

OSINT

Разведка по открытым источникам.
Рекогносцировка.

Виталий Малкин

Руководитель отдела анализа защищенности в ГК “Информзащита”

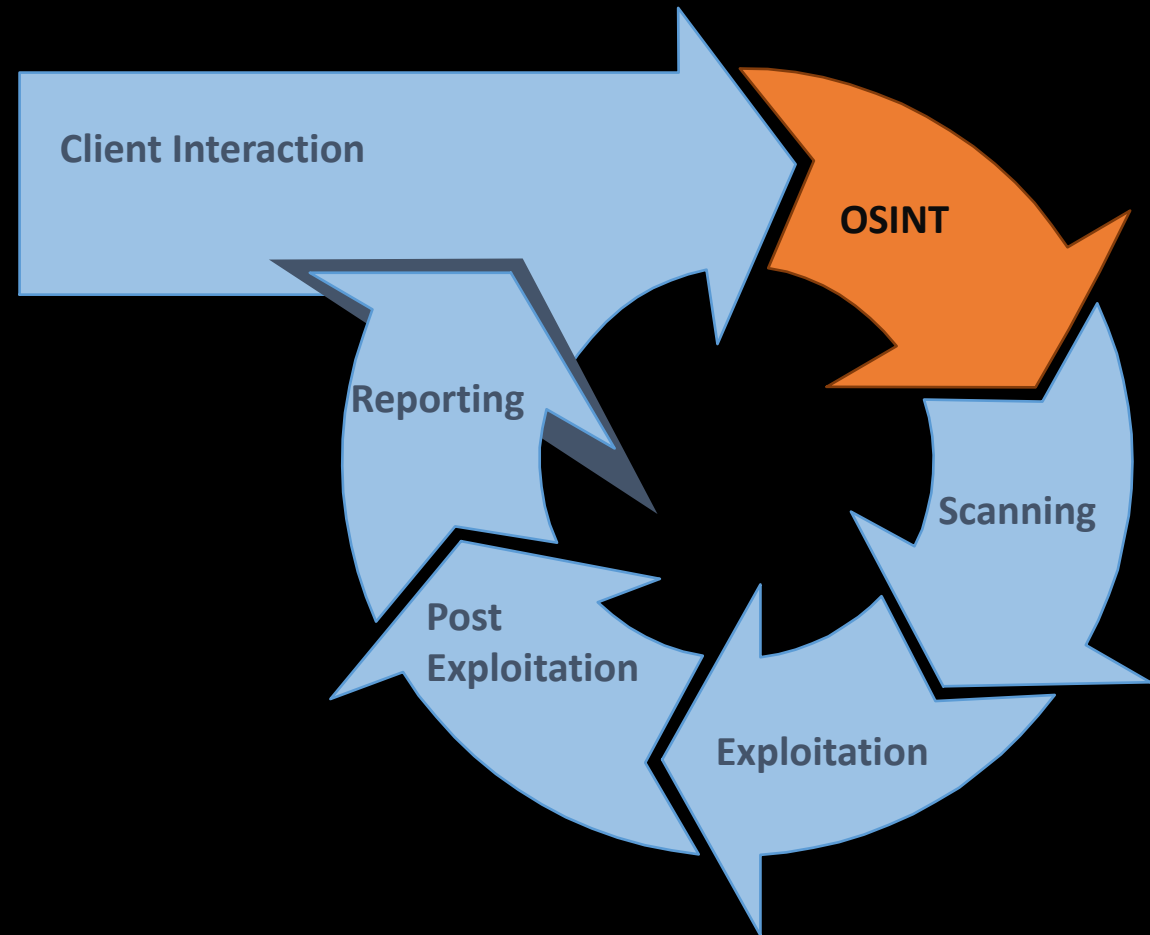
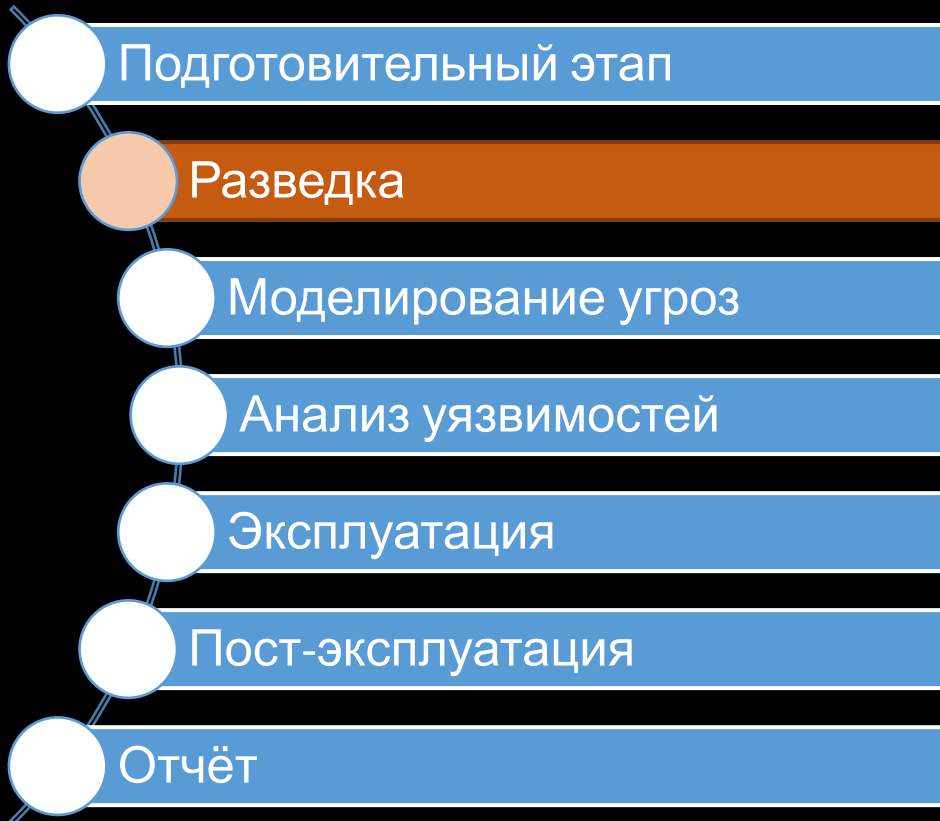
Telegram: @VitMalkin, E-Mail: vitmalkin@gmail.com

