بسم الله الرحمن الرحیم

دانشگاه محقق اردبیلی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز ماهر
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

آشنایی با ارزیابی امنیتی سامانه های تحت وب

امام صادق علیه‌السلام:

راز و اسرار تو به منزله‌ی خون توست، پس سعی کن که جز در شاهرگهایت به جریان نیفتند.

هدف کارگاه های آپا

آگاهی رسانی پشتیبانی امداد رسانی

هدف

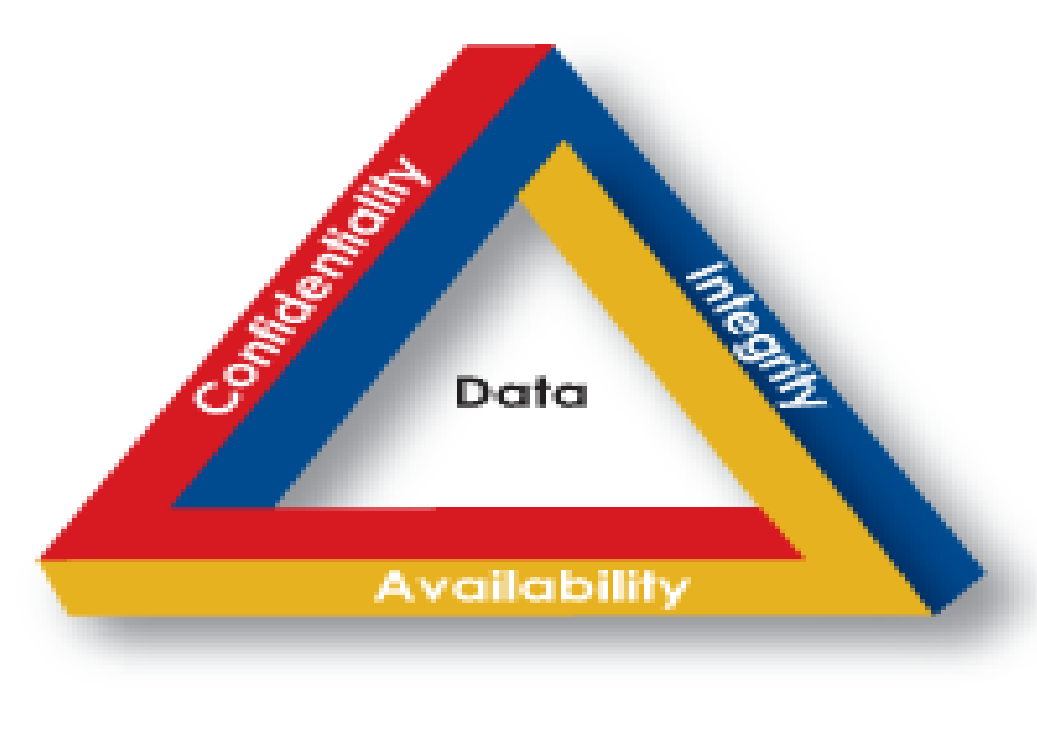
بالا بردن دانش نیروی کارآمد در حوزه امنیت

اهمیت یادگیری امنیت در وب

- هک nsa توسط shadowbrokers
- حمله DOS به بانکهای ایرانی
- تزریق کدهای استخراج ارزرمز در سایتهای دولتی
- انتشار خبر کذب در سایتهای خبری معتبر ایرانی

امنیت در وب

- مثلث امنیت یا CIA :



امنیت در وب

- مثلث امنیت یا CIA :

- ۱) محرمانگی (Confidentiality) : اطلاعات فقط باید برای افراد مربوطه در دسترس باشد .

- ۲) صحت یا تمامیت (Integrity) : اطلاعات باید سالم و بدون دستکاری باشد

- ۳) دسترسی پذیری (Availability) : اطلاعات در زمان مورد نیاز برای افراد در دسترس باشد .

