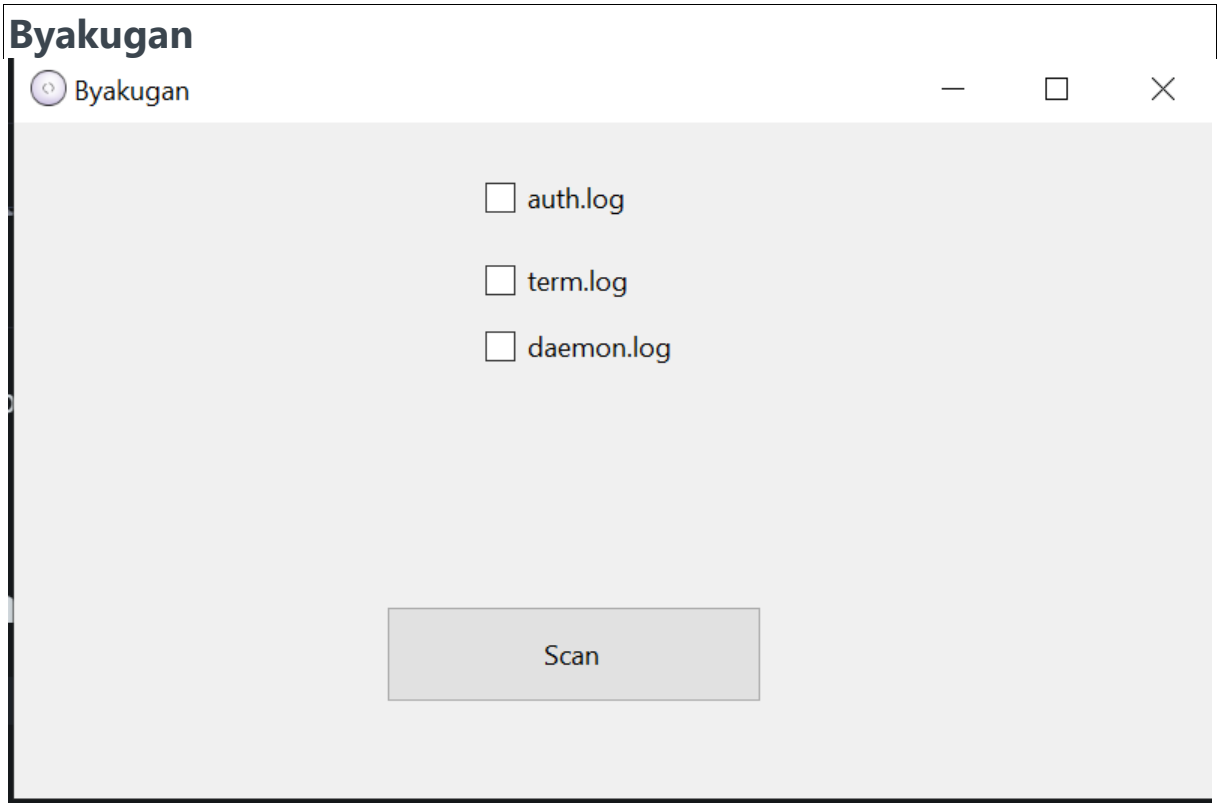
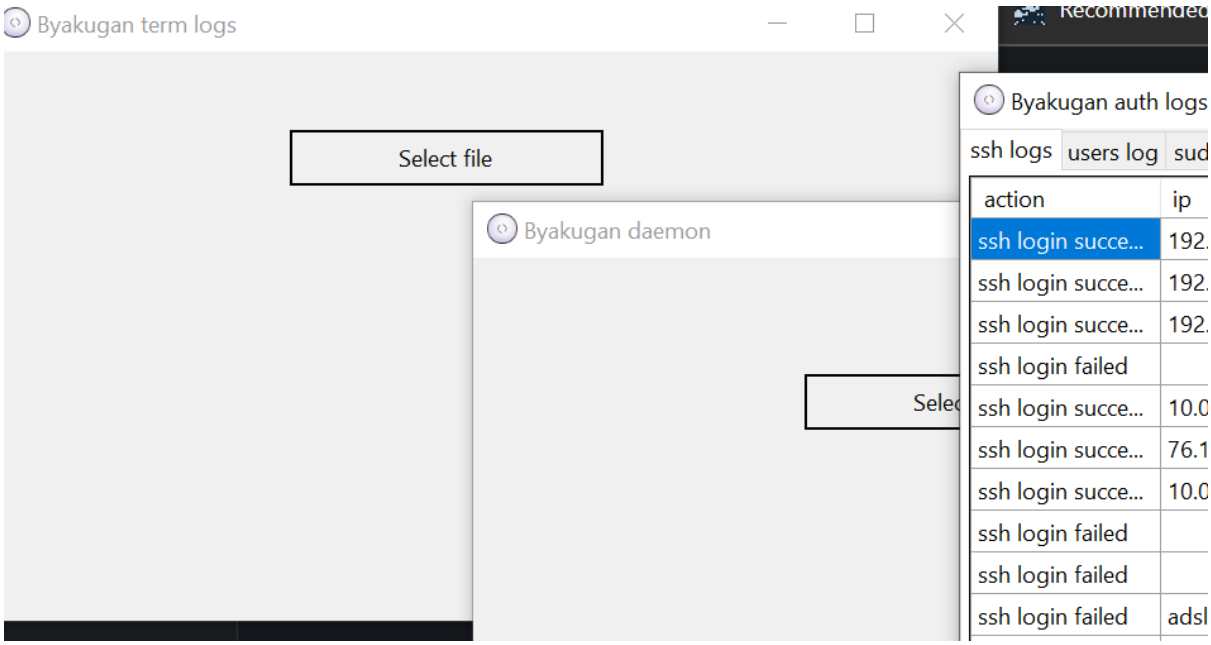
Linux forensics logs #1