ДИСКЛЕЙМЕР

Автор материала не несет ответственности за действия, совершенные слушателями.

Информация предоставлена исключительно в ознакомительных целях.

Этапы процесса анализа защищенности



Зачем при пентесте разведка?

- Расскажу 3 истории
 - Half Life 2 – AXFR запрос
 - Из курса OSCP про марки
 - Взлом почты по историческому форуму

Два подхода к разведке

Пассивная

- Поиск в интернете
- Сбор контактов
- Сбор документов
- Поиск IP адресов
- Поиск поддоменов

Активная

- Сканирование портов
- Перечисление поддоменов, директорий
- Атаки SMB, SMTP, SNMP enumeration, AXFR

Наличие активного взаимодействия с объектом

Пассивная: Поиск в интернете 1

- Чем занимаются?
- Как взаимодействуют с миром?
- Нанимают ли людей?
- Список сайтов



Пассивная: Поиск в интернете 2

- Изучение сайтов, мобильных приложений. Как вам дизайн сайта? HTML код чистый?
- Мероприятия
- Вакансии
- Имеется ли отдел продаж? Что продают, где и как продают, кто покупает, кто клиенты?

Пассивная: Сбор

Берем все, что не прикручено и структурируем:

- Все контакты
- Телефоны, факсы
- Имейлы
- Структура компании
- Документы
- Компании партнеры

Google Dorks

Логические операторы:

- Где живет Вася **OR** Петя
- “такую именно фразу хочу загуглить я”
- Виталий Малкин –**депутат**

Другие операторы:

site: filetype: inurl: intitle:

Пассивная: Сбор имейлов

- Google Dorks:
 - G: **email "example.com"**, Y: **"@example.com"**
- Дополнения Google Chrome:
 - EMAIL finder, Email Extractor
- Инструменты:
 - Sewl – поиск имейлов на сайт
 - TheHarvester
- Whois



Пассивная: Поиск по личности

- www.roum.ru/bases/people.html
- nomerorg.xyz
- nomer.io
- findface.ru
- Соцсети + восстановление доступа
- Google: поиск по фото
- Мобильный банкинг

Пассивная: Сбор и анализ документов

- Google Dorks
 - `site:example.com filetype:pdf`
- FOCA
 - Поиск документов
 - Экспорт метаданных
 - Консолидация



Пассивная: Поиск поддоменов

- Что будет первым пунктом?

