



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий (ИКБ)

КБ-2 «Информационно-аналитические системы кибербезопасности»

ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №10

**В РАМКАХ ДИСЦИПЛИНЫ «ПРИНЦИПЫ ПОСТРОЕНИЯ,
ПРОЕКТИРОВАНИЯ И ЭКСПЛУАТАЦИИ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

The screenshot shows the MaxPatrol 10 interface with the following details:

- Top Bar:** pt MaxPatrol 10, Events, System.
- Left Sidebar:**
 - Groups: All events, Unlinked, All assets (selected), Unmanaged hosts.
 - Filters: All events (selected), System filters, BAD-based analytics, BAD dashboards, Highest risk sc..., Count of proce..., Processes with...
- Central Area:**
 - Filter bar: Filter: All events * object.account.name = "b_rivers_admin" & action= "elevate".
 - List of events:
 - 11/23/22, 12:49:57 comp-2159.hv-logistics.stf The user b_rivers_admin with the administrator equivalent special rights logged in to host comp-2159.hv-logistics.stf
 - 11/23/22, 12:49:57 comp-2159.hv-logistics.stf The user d_jensen attempted to log in to host comp-2159.hv-logistics.stf with explicit b_rivers_admin privileges to b_rivers_admin on host comp-2159.hv-logistics.stf
 - 11/23/22, 12:49:57 comp-2159.hv-logistics.stf The user d_jensen escalated privileges to b_rivers_admin on host comp-2159.hv-logistics.stf
 - 11/23/22, 12:49:57 comp-2159.hv-logistics.stf The user d_jensen escalated privileges to b_rivers_admin on host comp-2159.hv-logistics.stf
 - 11/23/22, 12:49:57 comp-2159.hv-logistics.stf The user b_rivers_admin with the administrator equivalent special rights logged in to host comp-2159.hv-logistics.stf
 - 11/23/22, 12:49:57 comp-2159.hv-logistics.stf The user d_jensen is authenticated as the user b_rivers_admin on host comp-2159.hv-logistics.stf
- Bottom:** Total 128 events, 1 selected.

Рисунок 1 - Первый фильтр

The screenshot shows the MaxPatrol 10 interface with the following details:

- Top Bar:** pt MaxPatrol 10, Events, System.
- Left Sidebar:**
 - Groups: All events, Unlinked, All assets (selected), Unmanaged hosts.
 - Filters: All events (selected), System filters, BAD-based analytics, BAD dashboards, Highest risk sc..., Count of proce..., Processes with...
- Central Area:**
 - Filter bar: Filter: All events * object.account.name = "b_rivers_admin" & action= "elevate" time (oldest on top).
 - List of events:
 - 11/23/22, 12:40:09 comp-1095.hv-logistics.stf account elevate process failure on host comp-1095.hv-logistics.stf
 - 11/23/22, 12:40:09 comp-1095.hv-logistics.stf account elevate process failure on host comp-1095.hv-logistics.stf
 - 11/23/22, 12:41:48 comp-2159.hv-logistics.stf The user d_jensen attempted to log in to host comp-2159.hv-logistics.stf
 - 11/23/22, 12:41:48 comp-2159.hv-logistics.stf The user d_jensen escalated privileges to b_rivers_admin on host comp-2159.hv-logistics.stf
 - 11/23/22, 12:41:48 comp-2159.hv-logistics.stf The user d_jensen escalated privileges to b_rivers_admin on host comp-2159.hv-logistics.stf
 - 11/23/22, 12:41:48 comp-2159.hv-logistics.stf The user b_rivers_admin with the administrator equivalent special rights logged in to host comp-2159.hv-logistics.stf
 - 11/23/22, 12:41:48 comp-2159.hv-logistics.stf The user d_jensen attempted to log in to host comp-2159.hv-logistics.stf
 - 11/23/22, 12:41:48 comp-2159.hv-logistics.stf The user d_jensen escalated privileges to b_rivers_admin on host comp-2159.hv-logistics.stf
 - 11/23/22, 12:41:48 comp-2159.hv-logistics.stf The user d_jensen escalated privileges to b_rivers_admin on host comp-2159.hv-logistics.stf
 - Right Panel:**
 - Event details: 11/23/22, 12:41:48. The user d_jensen escalated privileges to b_rivers_admin on host comp-2159.hv-logistics.stf.
 - Request additional data:
 - Subject: d_jensen hv-logistics... (selected)
 - Action: elevate
 - Object: b_rivers_admin hv-lo...
 - Status: success
 - Source: 1792c8d6-2380-0001-0...
 - Destination: 1792c8d6-2380-0001-0...
 - Source: 1792c8d6-2380-0001-0...

