ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ CCTV ОБОРУДОВАНИЯ

Цель:
Обнаружение, получение доступа к настройкам, сетевой адресации, видеопотоку в реальном времени, записям видеоархива.

Обнаружение CCTV оборудования в сети:

Используемые порты и протоколы по умолчанию:

- HTTP (Hypertext Transfer Protocol):

Порт: 80 (обычно используется для незащищенного HTTP) или 8080.

- HTTPS (Hypertext Transfer Protocol Secure):

Порт: 443 (обычно используется для защищенного HTTPS).

- RTSP (Real-Time Streaming Protocol):

Порт: 554 (обычно используется для передачи видеопотока в реальном времени).

- RTMP (Real-Time Messaging Protocol):

Порт: 1935 (обычно используется для потоковой передачи видео в реальном времени).

- ONVIF (Open Network Video Interface Forum):

Порт: 8000, 8899, 6688 (обычно используется для коммуникации с устройствами, поддерживающими стандарт ONVIF).

- FTP (File Transfer Protocol):

Порт: 21 или 20 (21 используется для установки соединения, 20 для передачи данных).

- SSH (Secure Shell):

Порт: 22 (обычно используется для удаленного доступа к устройству по шифрованному соединению).

- Telnet:

Порт: 23 (обычно используется для удаленного управления устройством).

- DVR-IP, NetSurveillance, Sofia

Порт: TCP 34567 и UDP 34568 (используется компонентом NETSurveillance ActiveX)

Стандартные сетевые параметры оборудования

Вендор	Стандартный IP	Логин/Пароль
Hikvision	192.0.0.64	Логин: admin Пароль: 12345
Dahua	192.168.1.108	Логин: admin Пароль: admin, 888888, 666666, 123456
Axis	192.168.0.90	Логин: root Пароль: pass
Honeywell	192.168.1.10	Логин: admin Пароль: 1234
Avigilon	192.168.1.100	Логин: admin Пароль: admin
FLIR	192.0.0.30	Логин: admin Пароль: admin
Arecont Vision	192.168.1.20	Логин: admin Пароль: без пароля
GeoVision	192.0.0.205	Логин: admin Пароль: admin
ACTi	192.168.0.100	Логин: admin Пароль: 123456
Panasonic	192.168.0.253	Логин: admin Пароль: password
Bosch	192.168.0.1	Логин: admin Пароль: admin

Полный перечень стандартных настроек:
https://www.ispyconnect.com/userguide-default-passwords.aspx

Синтаксис поискового запроса для Shodan:

Пример поискового запроса:
product:"IP Camera" city:”NewYork" has_screenshot:true -"admin login" port:554 os:"Linux" org:"Hikvision" country:”US”

В этом примере мы используем несколько операторов для уточнения поиска:

- product:"IP Camera" - фильтр, указывающий на конкретный продукт или устройство. В данном случае мы ищем устройства с продуктом "IP Camera".
- city:"NewYork " - фильтр, используемый для ограничения поиска по городу. В данном случае мы ищем устройства, находящиеся в городе "Москва".
- has_screenshot:true - фильтр, указывающий, что мы ищем устройства, для которых доступны скриншоты.
- -"admin login" - оператор "-" используется для исключения определенных слов или фраз из результатов поиска. В данном случае мы исключаем устройства, в которых встречается фраза "admin login".
- port:554 - фильтр, указывающий на конкретный порт. В данном случае мы ищем устройства, использующие порт 554, который часто связан с протоколом RTSP для видеопотоков.
- os:"Linux" - фильтр, указывающий на операционную систему устройства. В данном случае мы ищем устройства, работающие на операционной системе Linux.
- org:"Hikvision" - фильтр, используемый для поиска устройств от определенной организации. В данном случае мы ищем устройства от производителя "Hikvision".
- country:”US" - фильтр, используемый для ограничения поиска по стране. В данном случае мы ищем устройства, находящиеся в Соединенных Штатах.

