Malware Event Logging (MEL)
Zərərverici Proseslərinin Loglaşdırılması

MEL zərərli proqram təminatlarını təhlükəsiz rejimdə (VM) analizini avtomatik şəkildə həyata keçirmək üçün hazırlanmışdır. Sistem guest-host əsaslı fəaliyyət göstərir. Bundan əlavə olaraq da sistemin fəaliyyəti üçün bəzi 3-cü tərəf proqram təminatlarının yazılması şərtdir.

MEL-in hazırlanmasında əsas məqsəd Azərbaycanda bu sahəyə olan marağı artırmaq və bu sahəyə dəstək olmaq üçün bu sahədə yeni fəaliyyətə başlamış mütəxəssisləri ilkin analiz vasitələri ilə təmin etməkdir.

Bildiyimiz kimi zərərvericilərin tətqiqində dinamik analiz vacib yer tutur. Analitiklər ilk öncə dinamik analiz ilə zərərvericilərin sistemdə etdikləri dəyişiklikləri təyin edirlər. Bəzən bunun üçün çox uzun vaxt lazım olur. MEL isə bu işdə sizə yardımçı olaraq avtomatik dinamik analiz üçün lazımı şəraiti yaradacaq.

Yuxarıda qeyd etdiyimiz kimi sistem 2 tərəfli işləyir:
Guest hissəsi (Virtual maşında)
Host hissəsi isə (Virtual maşının işlədiyi sistemdir).
Beləliklə zərərverici guest tərəfdə yani virtual maşında fəaliyyət göstərəcək.

Xatırladaq ki, sistemi hər bir şəxs öz fərdi komputerinə qura bilər və beləliklə dinamik analiz üçün öz ilkin labaratoriyasına sahib ola bilər.

Köməkçi proqram təminatları:

1. ***CaptureBat***
(Zərərvericilərin sistemdə etdiyi dəyişiklikləri qeydə alan kernel seviyyəsində fəaliyyət göstərən və açıq kodlu program) https://www.honeynet.org/node/315
2. ***Windump***
(Zərərvericilərin network əlaqələrini yaxalamaq üçün tcpdump əsaslı network sniffer) *https://www.winpcap.org/windump/*
3. ***Clamwin***
(clamav-engine açıq kodlu (open source) virus scan proqram təminatı) http://www.clamwin.com/
4. ***Avira command line virus scanner***
https://www.avira.com/en/download/product/avira-command-line-scanner-scancl

Sistem 2 tərəfli əlaqəni socket üzərindən qurur.

Daha öncə qeyd etdiyimiz kimi MEL-in əsas məqsədi görüləcək işləri avtomatlaşdırmaqdır. Guest tərəfində əsas fəaliyyət göstərən hissə Agent-dir. Məhz bu modul qarşı(host) tərəfdən lazımi nümunə faylı qəbul edir və analizə start verir. Agent sistemin işləməsi haqqında məlumatları qarşı(host) tərəfdə olan Event ilə socket üzərindən paylaşır.

Əsas iş ardcılığı belədir:

1.Host tərəfdə olan Event.py işə salınır.
   a)Event öz növbəsində Virtual sistemi avtomatik olaraq işə salır.
   b)İstifadəçı VM-də Agent.py-ı işə salır.
2.Host tərəfdə submit.py-ın köməkliyi ilə sample qarşı tərəfə göndərilir.
   a)Agent.py sample faylı qəbul edir və işə başlayır.
   b)Bütün məlumatlar host tərəfdə Event.py pəncərəsində göstərilir.

Agent.py ilk öncə fayl haqqında məlumat toplayır(c:\\logs).
   1.fayl antivirus filterdən keçir.(Clamav,Avira) təyin edilərsə (hər hansı biri tərəfindən) əməliyyat dayandırılır, əks təqdirdə növbəti addımlar həyata keçirilir.

   2.fayl haqqında aşağıdakı məlumatlar toplanılır.
      md5,sha1,filesize,ssdeep_digest

   3.Pe faylı parse edilir(Limit pe sectionlara qədər)
   4.İzlənmə üçün proqram təminatları(Windump,CaptureBat) işə salınır.
   5.Sample faylı işə salınır.
   6.Process modulları extract edilir.
   7.Proses sonlana qədər vəya TİMEOUT bitənə qədər gözlənilir 2 əməliyyatdan biri həyata keçərsə loglar toplanılır və qarşı(host) tərəfə göndərilir.

Əməliyyat sistemləri (Windows platforms):
Host tərəf Windows XP, Windows 7 əməliyyat sistemlərini dəstəkləyir.
Guest tərəf Windows XP SP3 üzərində tam test edilib və məsləhət görülür.

VM olaraq VirtualBox-a uyğunlaşdırlıb.