و بنسخدم اداة linux لجهاز نظامة logs بسم الله الرحمن الرحيم اليوم بنحلل برمجتها انا و وظيفتها مساعدتك بالفحص فقط

لتحميل الاداة و بنحلل هذي الملفات auth.log و daemon.log و term.log



اول ما نشغل الاداة بتجينا هذي الواجهة البسيطة حدد نوع الملف اللي تبي تفحصه طبعا حاليا بس فيه 3 انواع و ان شاء الله ازيدها ف بحدد على كل الملفات عشان يفحصها لي



بما اني حددت الثلاثة كلهم بيفتح لي 3 نوافذ و عشان تفرق بينهم تشوف العنوان او تقدر تحلل ملف ملف عشان ما تصير زحمة عندك و بيطلب منك تحدد مسار الملف و تقدر تبدأ

auth.log

بيكون اول ملف نشيك عليه و نفتحه بالاداة و نشوف وش يجي لنا

ssh login succeed	user3	192.168.126.1	Mar 16 08:26:06 app-1 sshd[4894]: Accepted password for us
ssh login succeed	user3	192.168.126.1	Mar 16 10:14:02 app-1 sshd[5142]: Accepted password for us
ssh login succeed	user3	192.168.126.1	Mar 16 17:12:24 app-1 sshd[5513]: Accepted password for us
ssh login failed			Mar 18 09:41:54 app-1 login[4673]: pam_unix(login:auth): auth
ssh login succeed	user3	10.0.1.2	Mar 18 09:42:22 app-1 sshd[4693]: Accepted password for us
ssh login succeed	user1	76.191.195.140	Mar 18 10:00:10 app-1 sshd[4764]: Accepted password for us
ssh login succeed	user3	10.0.1.2	Mar 18 10:00:30 app-1 sshd[4786]: Accepted password for us