نکته ای مهم و حیاتی

- طبق **قانون جرایم رایانه ای** نفوذ به سایتها و سیستمهای ایرانی جرم است و عواقب سنگینی را برای نفوذگران در پی خواهد داشت.

- http://www.cyberpolice.ir/page/42981

- یکی از ماده های این قانون :

- ماده۷۲۹ـ هرکس به طور غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.

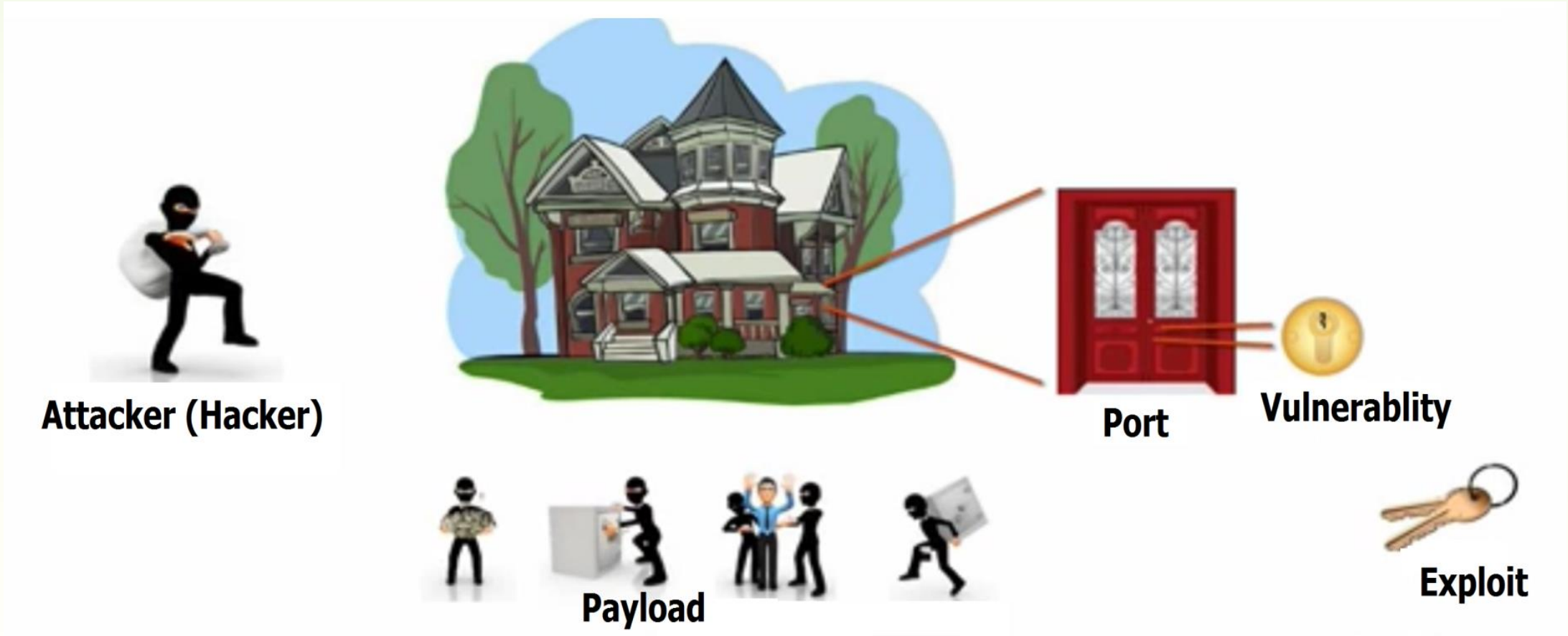
آشنایی با اصطلاحات رایج در حوزه وب

- هدف یا Target : سایت ، سرور ، یا سیستمی که قصد نفوذ به آن را داریم.
- Attack : اقدام به نفوذ به یک target با هر هدفی
- Attacker : کسی که با مقاصدی خاص قصد نفوذ به target ای دارد.
- آسیب پذیری یا Vulnerability : نقطه ضعف های یک سایت یا سیستم که میتوان با استفاده از آنها به سایت یا سیستم نفوذ کرد.
- اکسپلویت exploit : کد هایی مخرب نوشته شده برای یک آسیب پذیری خاص(روش نفوذ از یک حفره موجود در target)

