detect by tcp time

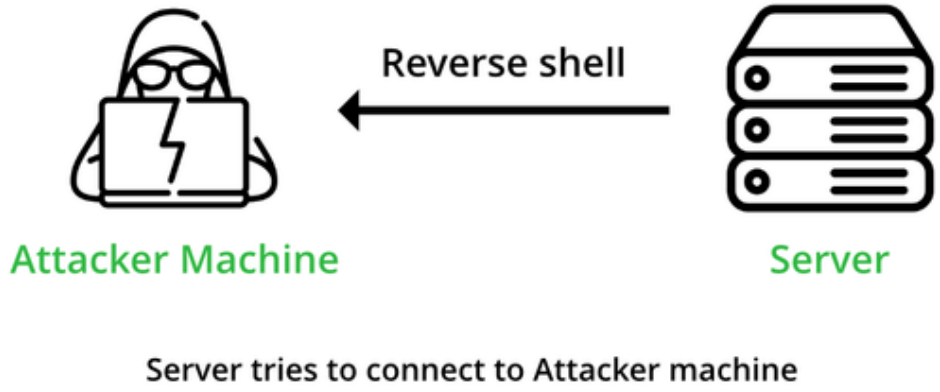
بسم الله الرحمن الرحيم

detect tcp connection by tcp time

فيه انواع كثيرة من ال reverse shells بس كلها تتشارك في انها تنقل المعلومات عبر الشبكة سواء كان على udp او tcp ف دامهم كلهم يشتركون بالشي هذا اذا قدرت اراقب الشبكة بشكل صحيح راح اقدر اني اكتشف كثير المالوير فقط من مراقبة الشبكة

detect by tcp time?

وش يعني اني اكتشفت المالوير من الوقت حق اتصال ال tcp؟ التروجين مثلا راح يعطي المخترق صلاحية انه ينفذ كوماندات على الجهاز و كل شي يمر عبر tcp connection او udp بس حاليا نركز على ال tcp فقط



ف ممكن اعتمد على مراقبة الاتصال و في المقالة السابقة تكلمنا عن حجم البيانات اللي تمر و نراقبها بس هذي بتكون ممتازة في مراقبة ال data exif اما في ال C2 الوضع مختلف لأن البايتات اللي تنرسل ممكن تكون صغيرة جدا مافيها اي تحميل ملفات ف راح تقل فعالية الخاصية ف عشان كذا سويت detect by time و اللي تعني البروسيس هذي كم لها ترسل و تستقبل كم الوقت اللي قاعدة ترسل فيه ممكن يوضح معكم مع مثال nc الحين

Demo

```
config.json
"whitelist_network_procs_time":[
"C:\\Program Files\\Google\\Chrome\\Application\\chrome.exe",
],
      "data_tcp_time":600
```

هنا نفس المقالة السابقة البروسيس اللي ما بنراقبها موجودة و الوقت اللي لو تعدته البروسيس في الاتصال راح يجيني alert عليه

```
C:\Users\kira2\Desktop\netcat-1.11>nc 127.0.0.1 1234 -vv
checkhost.local [127.0.0.1] 1234 (?) open

ls
^C
C:\Users\kira2\Desktop\netcat-1.11>nc 127.0.0.1 1234 -vv
checkhost.local [127.0.0.1] 1234 (?) open
zxcc
```

الحين مسوي اتصال nc بسيط اقدر ارسل و استقبل زي ما ابي و دامني ما وصلت لحد بايتات معين ف خاصية detect by size اللي بالمقالة السابقة ماراح تشتغل الا في حالة اني تعديت البايتات المسموحة راح يجيني alert بس زي ما قلنا في ال C2 فيه احتمال و لو كان ضعيف ان ماراح يجيك alert ف ايش تسوي في هذي الحاله؟ تكشفه من وقت الاتصال نفسه

الحين بعد ما خليت ال nc شغال لمدة 10 دقايق مع اني ما ارسلت الا حجم بايتات قليل جدا و ما سويت اي شي ضار الا انه بيعطيني alert

الملخص

الخاصية ذي تعطيك تحكم اكبر زي ما ان الخاصية الماضية تعطيك القدرة انك تكتشف من ال size هذي الخاصية تعطيك القدرة انك تكتشف من الوقت