İlk olaraq verilmiş qovluğu yükləməlisiniz. Tərkibində lazımı bütün köməkçi proqram təminatlarının quraşdırma faylları (setup) mövcuddur. Qovluğu (guest) tərəfdə arxivdən çıxarın (unpack) və PT-ləri quraşdırın (install), standart (defaoult) quraşdırma zamanı heç bir dəyişikliyə ehtiyac yoxdur.

Lakin quraşdırma standart olmadığı təqdirdə -> guest\lib\ qovluğundakı aşağıdakı scriptlərdə dəyişiklik etməlisiniz.

```
##########################################################################################
    Bu pathları etdiyiniz install əməliyyatına uyğun olaraq dəyişin.

    trapping.py
    Function __init__

    #windump executable path
    self.__windump = "C:\\Program Files\\windump\\windump.exe"
    #CaptureBat executable path
    self.__CaptureBat = "C:\\Program Files\\Capture\\CaptureBat.exe"
    ##########################################################################
    av.py
    Function clamav
    #clamscan executable path
    clampath = "C:\\Program Files\\ClamWin\\bin\\clamscan.exe"

    Function avira
    #Avira commandline executable path
    avirapath = "C:\\Program Files\\Avira\\scancl.exe"
```

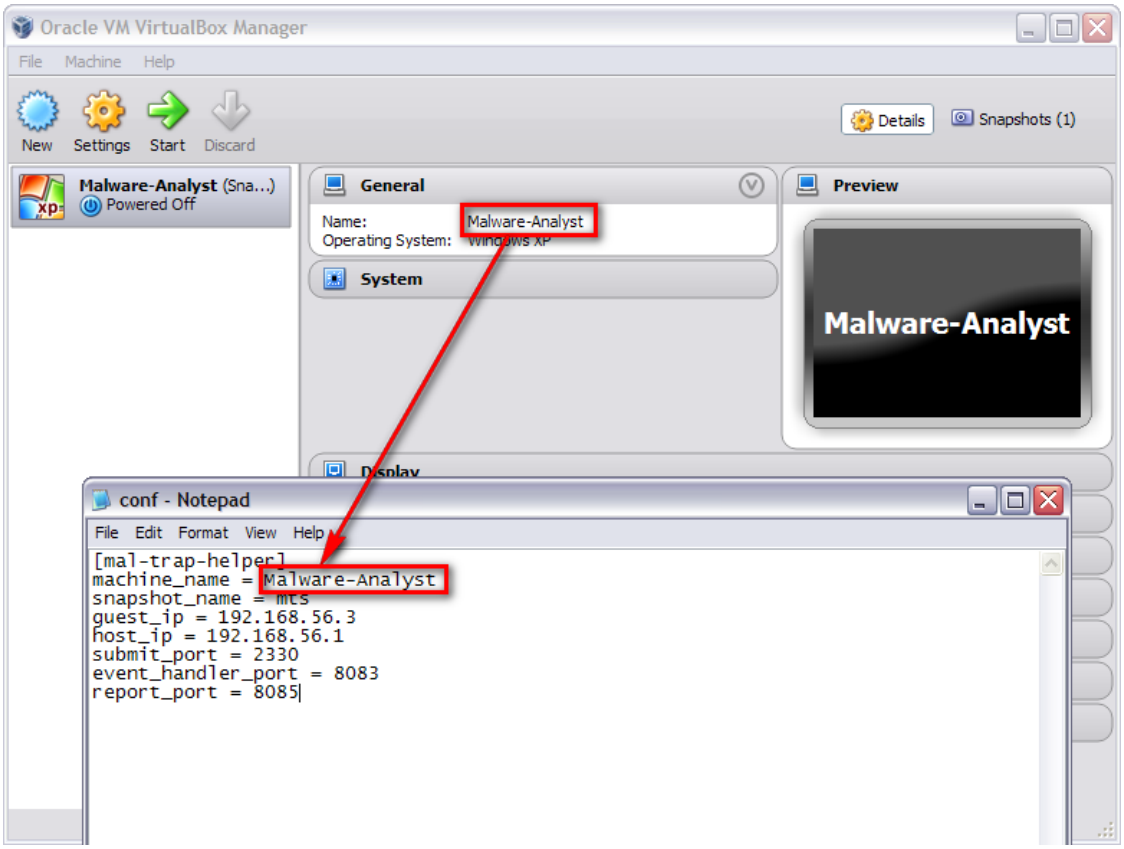
SAZLAMALAR

Hər iki tərəfdədə config qovluğu tərkibində isə conf.txt faylı mövcuddur.

