EMRECAN ATLIHAN

,

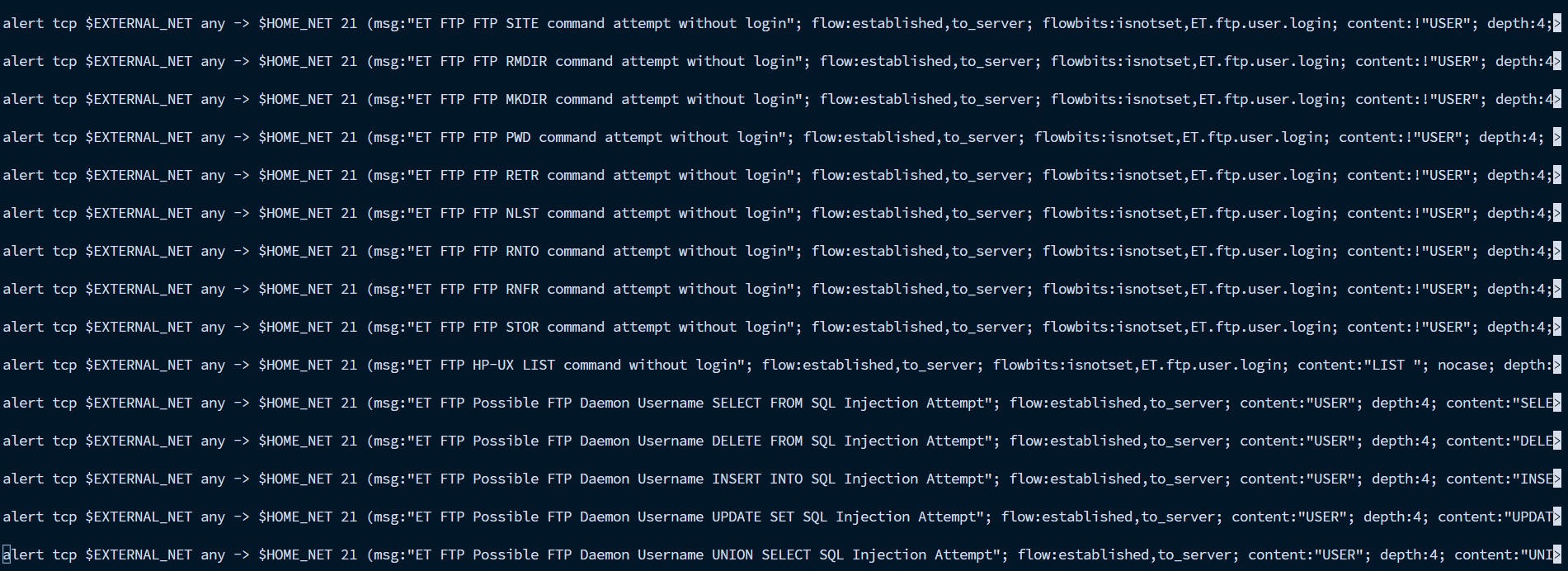
Wazuh üzerinde, FTP üzerinden yetkisiz dosya transferlerinin tespiti.

Wazuh üzerinde, Port tarama (Nmap) kullanımının tespiti.

Görev 2: Wazuh üzerinde, FTP üzerinden yetkisiz dosya transferlerinin tespiti.

VSFTPD Kurulumu:

