



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего  
образования

**РТУ МИРЭА**

**«МИРЭА – Российский технологический университет»**

---

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

---

Практическая работа № 8

«Матрица уязвимостей MITRE ATT&CK. Тактика: Выполнение.»

по дисциплине «Безопасность операционных систем»

Москва

2023

## 1. Выполнение

Выполнение (Execution) применение злоумышленниками средств и методов удаленного и локального выполнения в атакуемой системе различных команд, сценариев и исполняемых файлов, которые были доставлены в неё на предыдущем этапе. Набор техник:

T1204 Выполнение с участием пользователя

T1053 Запланированная задача (задание)

T1047 Инструментарий управления Windows

T1059 Использование интерпретаторов командной строки и сценариев

T1559 Межпроцессное взаимодействие

T1106 Нативный API

T1129 Общие модули

T1569 Системные службы

T1072 Средства развертывания ПО

T1203 Уязвимости в клиентском ПО

Для выполнения практической работы понадобятся виртуальные машины, которые мы настроили на прошлом практическом занятии:

1. Сервер SIEM-системы Wazuh
2. Kali с установленным wazuh-агентом
3. Windows с установленным wazuh-агентом

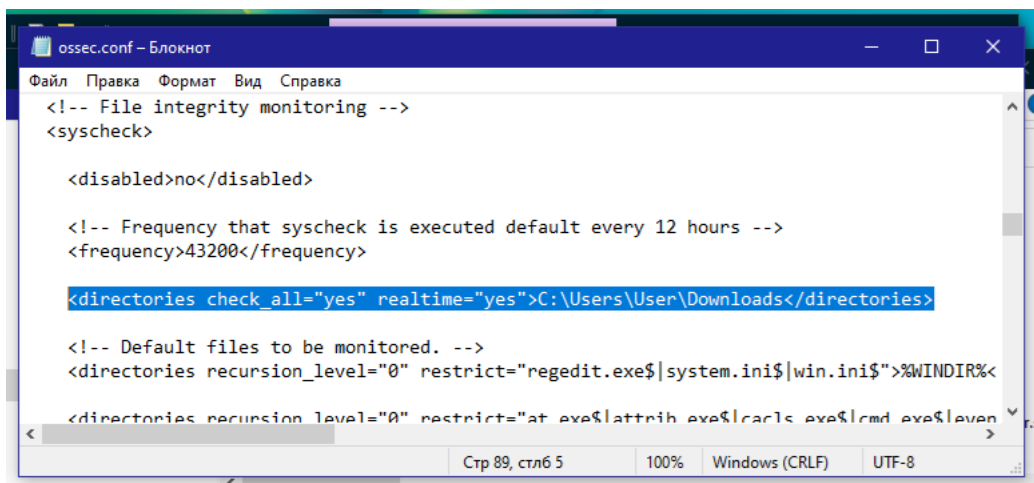
На прошлой практике мы рассматривали тактику получения первоначального доступа, с помощью техники целевого «фишинга» с вредоносным вложением. Таким образом мы попали на целевой хост и дальнейшие наши действия будем рассматривать с этого места.

## 1 Выполнение с участием пользователя. Вредоносный файл.

T1204 выполнение с участием пользователя предполагает активное участие пользователя либо для перехода по вредоносной ссылке (T1204.001), либо запуска вредоносного файла или скрипта (T1204.002).

Давайте рассмотрим технику T1204.002 на примере созданного вами самораспаковывающегося архива, который запускает командный интерпретатор powershell. У меня этот архив называется *ps.exe*, он лежит в директории *C:\Users\user\Download* эту директорию будем считать рабочей директорией для всех новых файлов, попадающих на ОС (собственно так оно и есть, ведь по умолчанию все загружаемые из интернета файлы попадают в неё). Переместите файл *ps.exe*, например, на рабочий стол, в дальнейшем будет понятно зачем мы это сделали. На прошлой практике мы настроили мониторинг запуска архивов, выполняющих подозрительные действия. На этот раз настроим мониторинг, таким образом, чтобы SIEM предупреждал нас о попадании на хост известных вредоносных файлов. В этом нам поможет модуль FIM (file integrity monitoring), познакомьтесь с его возможностями самостоятельно. Добавим в конфигурационный файл агента в раздел `<syscheck>` блок для контроля за рабочей директорией:

```
<directories check_all="yes"
realtime="yes">C:\Users\User\Downloads</directories>
```



Теперь перезапустим агента wazuh на VM Windows.