Пассивная: Поиск поддоменов

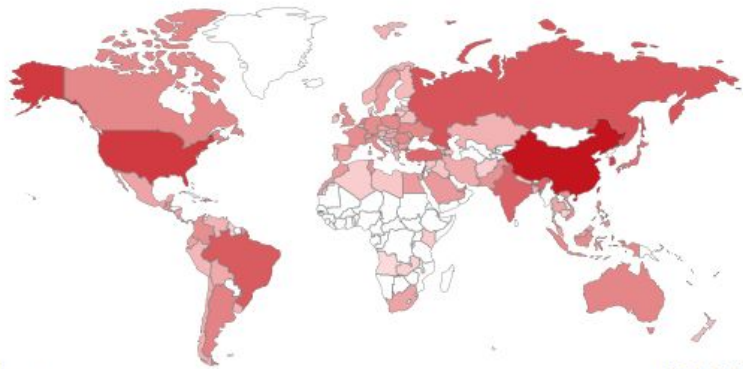
- Google Dorks:
 - [site:example.com -site:www.example.com](#)
- Сайты:
 - [searchdns.netcraft.com](#)
 - [virustotal.com/#/home/search](#)
 - [community.riskiq.com/home](#)
 - [crt.sh](#)
 - [Ssl-labs](#)

Пассивная: Поиск IP адресов

- apps.db.ripe.net/search/full-text.html
- riskiq.com
- dnsdumpster.com
- Whois
- bgp.he.net



TOP COUNTRIES



China	429,019
Taiwan, Province of China	199,779
United States	179,050
Korea, Republic of	166,754
Russian Federation	87,766

TOP ORGANIZATIONS

Korea Telecom	143,473
---------------	---------

Showing results 1 - 10 of 2,258,988

112.229.207.23

China Unicom Shandong

Added on 2016-01-03 13:10:02 GMT

 China, Jinan

[Details](#)

only a dns server!

Recursion: enabled

2607:fb90:5d00:cf1f:0:49:cc95:4201

Added on 2016-01-03 13:10:02 GMT

[Details](#)

dnsmasq-2.62

Recursion: enabled

117.253.245.216

BSNL

Added on 2016-01-03 13:10:00 GMT

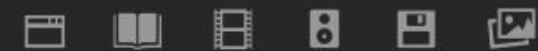
 India, New Delhi

[Details](#)

9.4.1

Recursion: enabled

Пассивная: web.archive.org



SIGN IN



[ABOUT](#) [CONTACT](#) [BLOG](#) [PROJECTS](#) [HELP](#) [DONATE](#) [JOBS](#) [VOLUNTEER](#) [PEOPLE](#)



Explore more than 310 billion [web pages](#) saved over time

DONATE



feedmag.com
Dec 23, 1996 10:53:17

Tools

[Wayback Machine Availability API](#)
Build your own tools.

[WordPress Broken Link Checker](#)
Banish broken links from your blog.

[404 Handler for Webmasters](#)

Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. [Visit Archive-It to build and browse the collections.](#)

Save Page Now

Capture a web page as it appears now for use as a trusted citation in the future.

Only available for sites that allow crawlers.



Feedback

Активная разведка

- Перечисление поддоменов
- Перечисление файловых ресурсов (shares)
- Перечисление имейлов
- Перенос DNS зоны (AXFR)
- Сканеры портов
- Сканеры уязвимостей



Активная: Перенос DNS зоны, AXFR

```
#> dig xname.org @ns2.xname.org axfr
```

...служебная информация, а затем:

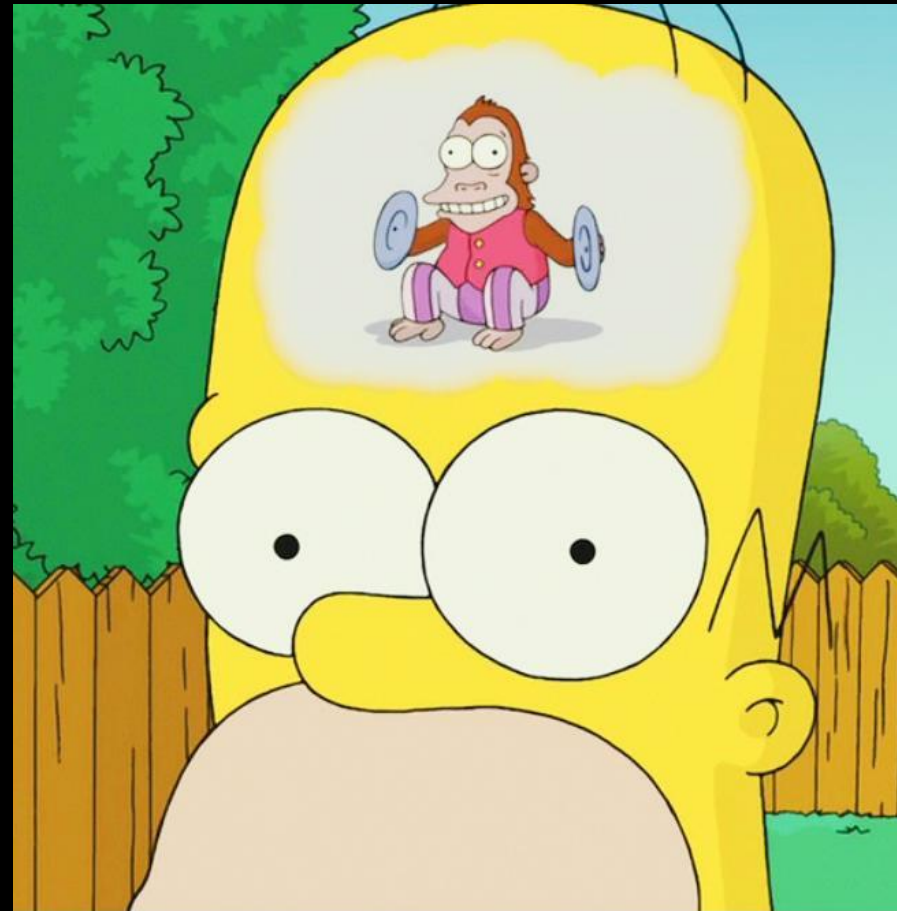
demo.xname.org	ns0.xname.org	source.xname.org
dev.xname.org	ns1.xname.org	test.xname.org
error.xname.org	ns2.xname.org	url.xname.org
g1.xname.org	o1.xname.org	www.xname.org
myip.xname.org	o1b.xname.org	xname.org

Активная: Анализ веб-сайта

- FOCA
- CEWL
- dvcs-ripper
- Aquatone
- Recon-ng

Как не сойти с ума от объемов информации?

- KeepNote
- Maltego
+
- Lair / Faraday
- Zenmap
+
- Screenshots



OSCP
Lab
10.11.1.73
ms11-046_PASS-qwe123.zip
10.11.1.73.proof.txt
nmap
10.11.1.8
9545_pass-qwe123.zip
10.11.1.8.proof.txt
nmap
hints
10.11.1.24
Exercises
OSCP-pwk-31486-316093.pdf
1.3.1.3 - bash usage
2.2.1 - ncat, sbd
2.3.5 - wireshark
2.4.3 - tcpdump
3.1.3 - Google Dorks
3.2.1 - theHarvester
3.3.3 - whois
Trash

Title	Created time	Modified time
Lab	Bc, 01 08:07	Чт, 05 05:33
10.11.1.73	Bc, 01 04:22	Чт, 05 06:23
10.11.1.8	C6, сен 30 04:39	Чт, 05 06:25
10.11.1.24	Чт, 05 07:51	Чт, 05 07:54

1) NMAP

Nmap scan report for 10.11.1.8

Host is up (0.093s latency).

Not shown: 90 filtered ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.0.1
22/tcp	open	ssh	OpenSSH 3.9p1 (protocol 1.99)
25/tcp	closed	smtp	
80/tcp	open	http	Apache httpd 2.0.52 ((CentOS))
111/tcp	open	rpcbind	
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: MYGROUP)
443/tcp	open	ssl/https?	
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: MYGROUP)
631/tcp	open	ipp	CUPS 1.1
3306/tcp	open	mysql?	

MAC Address: 00:50:56:B8:D0:7F (VMware)

Aggressive OS guesses: Linux 2.6.18 (94%), Linux 2.6.11 (93%), Linux 2.6.9 - 2.6.27 (93%), Linux 2.6.9 (92%), Cisco SA520 firewall (Linux 2.6) (90%), Linux 2.6.28 (90%), Linux 2.6.30 (90%), Linux 2.6.32 (90%), Linux 2.6.9 (CentOS 4.4) (90%), Riverbed Steelhead 200 proxy server (90%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Unix

2) goto http://10.11.1.8/

3) dirsearch

dirsearch -u http://10.11.1.8/ -e php -x 403

```
> # dirsearch -u http://10.11.1.8/ -e php
```