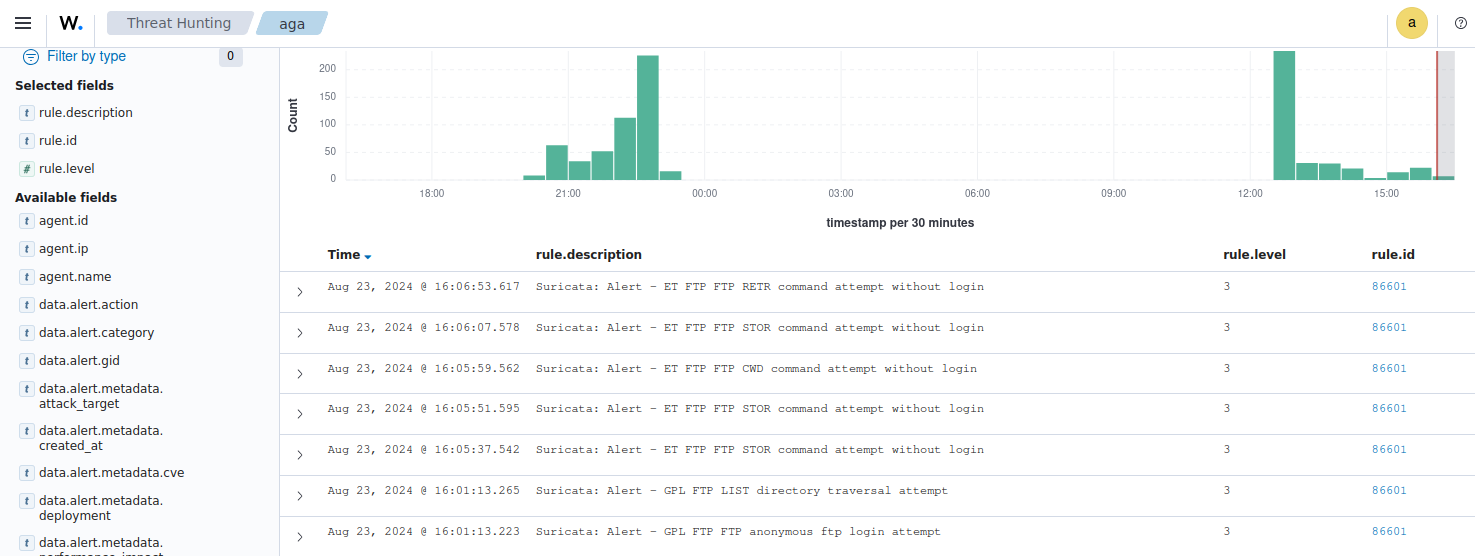
|  |
| --- |
| vsftpd (Very Secure FTP Daemon), Ubuntu sistemlerinde güvenli bir FTP sunucusu olarak yaygın şekilde kullanılmaktadır. İşte Ubuntu üzerinde vsftpd kurulumu ve yapılandırılması için adım adım bir kılavuz:    1. vsftpd Kurulumu  İlk olarak, vsftpd paketini yüklemek için terminalde aşağıdaki komutları kullanabilirsiniz:    sudo apt update  sudo apt install vsftpd  sudo apt update: Paket listelerini günceller.  sudo apt install vsftpd: vsftpd paketini yükler.  2. vsftpd Servisini Başlatma ve Etkinleştirme  Kurulum tamamlandıktan sonra, vsftpd servisini başlatabilir ve sistem açılışında otomatik olarak başlamasını sağlayabilirsiniz:    sudo systemctl start vsftpd  sudo systemctl enable vsftpd  sudo systemctl start vsftpd: vsftpd servisini başlatır.  sudo systemctl enable vsftpd: Servisin sistem açılışında otomatik olarak başlamasını sağlar.  3. vsftpd Konfigürasyonu  vsftpd yapılandırma dosyasını düzenlemek için şu komutu kullanın:    sudo nano /etc/vsftpd.conf  Bu dosyada yapılandırmak isteyebileceğiniz bazı önemli ayarlar şunlardır:    Anonim Erişim: Anonim FTP erişimini etkinleştirmek veya devre dışı bırakmak için:  anonymous\_enable=YES # Anonim erişimi etkinleştirir  anonymous\_enable=NO # Anonim erişimi devre dışı bırakır  Yerel Kullanıcı Erişimi: Yerel kullanıcıların FTP ile giriş yapabilmesini sağlamak için:    local\_enable=YES # Yerel kullanıcıların giriş yapmasına izin verir  Dosya Yükleme: Yerel kullanıcıların dosya yüklemesine izin vermek için:    write\_enable=YES # Dosya yüklemelerine izin verir  Chroot (Kapsama): Kullanıcıları sadece kendi dizinlerine kapatmak için:    chroot\_local\_user=YES # Kullanıcıları kendi dizinlerine kapatır  Güvenlik: Güvenliği artırmak için bazı ekstra ayarlar:    allow\_writeable\_chroot=YES # Yazılabilir kök dizinlerinde çalışmasına izin verir  Yapılandırma dosyasını düzenledikten sonra, değişikliklerin geçerli olması için vsftpd servisini yeniden başlatmanız gerekir:    sudo systemctl restart vsftpd  4. Güvenlik Duvarı Ayarları  Eğer bir güvenlik duvarı kullanıyorsanız, FTP trafiğine izin vermeniz gerekebilir:  sudo ufw allow from any to any 20,21,10000:10100 proto tcp  sudo systemctl status vsftpd  Bu komut, vsftpd servisinin durumunu gösterir  Oluşturduğum baba kullanıcısı için yarattığım komutlar  sudo adduser baba  mkdir /home/baba/ftp  chown nobody:nogroup /home/baba/ftp  chmod a-w /home/baba/ftp  mkdir /home/baba/ftp/upload  chown baba:baba /home/baba/ftp/upload  Anon olarak bağlandığımda dizinler çıkmıyordu. O yüzden user oluşturdum.  Linux makinemden şimdi ftp sunucusuna bağlanmayı deneyeceğim.      Suricata ruleslara bakarken ftp için rule olduğunu gördüm ve biraz inceledim. |

Kurallar yorum satırıyla kapatılmıştı ve anlama geldiğini gptye sordum.