Рисунок 2 - повышение привилегий

Heavy Logistics (2022) Низкий уровень сложности
Небезопасное хранение данных / Задание 7.1
100 баллов получено

Задание

В транспортной компании Heavy Logistics проблемы с выполнением требований парольной политики и с надежным хранением аутентификационных данных.

Однажды администратор Boyd Rivers оставил файл с паролем своей доменной учетной записи (b_rivers_admin) на компьютере одного из эйчаров: забыл удалить его после настройки. В результате фишинговой атаки злоумышленники получили доступ к устройству эйчара, нашли этот файл и воспользовались данными для повышения привилегий (23 ноября 2022 года с 09:30 по 09:50 UTC).

Укажите имя рабочей станции эйчара, на которой хранится файл с паролем.

Тактики, техники и подтехники атак по MITRE ATT&CK

- TA0006. Получение учетных данных | T1552. Незащищенные учетные данные | T1552.001. Учетные данные в файлах

Средства защиты

MaxPatrol SIEM

Принятый ответ Дата и время проверки
comp-2159.hv-logistics.stf 29 октября, 16:55

Рисунок 3 - первый ответ

The screenshot shows the MaxPatrol 10 interface. On the left, there's a sidebar with 'Groups' (All events, Unlinked, All assets, Unmanaged hosts), 'Filters' (All events, System filters, BAD-based analytics, BAD dashboards, Highest risk score, Count of processes, Processes with...), and a search bar. The main area displays a list of events with columns: event_src.host, object.path, object.hash, object.account.name, object.account.domain, count.fullname, jnt.session_id, jct.account.id, jct.account.name, jct.process.name, jct.process.path, s.original_na..., process.fullpath, process.cmdline, object.process.guid, object.process.id, object.process.hash, object.process.version, object.process.cwd, object.process.parent.name, cmd.exe, object.process.parent.path, object.process.parent.fullp... . A filter bar at the top says 'Filter: All events *' and has a dropdown for 'event_src.host = "comp-2159.hv-logistics.stf"'. Below the filter is a 'Change' button. The bottom of the screen shows a summary: 'Total 22 events, 1 selected'.

Рисунок 4 - второй фильтр

»	📅 11/23/22, 12:41:22	⋮
object.path	c:\users\d_jensen\documents\	▲
object.hash	340CC46BA058C2E554AF2431ADA7FB242AC7B6C6...	⋮
object.account.name	d_jensen	▲
object.account.domain	hv-logistics.stf	⋮
object.account.fullname	d_jensen@hv-logistics	▲
object.account.session_id	1342507	⋮
object.account.id	S-1-5-21-794427356-1309637812-1474570248-1152	▲
object.process.name	runascs_net2.exe	⋮
object.process.path	c:\users\d_jensen\documents\	▲
object.process.original_na...	RunasCs_net2.exe	⋮
object.process.fullpath	c:\users\d_jensen\documents\runascs_net2.exe	▲
object.process.cmdline	RunasCs_net2.exe B_Rivers_admin -p zY2oWqz2qn3Ne 71W -d hv-logistics.stf	⋮
	▲ Collapse	▼
object.process.guid	076CA06C-EAC2-637D-481E-000000003100	
object.process.id	5468	
object.process.hash	SHA256:340CC46BA058C2E554AF2431ADA7FB242A...	
object.process.version	0.0.0.0	
object.process.getcwd	C:\Users\D_Jensen\Documents\	
object.process.parent.name	cmd.exe	
object.process.parent.path	c:\windows\system32\	
object.process.parent.fullp...	c:\windows\system32\cmd.exe	

Рисунок 5 - пароль администратора

Heavy Logistics (2022) Низкий уровень сложности

Небезопасное хранение данных / Задание 7.2

100 баллов получено

Задание

В транспортной компании Heavy Logistics проблемы с выполнением требований парольной политики и с надежным хранением аутентификационных данных.