Проведем настройку сервера wazuh. Wazuh определяет является ли файл вредоносным по хэш-сумме файла посчитанной по алгоритму MD5, который хранится в специальном файле-списке в формате *ключ:значение* (подробнее

с файлами-списками можно ознакомиться [здесь](#)). Создадим такой файл в директории `/var/ossec/etc/lists/malware-hashes` и добавим в него данные вредоносных файлов:

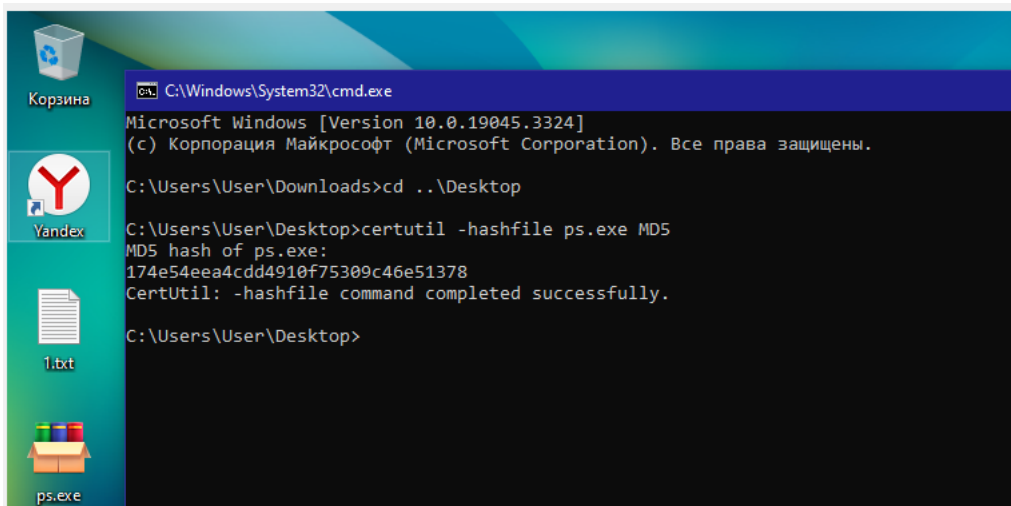
```
e0ec2cd43f71c80d42cd7b0f17802c73:mirai
```

```
174e54eea4cdd4910f75309c46e51378:test-malware
```

`mirai` это вредоносный файл, который добавляет хост в бот-сеть, для дальнейшей эксплуатации во вредоносных кампаниях. На сайте [virustotal.com](http://virustotal.com) можно проверить его хэш и убедиться, что он принадлежит «очень плохому файлу».

`Test-malware` это мой файл `ps.exe` и его хэш полученный командой:

`certutil -hashfile ps.exe MD5`, вычислите хэш-сумму своего «подопытного» файла:

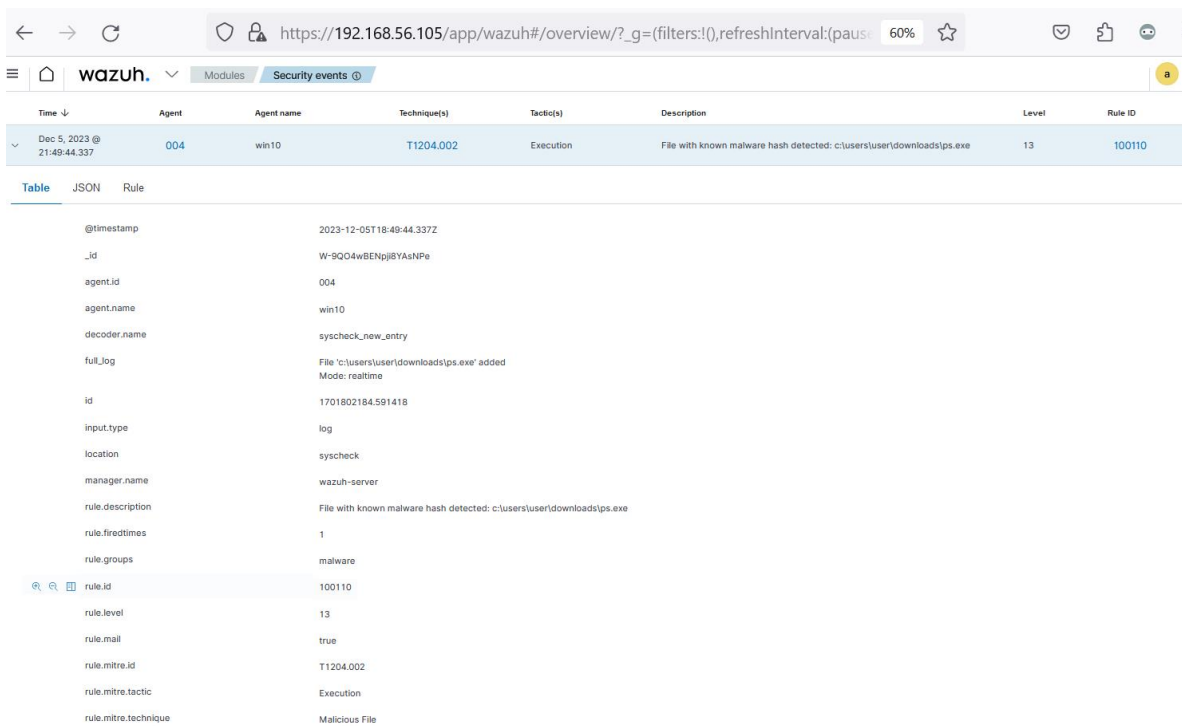


Далее добавим путь до файла с хэшами в конфигурационный файл сервера `wazuh /var/ossec/etc/ossec.conf` в раздел `<ruleset>`:

```
<list>etc/lists/malware-hashes</list>
```

```
root@wazuh-server:~  
GNU nano 2.9.8 /var/ossec/etc/ossec.c  
  
<log_format>full_command</log_format>  
<command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:d  
<alias>netstat listening ports</alias>  
<frequency>360</frequency>  
</localfile>  
  
<localfile>  
<log_format>full_command</log_format>  
<command>last -n 20</command>  
<frequency>360</frequency>  
</localfile>  
  
<ruleset>  
<!-- Default ruleset -->  
<decoder_dir>ruleset/decoders</decoder_dir>  
<rule_dir>ruleset/rules</rule_dir>  
<rule_exclude>0215-policy_rules.xml</rule_exclude>  
<list>etc/lists/audit-keys</list>  
<list>etc/lists/amazon/aws-eventnames</list>  
<list>etc/lists/security-eventchannel</list>  
<list>etc/lists/malware-hashes</list>
```

Теперь перезапустим менеджер wazuh на ВМ Wazuh. Перейдем в ВМ Windows и скопируем (теперь уже вредоносный) файл *ps.exe* в директорию *C:\Users\user\Downloads*.



Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Dec 5, 2023 @ 21:49:44.337	004	win10	T1204.002	Execution	File with known malware hash detected: c:\users\user\downloads\ps.exe	13	100110

Table	JSON	Rule
@timestamp		2023-12-05T18:49:44.337Z
_id		W-9Q04wBENpj8YAANPe
agent.id		004
agent.name		win10
decoder.name		syscheck_new_entry
full_log		File 'c:\users\user\downloads\ps.exe' added Mode: realtime
id		1701802184.591418
input.type		log
location		syscheck
manager.name		wazuh-server
rule.description		File with known malware hash detected: c:\users\user\downloads\ps.exe
rule.firedtimes		1
rule.groups		malware
rule.id		100110
rule.level		13
rule.mail		true
rule.mitre.id		T1204.002
rule.mitre.tactic		Execution
rule.mitre.technique		Malicious File

На «дашборде» *security events* должно появиться событие безопасности с уровнем угрозы 13.

**Отчет:**

1. Напишите в отчет возможности модуля FIM.
2. Добавьте в отчет «скриншот» с листингом созданного файла-списка, содержащего посчитанный Вами хэш.
3. Напишите в отчет, что можно контролировать с помощью CDB файл-списков.
4. Обойдите настроенную нами систему оповещения о появлении вредоносного файла в контролируемой директории. Используйте тот же самораспаковывающийся архив, запускающий командный интерпретатор *powershell*.