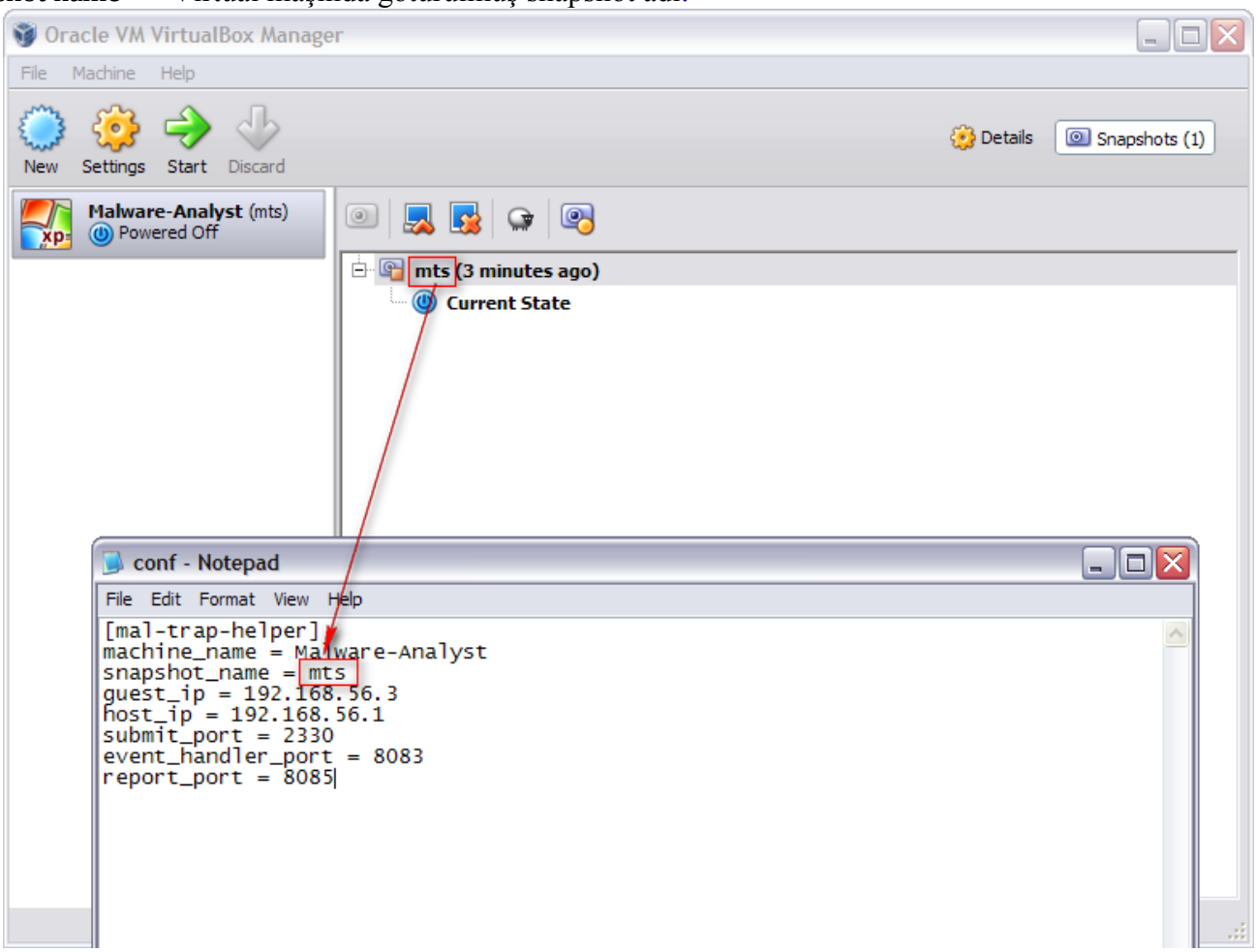
HOST

HOST tərəfində olan conf.txt faylının tərkibində bu dəyişiklikləri etməlisiniz.

machine name => VirtualMaşının(GUEST) işlədiyi maşının adı.



snapshot name => Virtual maşında götürülmüş snapshot adı.



Portlarda problem yaranmadığı təqdirdə dəyişiklik etməmək məsləhət görülür.
guest_ip => Qarşı tərəfin ip ünvanı (VM)
host_ip = > Cari host tərəfin ip ünvanı.
ipconfig əmrindən istifadə edə bilərsiniz.

GUEST

GUEST tərəfində olan conf.txt faylının tərkibində
agent_ip => Agent.py -ın işlədiyi ip
host_ip host tərəfin ip ünvanı
ipconfig əmrindən istifadə edə bilərsiniz.

LOGLAŞDIRMA

log fayllarına log qovluğunda (c:\\logs\\) heç bir dəyişiklik etməmək şərtı ilə istədiyiniz adı verə bilərsiniz.

Bizimlə əlaqə / Bug Report: malware_lab@cert.gov.az
Web: http://www.cert.gov.az