RETR komutu, FTP protokolünde bir dosyayı sunucudan indirmek için kullanılır

STOR komutu, FTP protokolünde bir dosyayı sunucuya yüklemek için kullanılır ve bu komutun genellikle bir giriş işlemi yapıldıktan sonra gönderilmesi beklenir.

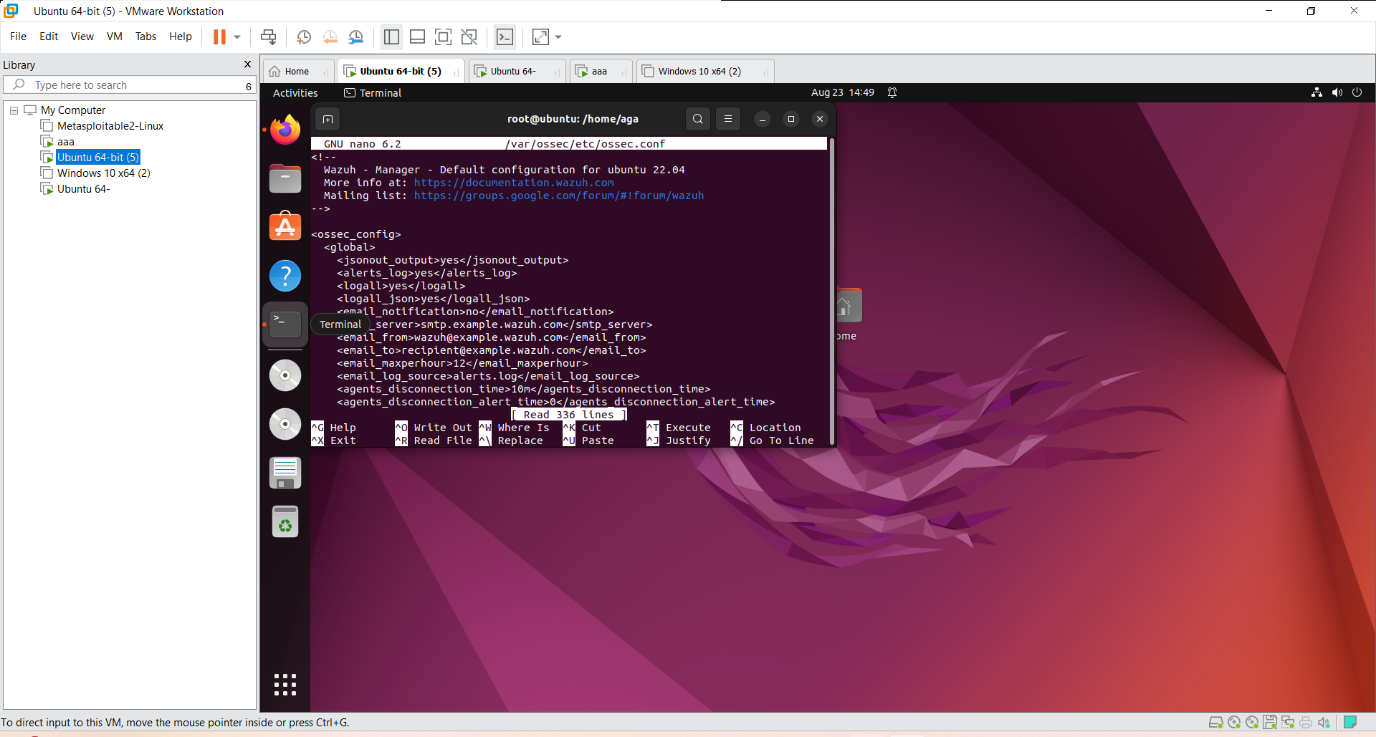
Sizin istediğinizi tam yapamadım ama kullanıcı giriş yaptığında ve dosya yüklediğinde kendi bilgisayarına dosya indirdiğinde uyarı düşüyor.



Görev 3: Nmap kullanım tespiti

İlk olarak kurulum kısmını ve agent bağlama kısmını atlıyorum. Agentim Ubuntu Live Server manager ise Ubuntu.