آشنایی با اصطلاحات رایج در حوزه وب (ادامه)

- Bypass : عبور کردن و دور زدن از موانع موجود در مسیر نفوذ به target موردنظر
- Shell شل : گرفتن دسترسی کامل از سایت یا سرور یا سیستم است . دسترسی به خط فرمان یا command line یک target
- Dork : یک سری کلمات که با ترکیب درست آن ها میتوان target های جدید یافت یا اطلاعات جدیدی در مورد target خاص به دست آورد.
- Payload :
- Deface : ایجاد تغییر در target نفوذ شده
- Mass deface : ایجاد تغییرات در همه سایتهای هاست شده روی سرور خاص

مثال مفهومی



ارزیابی امنیت

یک فرآیند سیستماتیک و برنامه ریزی شده است که آسیب پذیری ها و حفره های امنیتی سرور، شبکه و منابع و برنامه های متصل به آن را از طریق شبیه سازی یک حمله نفوذگر، بررسی می کند.

مراحل ارزیابی امنیت

- جمع آوری اطلاعات (Footprinting)
- اسکن کردن (Scanning)
- بدست آوردن دسترسی (Gaining Access)
- حفظ سطح دسترسی (Maintaining access)
- پاک کردن رد پاها و لاگ ها (Covering Tracks)

FOOTPRINTING

جمع آوری اطلاعات

Footprinting

Footprinting چیست ؟

به فرآیند پیدا کردن و جمع آوری اطلاعات در خصوص سایت هدف و محیط هایی که هدف در آنها سرویس دهی می کند، گفته می شود.

اهداف Footprinting :

- جمع آوری اطلاعات در مورد شبکه
- جمع آوری اطلاعات در مورد سیستم
- جمع آوری اطلاعات در مورد سازمان

از کجاها اطلاعات جمع کنیم؟

- جمع آوری اطلاعات در مورد یک هدف از منابع در دسترس عموم (نامحسوس)
- جمع آوری اطلاعات از طریق مهندسی اجتماعی ، ملاقات و ....
- جمع آوری اطلاعات به وسیله نام های مستعار و...
- جمع آوری اطلاعات از مشخصات سازمانی و...
- و ...

