Neo4j 3.1.7 (zip)	Neo4j 3.1.7 (zip)

Install/database Neo4j

Next And Next ///



Run Database Neo4j //

اضغط

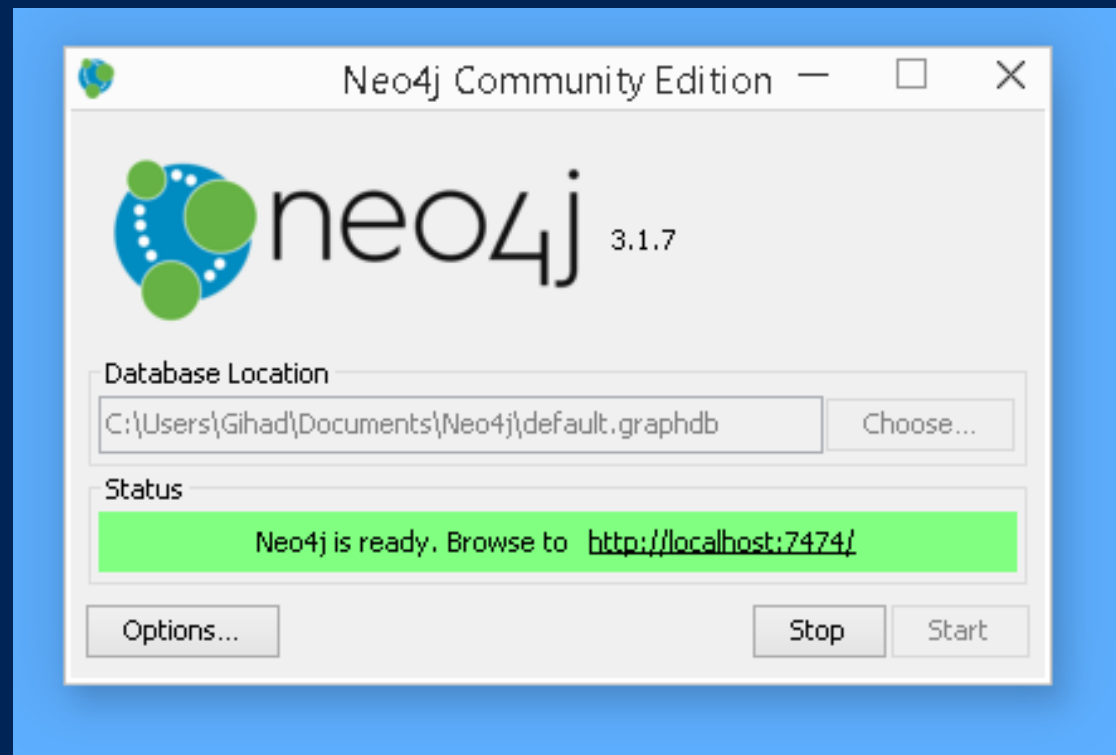
Start //



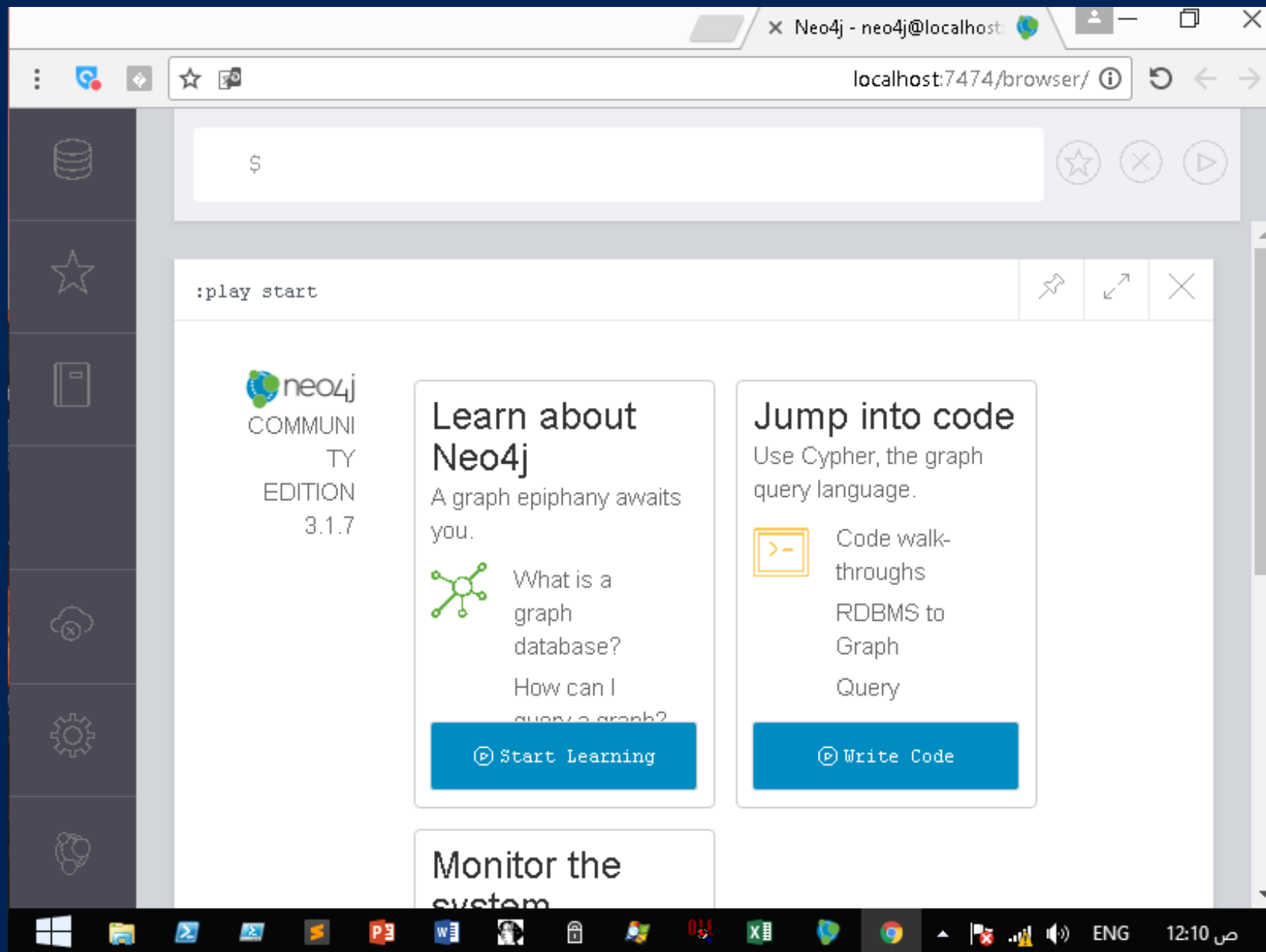
Open () // Database Neo4j

اضغط

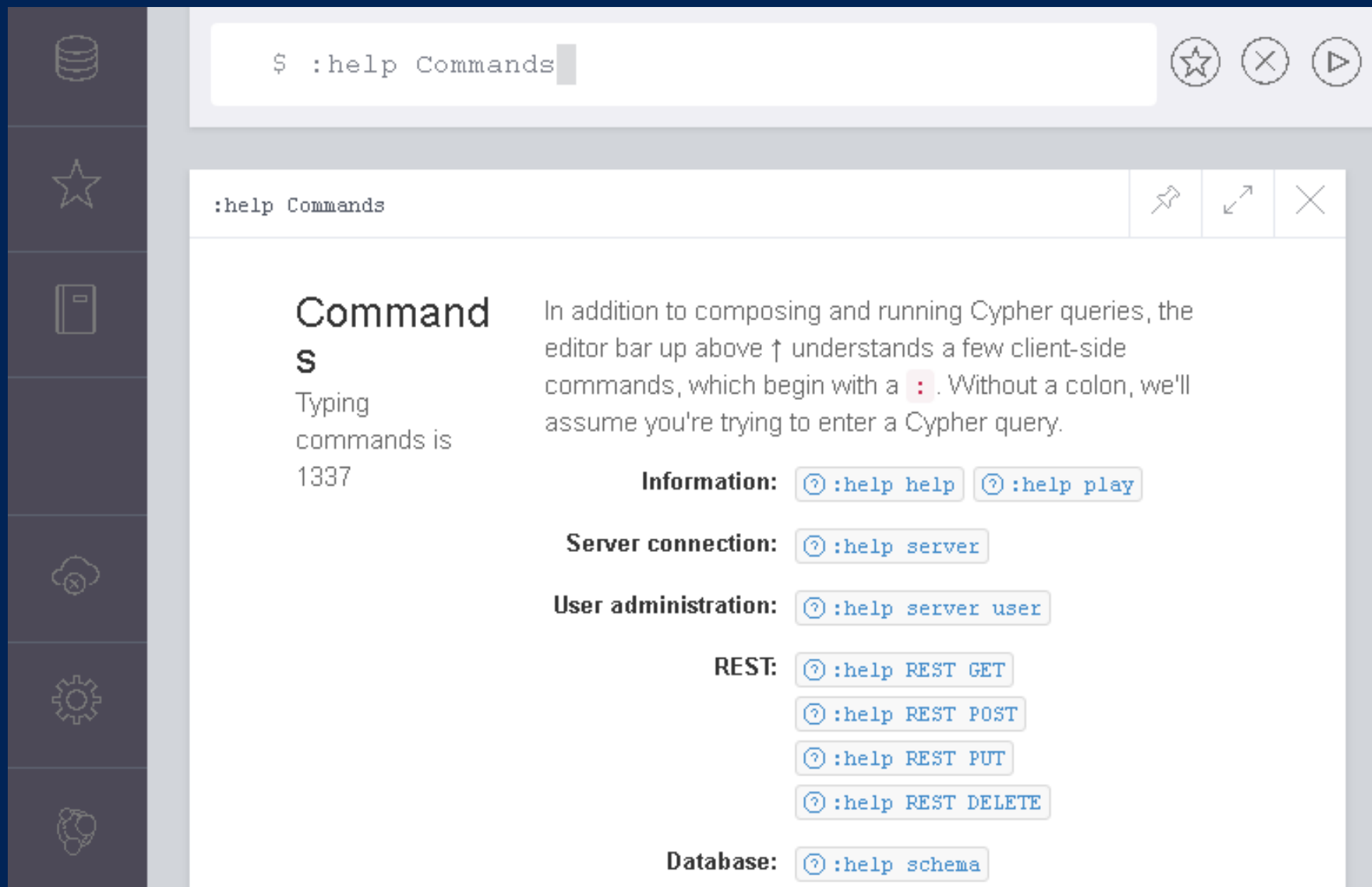
On this host localhost



This interface to database/Neo4j



Now write // :help Commands



The screenshot shows the PowerShell interface with a dark blue sidebar on the left containing icons for database, star, folder, cloud, gear, and brain. The main window has a title bar with a search icon, a close icon, and a play icon. The command prompt shows the command `$:help Commands` being entered. Below