بنشوف هنا ان فيه كثير ناس حاولو يتصلو ssh و دخلهم و فيه اكثر من ايبي بنسوي ترتيب حسب الوقت و نشوف

ssh login failed	58.17.30.49		Apr 19 05:18:35 app-1 sshd[7155]: pam_unix(sshd:auth): aut
ssh login failed	58.17.30.49		Apr 19 05:18:40 app-1 sshd[7157]: pam_unix(sshd:auth): aut
ssh login failed	58.17.30.49		Apr 19 05:18:45 app-1 sshd[7159]: pam_unix(sshd:auth): aut
ssh login failed	58.17.30.49		Apr 19 05:18:49 app-1 sshd[7161]: pam_unix(sshd:auth): aut
ssh login failed	58.17.30.49		Apr 19 05:18:54 app-1 sshd[7163]: pam_unix(sshd:auth): aut
ssh login failed	58.17.30.49		Apr 19 05:18:59 app-1 sshd[7165]: pam_unix(sshd:auth): aut
ssh login failed	58.17.30.49		Apr 19 05:19:04 app-1 sshd[7167]: pam_unix(sshd:auth): aut

فيه ايبيات قاعدين يحاولون يسوون bruteforce لو تلاحظ الوقت و انه مادخله بتعرف انه يخمن

ssh logs | users log | sudo logs

action	user	log msg
useradd	user4	Mar 16 08:12:13 app-1 useradd[4692]: new user: name=user4, UID=1001, GID=1001, home=/home/user4
userdel		Mar 16 08:12:31 app-1 userdel[4700]: delete user `user4'
userdel		Mar 16 08:12:31 app-1 userdel[4700]: removed group `user4' owned by `user4'
useradd	user1	Mar 16 08:12:38 app-1 useradd[4703]: new user: name=user1, UID=1001, GID=1001, home=/home/user1
useradd	user2	Mar 16 08:12:55 app-1 useradd[4711]: new user: name=user2, UID=1002, GID=1002, home=/home/user2
useradd	sshd	Mar 16 08:25:22 app-1 useradd[4845]: new user: name=sshd, UID=104, GID=65534, home=/var/run/sshd
useradd	Debian-exim	Mar 18 10:15:42 app-1 useradd[5393]: new user: name=Debian-exim, UID=105, GID=114, home=/var/spo
useradd	mysql	Mar 18 10:18:26 app-1 useradd[6966]: new user: name=mysql, UID=106, GID=115, home=/var/lib/mysql,
useradd	packet	Apr 19 22:38:00 app-1 useradd[2019]: new user: name=packet, UID=0, GID=0, home=/home/packet, shel
useradd	dhg	Apr 19 22:45:13 app-1 useradd[2053]: new user: name=dhg, UID=1003, GID=1003, home=/home/dhg, sl
useradd	messagebus	Apr 24 19:27:35 app-1 useradd[1386]: new user: name=messagebus, UID=108, GID=117, home=/var/run,
useradd	fido	Apr 25 10:41:44 app-1 useradd[9596]: new group: name=fido, GID=1004
useradd	fido	Apr 25 10:41:44 app-1 useradd[9596]: new user: name=fido, UID=0, GID=1004, home=/home/fido, shell=
useradd	wind3str0y	Apr 26 04:43:15 app-1 useradd[20115]: new user: name=wind3str0y, UID=1004, GID=1005, home=/home