بخش های Footprinting

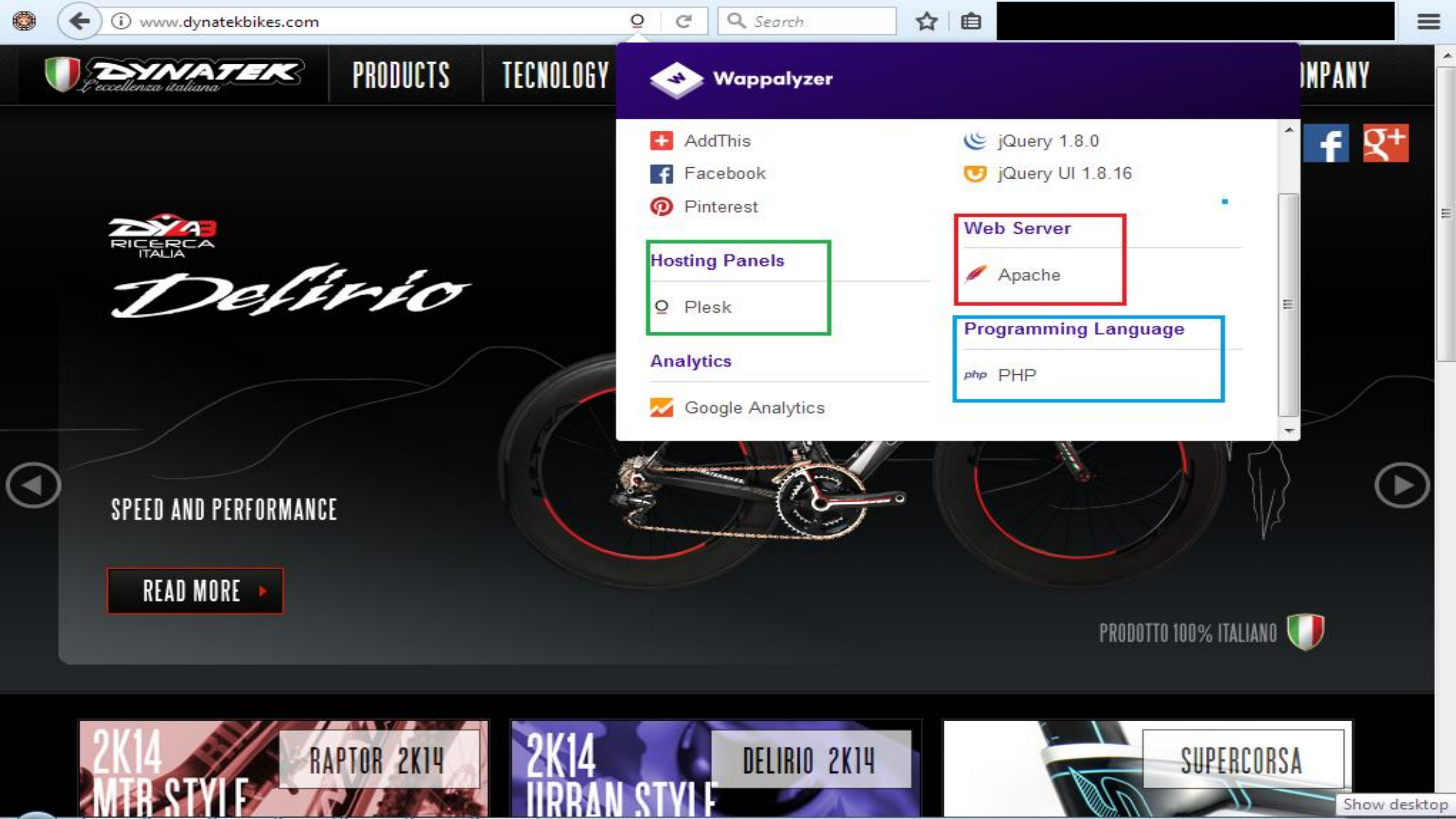
- Network Footprinting
- Website Footprinting
- E-mail Footprinting
- Google Hacking
- Social Engineering
- Internet Footprinting
- Competitive Intelligence
- Social Networking Sites
- Whois Footprinting
- DNS Footprinting