Clipboard: Paste, Clear All, Copy, Cut, Delete

Transform Results: Number of Results (slider)

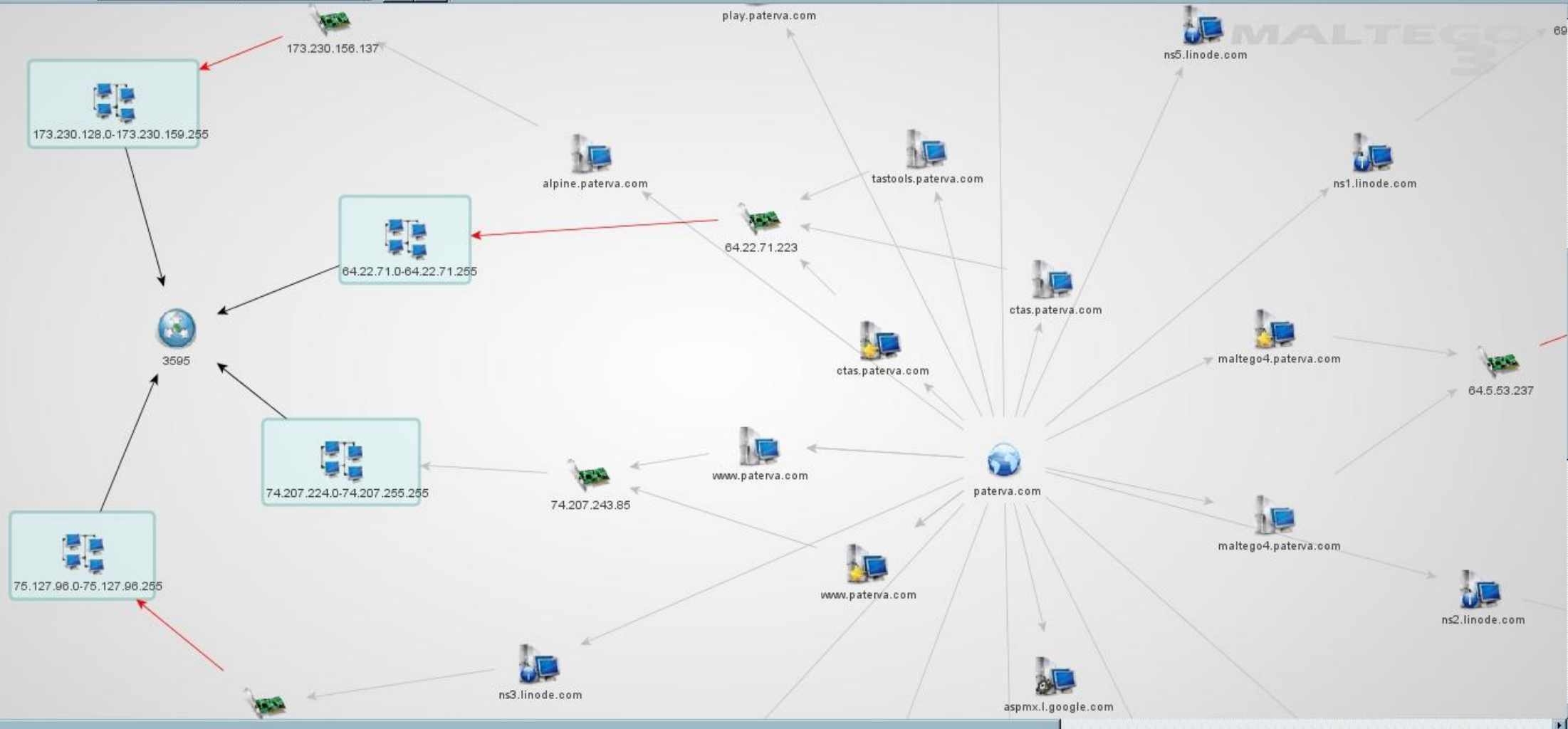
Find: Quick Find

Selection: Select All, Invert Selection, Select parents, Add parents, Select children, Add children, Select neighbours, Add neighbours

Zoom: Zoom in, Zoom out, Zoom to, Zoom to fit

New Graph (1) *

Mining View Dynamic View Edge Weighted View Entity List



Output

Property View Overview

От теории к практике

Произвести пассивную (!) разведку и предоставить подробный отчет о выполненных шагах и результатах в структурированном формате.