the command prompt, a panel titled `:help Commands` displays the help text for the `:help` command. The text explains that the editor bar understands client-side commands starting with a colon, and without a colon, it assumes a Cypher query. The help text is organized into sections: Command, Information, Server connection, User administration, REST, and Database. Each section has a corresponding icon and a list of commands.

Command
S
Typing
commands is
1337

In addition to composing and running Cypher queries, the editor bar up above ↑ understands a few client-side commands, which begin with a `:`. Without a colon, we'll assume you're trying to enter a Cypher query.

Information: `:help help` `:help play`

Server connection: `:help server`

User administration: `:help server user`

REST: `:help REST GET`
`:help REST POST`
`:help REST PUT`
`:help REST DELETE`

Database: `:help schema`

Write // :server connect // to View //Windows
login to BloodHound And Database/Neo4j

اول شي لازم تسجل دخولك

من ميزات يحدد الهوست والمنفذ تلقائي لاجابة
لكتابة ولكن هيطالعك بي كلمة لوكل هوست اد كان
ويندوز خليها واد كان نضام غير

Mac/linux//write 127.0.0.1 in site localhost

وطبعا خلي اليوزر مثل نفسة وقم بكتابة بسورد
لتسجيل وبعد وقم بنسخ هوست التسجيل كلة

\$:server connect

Connect to Neo4j

Database access requires an authenticated connection.