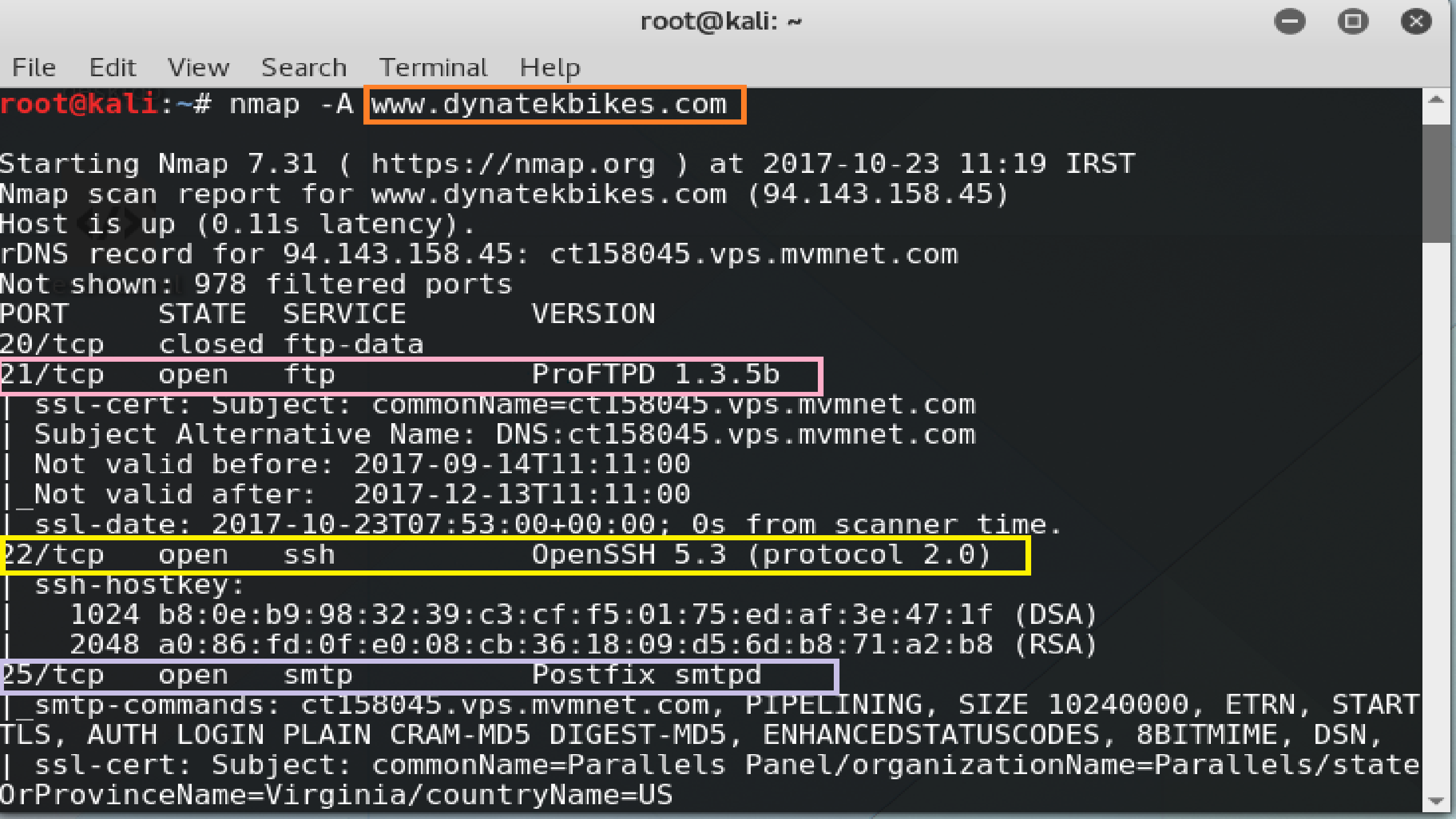
Website Footprinting

در این بخش به آنالیز سایت هدف پرداخته و اطلاعاتی مثل نوع سیستم عامل ، پلتفرم های مورد استفاده ، وب سرورها و نسخه سرورها و سرویس های ارائه شده و... را به دست می آوریم.

برخی از ابزارهایی که در این زمینه وجود دارد :

nmap , zenmap , paros proxy , brup suite ,wappalyzer و Whatweb و ...


www.dynatekbikes.com
Search
DYNATEK
L'eccellenza italiana
PRODUCTS
TECNOLOGY
MPANY
Wappalyzer
AddThis
Facebook
Pinterest
jQuery 1.8.0
jQuery UI 1.8.16
Hosting Panels
Plesk
Web Server
Apache
Programming Language
php PHP
Analytics
Google Analytics
DYNA3
RICERCA
ITALIA
Delirio
SPEED AND PERFORMANCE
READ MORE
PRODOTTO 100% ITALIANO
2K14
MTB STYLE
RAPTOR 2K14
2K14
URBAN STYLE
DELIRIO 2K14
SUPERCORSA
Show desktop