هنا نشوف اليوزرات اللي انضافت او انحذف و مع الوقت حقها

user3	/bin/su	Mar 18 10:00:36 app-1 sud
user1	/bin/su -	Mar 18 10:01:03 app-1 sud
user1	/bin/su -	Mar 18 10:02:09 app-1 sud
user1	/usr/bin/vi /opt/software/base/vmscripts...	Mar 18 10:34:55 app-1 sud
user3	/bin/su	Mar 18 10:35:25 app-1 sud
user1	/bin/rm software.wsgi	Mar 18 10:36:00 app-1 sud
user1	/bin/ln -sf /opt/software/web/app/domai...	Mar 18 10:36:13 app-1 sud
user1	/usr/bin/vi settingsdebug.py	Mar 18 10:38:07 app-1 sud
user1	/usr/bin/svn commit -m settingsdebug s...	Mar 18 10:41:09 app-1 sud
user1	/usr/bin/svn commit -m settingsdebug s...	Mar 18 10:41:13 app-1 sud
user1	/usr/bin/vi settingsdebug.py	Mar 18 10:43:36 app-1 sud
user1	/usr/bin/vi settingsextra.py	Mar 18 10:44:09 app-1 sud
user1	/usr/bin/vi /etc/hosts	Mar 18 10:45:44 app-1 sud
user1	/usr/bin/vi manage.py	Mar 18 10:54:47 app-1 sud
user1	/usr/bin/vi /opt/software/base/vmscripts...	Mar 18 10:55:31 app-1 sud
user1	/usr/bin/vi settingsdebug.py	Mar 18 10:56:12 app-1 sud
user1	/usr/bin/vi /opt/software/base/vmscripts...	Mar 18 10:56:51 app-1 sud
user1	/usr/bin/vi /opt/software/base/vmscripts...	Mar 18 10:56:56 app-1 sud
user1	/usr/bin/vi /opt/software/base/vmscripts...	Mar 18 10:59:49 app-1 sud

و هنا بعض الاوامر اللي سوا لها اليوزر sudo و نقدر نشوف اليوزر و الكوماند اللي سواه

	/sbin/iptables -A INPUT -p ssh -dport 2424 -j ACCEPT
	/sbin/iptables -A INPUT -p tcp -dport 53 -j ACCEPT
	/sbin/iptables -A INPUT -p udp -dport 53 -j ACCEPT
	/sbin/iptables -A INPUT -p tcp --dport ssh -j ACCEPT
	/sbin/iptables -A INPUT -p tcp --dport 53 -j ACCEPT
	/sbin/iptables -A INPUT -p tcp --dport 113 -j ACCEPT
	/usr/sbin/ufw disable
	/usr/sbin/ufw enable

نشوف انه قعد يلعب في firewall

و هذي هي الطريقة تشوف اللقوز و بناء عليها تعرف اذا فيه شي او لا

term.log

و يكون فيه اشياء حقت apt و اللي انت محملها ف نحط الملف في الاداة و نشوف

133	libgnome2-0 (2.22.0-0ubuntu1) ...
134	libbonoboui2-0 (2.21.90-1) ...
135	libgnomeui-0 (2.22.1.0-0ubuntu2) ...
136	firestarter (1.0.3-6ubuntu3) ...
137	nmap (4.53-3) ...
138	dpkg (1.14.16.6ubuntu4.1) ...
139	tzdata (2010h~repack-0ubuntu0.8.04) ...
140	libkrb53 (1.6.dfsg.3~beta1-2ubuntu1.4) ...
141	exim4-config (4.69-2ubuntu0.1) ...

ف نشوف ان nmap محمل بالجهاز ممكن يكون شي عادي عندك هذا يعتمد على الشغل اللي كان يصير على الجهاز ف مو شرط يعتبر شي ضار او خطير

daemon.log

	Mar 18 10:18:42 app-1 /etc/mysql/debian-start[7566]: mysql.user contains 2 root accounts without password!
	Mar 18 17:01:44 app-1 /etc/mysql/debian-start[14717]: mysql.user contains 2 root accounts without password!
	Mar 22 13:49:49 app-1 /etc/mysql/debian-start[5599]: mysql.user contains 2 root accounts without password!
	Mar 22 18:43:41 app-1 /etc/mysql/debian-start[4755]: mysql.user contains 2 root accounts without password!

هذا ملف تلاقي فيه اغلب اشياء services و لو نشوف mysql يعطي انذار ان فيه يوزرين root بدون باسوورد

الملخص

قدرت تحلل بعض ملفات logs في اللينكس و تعرف وش قاعد يصير بالجهاز طبعا فيه ملفات كثير غيرها و بنفس الملفات فيه اشياء ثانيه بس ماحبيت اطول المقالة اكثر من كذا و ان شاء الله تعجبكم