İlk olarak manager dosyasındaki conf dosyasından tüm logların gelmesini sağlamak için belli başlı komutları değiştirdim.

<logall>yes</logall> <logall\_json>yes</logall\_json>

Ikisi de no idi.

IDS SURICATA KURULUMU:

Nmap taramasını yakalayabilecek rules yazamadığım için hintli abimizin gösterdiği suricatayı kullandım. IDS engine’ler tek başına bir şey yapamaz bunu bizim kendimiz düzenlememiz gerekiyor.

Başlangıç olarak:

sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt-get update

sudo apt-get install suricata –y

Devamında:

cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz

sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/\*.rules /etc/suricata/rules/

sudo chmod 640 /etc/suricata/rules/\*.rules

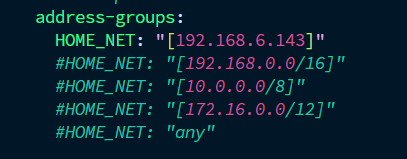
Suricatanın içinde rules diye directory olmayabilir bunu kendiniz yaratmalısınız.

Ve en son olarak

/etc/suricata/suricata.yaml dosyasını konfigre etmeniz lazım.

HOME\_NET: "<UBUNTU\_IP>" ------> bu kısıma agentin ipsi

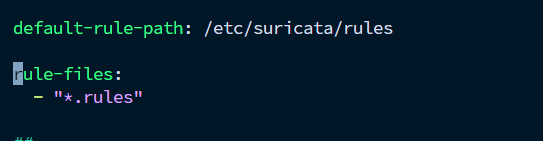
EXTERNAL\_NET: "any"



default-rule-path: /etc/suricata/rules

rule-files:

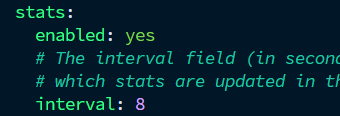
- "\*.rules"



# Global stats configuration

stats:

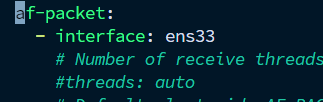
enabled: Yes



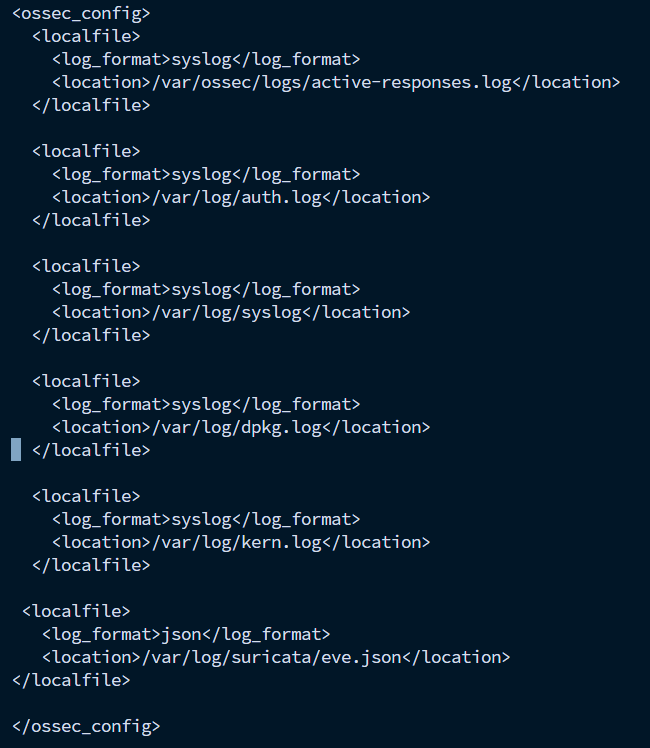
# Linux high speed capture support

af-packet:

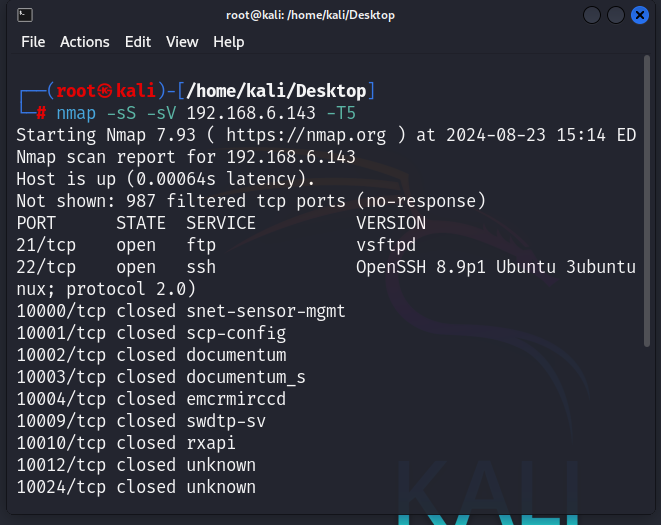
- interface: eth0 --------> ifconfig attığınızda ipniz yanında yazan kısım