Host

Username

Password

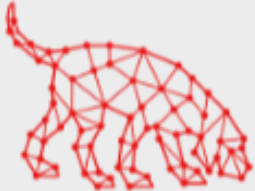
Connect

الملخص المفيد من اخذ

ID is / http to Ports // And not Name/Browser

// bolt://localhost:7687 //

And //User//Password



BLOODHOUND

Log in to Neo4j Database

Database URL	bolt://localhost:7687
DB Username	neo4j
DB Password	neo4j

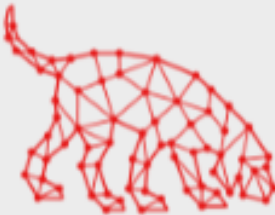
☐ Save Password

Login

قم بكتابة اليوزر والبسورد الذي سجلته في تسجيلك في
Database // Neo4j //

ونسبة لي
URL
خط

bolt://id of neo4j:7687



BLOODHOUND

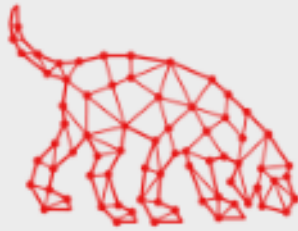
Log in to Neo4j Database

Database URL	bolt://localhost:7687
DB Username	neo4j
DB Password	neo4j

☐ Save Password

Login

إذا كان التسجيل الدخول صحيح سوف يدخل اد كان غلط
هيعطيك وصفة التحقق من اليوزر والبسورد والان بمجرد
نعطيلة دخول سوف يدخل



BLOODHOUND

Log in to Neo4j Database

Database URL	<input type="text" value="bolt://localhost:7687"/>
DB Username	<input type="text" value="neo4j"/>
DB Password	<input type="password" value="....."/>

☐ Save Password

Success!

Interface //BloodHound// \$

The screenshot shows the BloodHound web interface within a PowerShell window. The interface has a title bar 'BloodHound' and standard window controls. At the top, there is a search bar with the placeholder text 'Start typing to search for a node...' and two icons: a magnifying glass and a double arrow. Below the search bar are three tabs: 'Database Info' (selected), 'Node Info', and 'Queries'. The 'Database Info' tab displays the following information:

Database Info	
DB Address	bolt://localhost:7687
DB User	neo4j
Users	0
Computers	0
Groups	0
Sessions	0
Relationships	0

Below the table are four buttons: 'Refresh DB Stats' (green), 'Clear Sessions' (blue), 'Log Out/Switch DB' (orange), and 'Clear Database' (red). On the right side of the interface, there is a vertical toolbar with icons for refresh, home, user, add node, graph, settings, and help. At the bottom center, there is a button labeled 'Raw Query' with up and down arrows. On the bottom right, there are three buttons: a plus sign, a circle with a slash, and a minus sign.

Now //Generation // Files // Analysis // (AD) Via Module In /Empire

```
(Empire: matthomjxi0e) > usemodule situational_awareness/network/bloodhound  
(Empire: powershell/situational_awareness/network/bloodhound) > execute  
[>] Module is not opsec safe, run? [y/N] y  
(Empire: powershell/situational_awareness/network/bloodhound) >  
Job started: STCLA9
```

```
Writing output to CSVs in: C:\Windows\system32\  
Done writing output to CSVs in: C:\Windows\system32\  
Invoke-BloodHound completed!
```

This Generation In Path:> C:\Windows\system32

Will Generation 4 Files In the Path //

Users

Computers

Groups

Users

هو يقوم بجمع معلومات المستخدم كاملة

ويوجد فيه كثير من اقسام ملف المستخدم اهاد تحتوي على

معلومات سوف تعرض في اطار بلودهوند

-Name: This is the name for the node, and is in domain simple format.