Google Dork для поиска сетевых видеокамер:

- intext:"Powered by IP Camera Viewer" - ищет веб-страницы, содержащие текст "Powered by IP Camera Viewer".
- intitle:"Network Camera" inurl:top.htm - ищет веб-страницы с заголовком "Network Camera" и с URL, содержащим "top.htm".
- intitle:"Live View / - AXIS" - ищет веб-страницы с заголовком "Live View / - AXIS".
- intitle:"D-Link" inurl:top.htm - ищет веб-страницы с заголовком "D-Link" и с URL, содержащим "top.htm".
- intitle:"Network Camera" intext:"Video Web Server" - ищет веб-страницы с заголовком "Network Camera" и содержащие текст "Video Web Server".
- inurl:view/view.shtml - ищет веб-страницы, в URL которых присутствует "view/view.shtml".
- intitle:"Hikvision" inurl:"/login.html" - ищет веб-страницы с заголовком "Hikvision" и в URL содержится "/login.html".
- site:axis.com intitle:"Live View / - AXIS" - ищет веб-страницы на сайте axis.com с заголовком "Live View / - AXIS".
- inurl:"/nphMotionJpeg?Resolution=" - ищет веб-страницы, в URL которых присутствует "/nphMotionJpeg?Resolution=".
- inurl:/cgi-bin/guestimage.html - ищет веб-страницы, в URL которых присутствует "/cgi-bin/guestimage.html".

Сервисы для поиска сетевых видеокамер в Интернет:

- Shodan: https://www.shodan.io
- Censys: https://censys.io
- ZoomEye: https://www.zoomeye.org
- Thingful: https://www.thingful.net

ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ БРАУЗЕРОВ

Цель:
Получение доступа к данным хранящихся в браузере пользователя для дальнейшего анализа.

Подключение видеопотоков к сетевому плейеру:

URL-адрес MJPEG

http://username:password@ip_address:port/path/to/mjpeg/stream

- username - имя пользователя для аутентификации, если необходимо.
- password - пароль для аутентификации, если необходимо.
- ip_address - IP-адрес устройства или источника MJPEG-потока.
- port - порт для подключения к устройству или источнику MJPEG-потока (обычно 80).
- path/to/mjpeg/stream - путь или местоположение MJPEG-потока на устройстве.

FFMPEG (H.264)

rtsp://username:password@ip_address:port/video_stream

- username - имя пользователя для аутентификации.
- password - пароль для аутентификации.
- ip_address - IP-адрес устройства или источника видеопотока.
- port - порт для подключения к устройству или источнику видеопотока (обычно 554 для RTSP).
- video_stream - путь или потоковый идентификатор для видеопотока.

Onvif

rtsp://username:password@ip_address:port/onvif/profile/profile_token

- username - имя пользователя для аутентификации ONVIF.
- password - пароль для аутентификации ONVIF.
- ip_address - IP-адрес устройства ONVIF.
- port - порт для подключения к устройству ONVIF (обычно 80 или 554).
- profile_token - токен профиля медиа-сервиса ONVIF.

Конкретный путь к потоку можно определить используя Fiddler или Wireshark

Инструмент:	Где взять:	Для чего:
ZENMAP	https://nmap.org/zenmap	Сетевые сканеры *Win/linux*
Angry IP scanner	https://angryip.org	
Advanced IP scanner	https://www.advanced-ip-scanner.com	
Fiddler	https://www.telerik.com/fiddler	Анализатор сетевого трафика для поиска всех web ресурсов камеры (поиск страницы с видеопотоком) *Мульти платформенный*
Fing	https://www.fing.com	Сетевой сканер *Android/iOS*
WiFiman	https://play.google.com/store/apps/details?id=com.ubnt.usurvey&hl=ru	
IoPT: Network Security Scanner	http://www.iopt.pro	Сетевой сканер с функцией аудита безопасности *Android*
TinyCAM	https://tinycammonitor.com/	Приложение для мониторинга с сетевых видеокамер, NVR и DVR с функцией поиска. *Android*
IVMS - 4200	https://www.hikvision.com/en/support/download/software/ivms4200-series	Поиск, настройка и просмотр сетевых видеокамер *Windows*
iSpy	https://www.ispyconnect.com/	Система организации видеонаблюдения с возможностью поиска и просмотра *Мульти платформенный*
Avigilon Camera Installation Tool	https://www.avigilon.com/security-cameras/configuration-tool	Поиск и настройка видеокамер в сети *Windows*
VLC media player	https://www.videolan.org/	Просмотр видеопотока *Мульти платформенный*