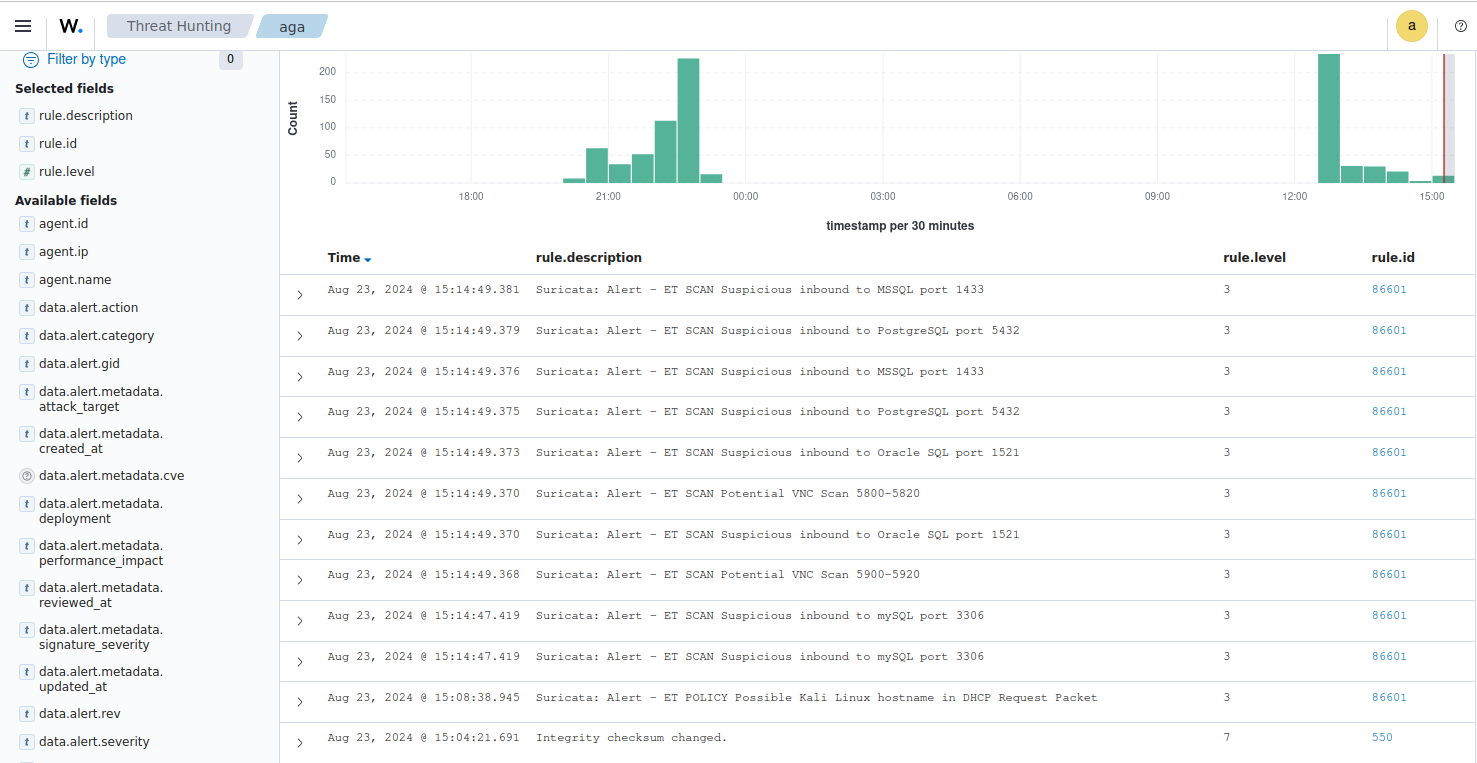
Daha sonra bunu wazuha config etmemiz gerekiyor. Bu neyin configi peki? Ossec.cof dosyasının için bir kısımda wazuhun izleyeceği logları belirliyebiliyorsunuz. Biz de en sondaki kodu ekliyoruz. Suricatanın içinde başka türlü log dosyaları da var.



Ayarlarımızı yaptıktan sonra NMAP saldırısını deneyelim ve sonuçları görelim.



Şimdi manager sayfasına bakalım.



Daha detaylı bakalım.