-SAMAccountName:

This is the SAMAccountName for the user. This information is not currently collected by the ingestor.

-Display Name:

This is the Windows display name for the user. This information is not currently collected by the ingestor.

-Password Last Changed:

This is the date for when the user's password last changed. This information is not currently collected by the ingestor.

-Sessions:

These are all the computers the ingestor identified the user as logged onto during collection.



Computers //

-Name:

This is the name of the node, and is in fully qualified format.

-OS:

The OS for the computer. This information is not currently gathered by the ingestor.

-Allows Unconstrained Delegation:

Whether the computer allows unconstrained delegation. This information is not currently gathered by the ingestor.

-Sessions:

These are the user sessions on the computer the ingestor identified during data collection.



Local Admins

Computers // 2

-Explicit Admins: These are the explicit users and groups that have local administrator rights on the system. This is the equivalent of running `net localgroup administrators` on the host.

-Unrolled Admins: These are all of the effective groups and users that have administrator rights on the system. This is the equivalent of running `Get-NetLocalGroup -ComputerName computename -Recurse`

-Derivative Local Admins: These are all the effective groups and users that have a derivative admin style attack path to the computer.

Group Memberships

-First Degree Group Membership: These are the groups that the computer belongs to.

-Unrolled Group Memberships: These are all of the effective group memberships the computer has.

-Foreign Group Memberships: These are all of the foreign groups that the computer belongs to.

Local Admin Rights

Computers // 3 //

-First Degree Local Admin: These are the computers where the computer object is added explicitly as a local administrator on a system.

-Group Delegated Local Admin Rights: These are the computers that the computer gains administrator privileges to based on delegated group rights.

-Derivative Local Admin Rights: These are the computers the computer can gain administrator rights to by impersonating a user currently using a computer the user has administrator privileges to, regardless of how deep this chaining goes.

Outbound Object Control

-First Degree Object Control: These are the other objects that this computer has direct control over.

-Group Delegated Object Control: These are the objects that this computer has control over via security group delegation.

-Transitive Object Control: These are the objects that this computer has an ACL-only attack path to.

Group // 1

Node Info

-Name:

The display name of the group.

-Sessions:

These are all the computers the ingestor identified the effective users of the group as logged onto during collection.



Group // 2 //

Group Members

-Direct Members: These are the users and groups that are explicitly added to this group. This is the information you would see when typing `net group groupname /domain`

-Unrolled Members: These are all of the effective group memberships for the group. This is the equivalent of running `Get-NetGroup`

`-GroupName groupame -Recurse`

-Foreign Members: These are users belonging to this group which themselves belong to a foreign domain

Group Membership

-First Degree Group Memberships: These are the groups that the group is explicitly a member of.

-Unrolled Group Memberships: These are all of the group's effective group memberships.

-Foreign Group Memberships: These are all of the foreign groups that the group belongs to.



Group // 3 //

Local Admin Rights

-First Degree Local Admin:

These are the computers where the group itself is added explicitly as a local administrator on a system.

-Group Delegated Local Admin Rights:

These are the computers that the user group administrator privileges to based on delegated group rights.



-Derivative Local Admin Rights:

These are the computers the group can gain administrator rights to by impersonating a user currently using a computer the user has administrator privileges to, regardless of how deep this chaining goes.

Group // 4 //

Outbound Object Control

-First Degree Object Control:

These are the other objects that this group has direct control over.

-Group Delegated Object Control:

These are the objects that this group has control over via security group delegation.



-Transitive Object Control:

These are the objects that this group has an ACL-only attack path to.

Group // 5 //

Inbound Object Control

-Explicit Object Controllers:

The other principals which have first degree control over this group.