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A www.dynatekbikes.com
Starting Nmap 7.31 (https://nmap.org) at 2017-10-23 11:19 IRST
Nmap scan report for www.dynatekbikes.com (94.143.158.45)
Host is up (0.11s latency).
rDNS record for 94.143.158.45: ct158045.vps.mvmnet.com
Not shown: 978 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp ProFTPD 1.3.5b
| ssl-cert: Subject: commonName=ct158045.vps.mvmnet.com
| Subject Alternative Name: DNS:ct158045.vps.mvmnet.com
| Not valid before: 2017-09-14T11:11:00
|_Not valid after: 2017-12-13T11:11:00
| ssl-date: 2017-10-23T07:53:00+00:00; 0s from scanner time.
22/tcp open ssh OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
| 1024 b8:0e:b9:98:32:39:c3:cf:f5:01:75:ed:af:3e:47:1f (DSA)
| 2048 a0:86:fd:0f:e0:08:cb:36:18:09:d5:6d:b8:71:a2:b8 (RSA)
25/tcp open smtp Postfix smtpd
|_smtp-commands: ct158045.vps.mvmnet.com, PIPELINING, SIZE 10240000, ETRN, START
TLS, AUTH LOGIN PLAIN CRAM-MD5 DIGEST-MD5, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=Parallels Panel/organizationName=Parallels/state
OrProvinceName=Virginia/countryName=US

E-mail Footprinting

در این بخش از فرآیند جمع آوری اطلاعات سعی می شود تا آدرس ایمیل کاربران سایت هدف به دست آید. از این ایمیل ها برای انجام عمل brute force با هدف کشف پسورد کاربران می توان استفاده کرد.

ابزارهای مفید در این زمینه:

- Theharvestar
- SimplyEmail

Whois Footprinting

از طریق انجام whois می توان اطلاعات مهمی مثل ip , dns ، اسم ثبت کننده و ... سایت را به دست آورد.

برخی از سایت هایی که در این زمینه استفاده می شوند:

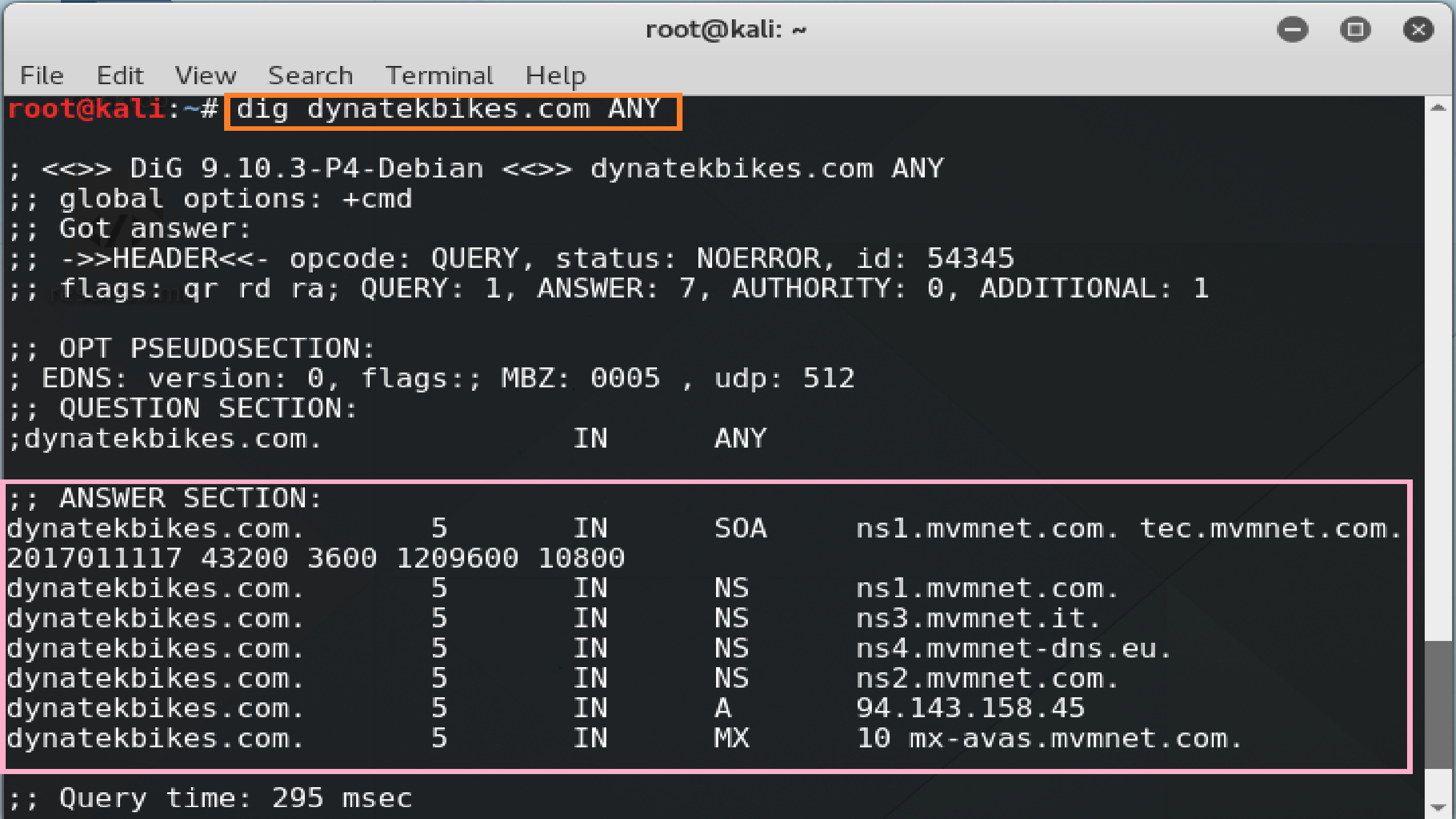
- http://whois.sc
- https://www.whois.net/
- http://network-tools.com/