Однажды администратор Boyd Rivers оставил файл с паролем своей доменной учетной записи (b_rivers_admin) на компьютере одного из эйчаров: забыл удалить его после настройки. В результате фишинговой атаки злоумышленники получили доступ к устройству эйчара, нашли этот файл и воспользовались данными для повышения привилегий (23 ноября 2022 года с 09:30 по 09:50 UTC).

Приведите пароль учетной записи b_rivers_admin.

Тактики, техники и подтехники атак по MITRE ATT&CK

- TA0004. Повышение привилегий | T1078. Существующие учетные записи | T1078.002. Доменные учетные записи

Средства защиты

MaxPatrol SIEM

Принятый ответ
zY2oWqz2qn3Ne71W

Дата и время проверки
29 октября, 17:12

Рисунок 6 - второй ответ

The screenshot shows the MaxPatrol SIEM interface with the following details:

- Event Details:** Event ID: 11/22/22, 20:25:09, Host: comp-2159.hv-logistics.stf, Account: account_s.
- Event Properties:**
 - event_src.host = "comp-2159.hv-logistics.stf"
 - event_src.category = Other
 - origin_app_id = 177a7e61-c000-0001-0000-000000000003
 - primary_siem_app_id = 177a7e61-c000-0001-0000-000000000003
 - storage_app_name = MaxPatrol 10
 - storage_app_alias = MP-1
 - storage_app_id = 1ab005a0-9100-0001-0000-000000000004
- Filter Bar:** Shows a complex filter query: event_src.host = "comp-2159.hv-logistics.stf" and object.process.parent.cmdline contains ":\\Attachments" and (object.process.parent.cmdline contains ".doc" or object.process.parent.cmdline contains ".xls") and action = "start" and subject.account.name = "d_jensen" and object.process.parent.cmdline not contains ".doc" and object.process.parent.cmdline not contains "wiword.exe".
- Left Sidebar:** Groups, All assets (selected), Unmanaged hosts.
- Bottom Navigation:** Events for November 22, 2022-24, All assets.

Рисунок 7 - третий фильтр

MaxPatrol 10

Events for November 22, 2022–24

Filter: All events *

Additional information:

- action: start
- status: success
- datafield1: 1342507
- datafield2: 2120
- datafield3: c:\windows\system32\
- datafield4: cmd.exe
- datafield5: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /dde
- datafield6: 076CA06C-84D3-637B-2B7C-140000000000
- datafield7: 1342507
- datafield8: 076CA06C-05F5-637D-3F14-000000003100
- datafield9: C:\Windows\System32\cmd.exe /c "start C:\Attachments\ts76bcf5a5e7b44630b01b9821db94c360book_withcob.xls"
- datafield10: excel.exe -- cmd.exe -- checker.exe -- checker.exe -- ..
- msgid: 1

Event source: event_src.host comp-2159.hv-logistics.stf

Рисунок 8 - найденный файл

CYBERBONES Бесплатная версия

Heavy Logistics (2022) Низкий уровень сложности

Небезопасное хранение данных / Задание 7.3

100 баллов получено

Задание

В транспортной компании Heavy Logistics проблемы с выполнением требований парольной политики и с надежным хранением аутентификационных данных.

Однажды администратор Boyd Rivers оставил файл с паролем своей доменной учетной записи (b_rivers_admin) на компьютере одного из юзеров: забыл удалить его после настройки. В результате фишинговой атаки злоумышленники получили доступ к устройству юзера, нашли этот файл и воспользовались данными для повышения привилегий (23 ноября 2022 года с 09:30 по 09:50 UTC).

Укажите имя файла из фишинговой рассылки, открытие которого привело к развитию атаки.

Тактики, техники и подтехники атак по MITRE ATT&CK

- TA0001. Первоначальный доступ | T1566. Фишинг | T1566.001. Целевой фишинг с вложением

Средства защиты

MaxPatrol SIEM

Принятый ответ book_withcob.xls Дата и время проверки 29 октября, 17:39

Рисунок 9 - третий ответ