-Unrolled Object Controllers:

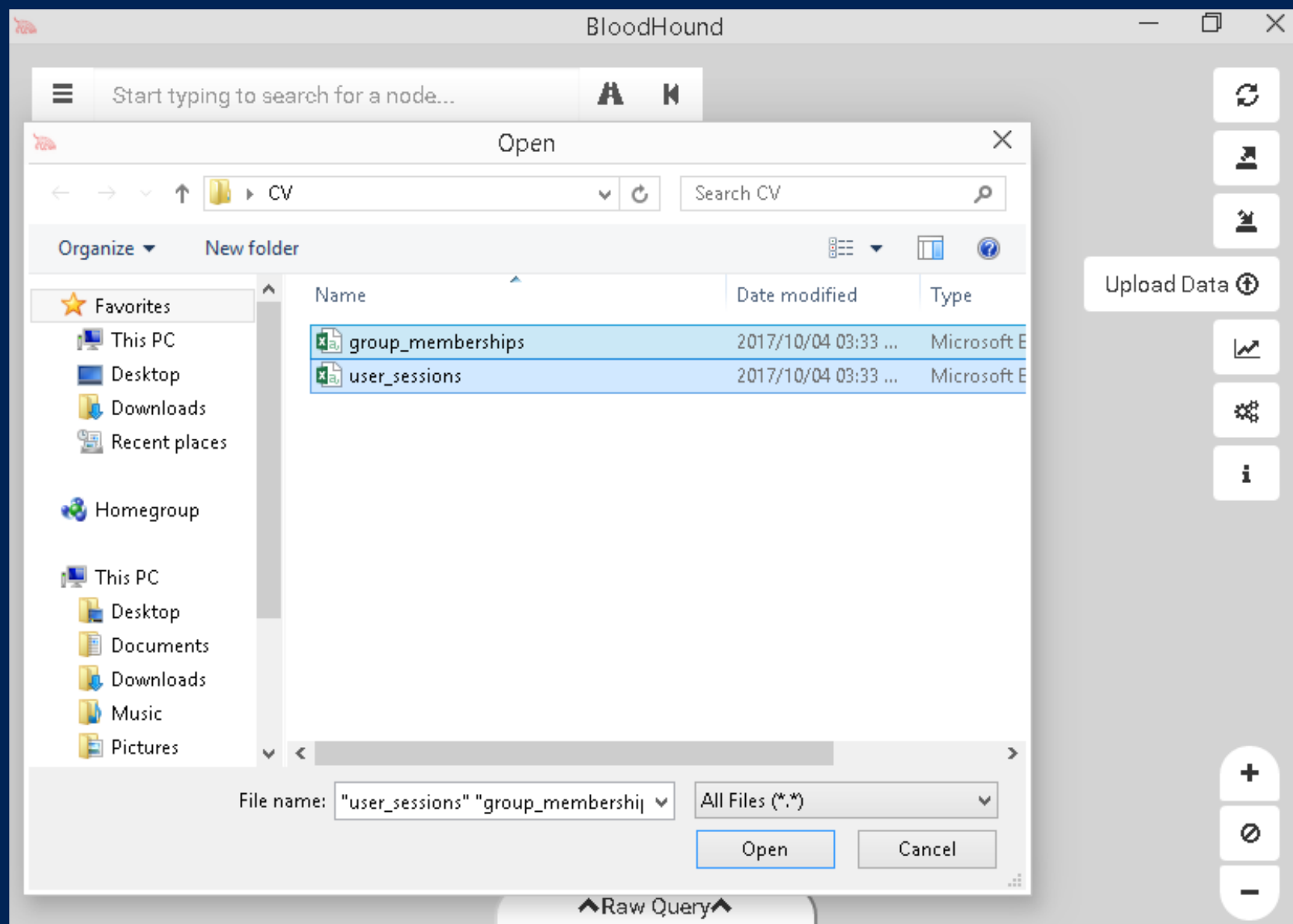
By unrolling the first degree groups with control of this group, we see all the effective principals which control over this object via security group delegation



-Transitive Object Controllers:

These are the other principals in the environment that have an ACL-only attack path to this group object.

Now // Exporting the Files in BloodHound // Upload of Path Generation //



This End the to
BloodHound Framework

What ?



This End On Course
Good // Bye



Soon Update This pdf // Soon //

Author: (@matthomjxi0e)

Twitter: <https://twitter.com/homjxi0e>

Github: <https://github.com/jihadLkmaty218>

