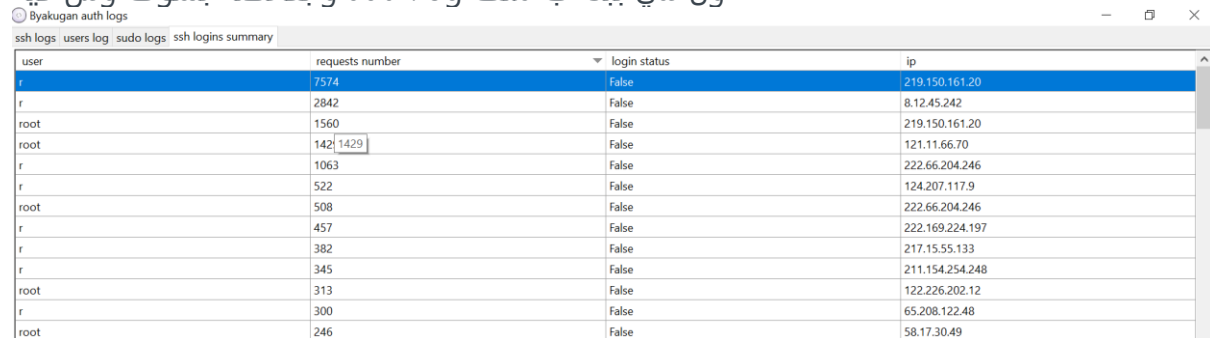


securityLinux forensics logs #2

بسم الله اليوم بتكلم عن فحص logs لنظان لينكس و اليوم بيكون سيناريو واقعي
في البداية باستخدام اداتي المتواضعه [بياكوغان](#)

auth.log

اول شي بدأ ب ملف auth.log و بفحصه بشوف وش فيه



user	requests number	login status	ip
r	7574	False	219.150.161.20
r	2842	False	8.12.45.242
root	1560	False	219.150.161.20
root	1421	False	121.11.66.70
r	1063	False	222.66.204.246
r	522	False	124.207.117.9
root	508	False	222.66.204.246
r	457	False	222.169.224.197
r	382	False	217.15.55.133
r	345	False	211.154.254.248
root	313	False	122.226.202.12
r	300	False	65.208.122.48
root	246	False	58.17.30.49

زي ما نلاحظ هنا كل ابيي و كم ريقويست ارسل و هل تم تسجيل دخوله بشكل صحيح ب ssh او
لا نأخذ الابيي الاول اللي ارسل 7574 ريقويست و اليوزر اللي يخمن عليه r و هذا شي بفتح
auth.log اشيك ممكن تكون مشكله بالاداة

```
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
```

و مظهر لي اي يوزر في اللوقز ما اعرف وش السبب بس مافيه مشكله نكمل فحص باخذ ابيي
219.150.161.20 و بشوفه باللوقز هل هو قاعد يسوي تخمين على ssh او لا

ip	user	time
219.150.161.20	r	Apr 19 06:15:42
219.150.161.20	r	Apr 19 06:15:42
219.150.161.20	r	Apr 19 06:15:44
219.150.161.20	r	
219.150.161.20	r	
219.150.161.20	r	
219.150.161.20	r	
219.150.161.20	r	
219.150.161.20	r	Apr 19 06:15:56
219.150.161.20	r	Apr 19 06:15:57
219.150.161.20	r	Apr 19 06:15:58
219.150.161.20	r	Apr 19 06:16:00
219.150.161.20	r	Apr 19 06:16:01
219.150.161.20	r	Apr 19 06:16:02

Find

What you want to find

OK

Cancel

219.150.161.20

في البداية رتبت الايبيات بناء على الرقم و ضغطت كلك يمين و بحثت عن الايبي و بشوف الوقت من بين كل ريقويست و واضح انه كل ثانيه الى ثانيتين يرسل ف واضح انه تخمين و اصلا كان واضح من يوم شفنا انه ادخل 7574 باس غلط في ssh حلو الحين عرفنا انه تخمين + عرفنا انه ارسل 7574 باس غلط السؤال يقول هل قدر يلقي الباس و يدخل او لا؟

user	requests number	login status	ip
root	4	True	188.131.23.37
root	1	True	94.52.185.9
user3	3	True	192.168.126.1
dhg	2	True	190.167.74.184
root	1	True	222.169.224.197
root	1	True	201.229.176.217
dhg	20	True	190.166.87.164
root	1	True	193.1.186.197
root	4	True	219.150.161.20
user1	1	True	166.129.196.88
user3	1	True	208.80.69.74
user1	1	True	67.164.72.181
root	1	True	10.0.1.2
user3	1	True	65.195.182.120
user1	1	True	65.195.182.120

استخدم خاصيه البحث مره ثانيه و ارتبها حسب التسجيل الدخول صحيح و نشوف انه قدر يدخل و بيوزر روت! و دخل على نظامنا 4 مرات طيب هل هو الايبي الوحيد اللي دخل عن طريق التخمين؟ نسوي نفس الخطوات على ايبي ثاني

user	requests number	login status	ip
root	1	True	222.66.204.246
root	1	True	201.229.176.217
root	1	True	190.167.70.87
r	1	False	mail.mediamonitors.com.pk
user3	2	True	208.80.69.69

هذا الايبي دخل روت بعد و كان يخمن على بورت ssh

action	ip	user	time
ssh login succeed	219.150.161.20	root	Apr 19 05:42:27
ssh login succeed	76.191.195.140	user1	Apr 15 19:48:38

و هذا تاريخ دخول احد الايبيات عن طريق ssh و بيوزر روت

vsftpd.log

بنشوف ملف vsftpd.log و يمكن نحصل شي

user	command	file	ip	size (bytes)	time
kali	DOWNLOAD	/home/kali/Downloads/LoveReverse	mail.mediamonitors.com.pk	19432	Fri Feb 4 12:49:03
kali	UPLOAD	/home/kali/Downloads/auth.log	mail.mediamonitors.com.pk	25643	Fri Feb 4 12:50:33
kali	DOWNLOAD	/home/kali/Downloads/LoveReverse	mail.mediamonitors.com.pk	19432	Fri Feb 4 12:49:03
kali	UPLOAD	/home/kali/Downloads/auth.log	mail.mediamonitors.com.pk	25643	Fri Feb 4 12:50:33
kali	UPLOAD	/home/kali/Downloads/Labs.7z	mail.mediamonitors.com.pk	7584879	Mon Jan 24 22:45:06 2022

هذي الاشياء اللي صارت من اشياء انرفعت او تحملت

admin	False	76.191.195.140	Sat Feb 5 11:55:22
admin	False	76.191.195.140	Sat Feb 5 11:55:22
admin	False	76.191.195.140	Sat Feb 5 11:55:22
admin	False	76.191.195.140	Sat Feb 5 11:55:25
admin	False	76.191.195.140	Sat Feb 5 11:55:25
admin	False	76.191.195.140	Sat Feb 5 11:55:25
admin	False	76.191.195.140	Sat Feb 5 11:55:28
admin	False	76.191.195.140	Sat Feb 5 11:55:28
admin	False	76.191.195.140	Sat Feb 5 11:55:28
admin	False	76.191.195.140	Sat Feb 5 11:55:32
admin	False	76.191.195.140	Sat Feb 5 11:55:32
admin	False	76.191.195.140	Sat Feb 5 11:55:32
admin	False	76.191.195.140	Sat Feb 5 11:55:35
admin	False	76.191.195.140	Sat Feb 5 11:55:35
admin	False	76.191.195.140	Sat Feb 5 11:55:35
admin	False	76.191.195.140	Sat Feb 5 11:55:38

و من ناحية محاولات الدخول نفس الشي فيه تخمين كيف عرفت؟ الوقت و الايبي طيب هل قدر يدخل على يوزر الادمن؟

user	requests number	login_status	ip
kali	4	True	mail.mediamonitors.com
root	2	False	208.80.69.74
anonymous	2	False	208.80.69.74
admin	605	False	76.191.195.140
anonymous	3	False	192.168.210.10
kali	4	True	65.195.182.120
root	1	False	65.195.182.120
ftpuser	1	True	65.195.182.120

الحمد لله ماقدر يدخل ftp حقنا حاول يخمن 605 مره بس ماقدر يدخل بس فيه شي غريب mail.mediamonitors.com.pk هذا وش يبي ليه دخل ftp و بيوزر كالي؟ هذي ممكن ترفقها بالتقرير حقا بس لو طلع سيرفر عادي مصرح له يدخل ف مافيه مشكله لو انه تخمين بيطلع لنا انه خمن بس كل محاولات تسجيل الدخول صحيحة بنسبة 100% ممكن نرجع و نشوف الوقت اللي دخل فيه

user	login status
ftpuser	True
kali	True
root	False
anonymous	False
kali	True
anonymous	False
kali	True
anonymous	False
kali	True

احد الخصائص الحلو انك تقدر تحفظ النتائج ك csv عشان تستفيد من كل خصائص excel

A1						
	A	B	C	D	E	F
1	user	command	file	ip	size (bytes)	time
2	kali	DOWNLOAD	/home/kali/Downloads/ILoveReverse	127.0.0.1	19432	Fri Feb 4 12:49:03
3	kali	UPLOAD	/home/kali/Downloads/auth.log	127.0.0.1	25643	Fri Feb 4 12:50:33
4	kali	DOWNLOAD	/home/kali/Downloads/ILoveReverse	127.0.0.1	19432	Fri Feb 4 12:49:03
5	kali	UPLOAD	/home/kali/Downloads/auth.log	127.0.0.1	25643	Fri Feb 4 12:50:33
6	kali	UPLOAD	/home/kali/Downloads/Labs.7z	192.168.210.10	7584879	Mon Jan 24 22:45:06 2022
7						

الملخص

شفنا اللوقز حقت ال ftp , ssh و شفنا مين من اليوزرات سجل دخول و مين منهم bruteforce و
كل من دخل ftp وش سوا بالضبط