DNS Footprinting

در این بخش از جمع آوری اطلاعات به کمک ابزارها و سایت های موجود در این زمینه به رکوردهای dns یک سایت می توان دست یافت .

چند نمونه از ابزارهای موجود در این زمینه:

- DIG
- DnsRecon
- DNS Watch
- My DSN Tools
- Professional Toolset
- DNS Query Ultility
- DNS Data View


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dig dynatekbikes.com ANY
; <<>> DiG 9.10.3-P4-Debian <<>> dynatekbikes.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54345
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 512
;; QUESTION SECTION:
;dynatekbikes.com. IN ANY
;; ANSWER SECTION:
dynatekbikes.com. 5 IN SOA ns1.mvmnet.com. tec.mvmnet.com.
2017011117 43200 3600 1209600 10800
dynatekbikes.com. 5 IN NS ns1.mvmnet.com.
dynatekbikes.com. 5 IN NS ns3.mvmnet.it.
dynatekbikes.com. 5 IN NS ns4.mvmnet-dns.eu.
dynatekbikes.com. 5 IN NS ns2.mvmnet.com.
dynatekbikes.com. 5 IN A 94.143.158.45
dynatekbikes.com. 5 IN MX 10 mx-avas.mvmnet.com.
;; Query time: 295 msec

Social Engineering

مهندسی اجتماعی سوء استفاده زیرکانه از تمایل طبیعی انسان به اعتماد کردن است که به کمک مجموعه‌ای از تکنیک‌ها، فرد را به فاش کردن اطلاعات یا انجام کارهایی خاص متقاعد می‌کند.

در این روش مهاجمان چند مرحله تا رسیدن به هدف فاصله دارند:

- تحقیقات اولیه
- جلب اطمینان
- دریافت اطلاعات
- سوء استفاده از اطلاعات

.

Google Hacking

یکی از مهمترین قسمت ها در انجام Footprinting ، گوگل هکینگ هست .
بدست اوردن اطلاعات از گوگل را گوگل هکینگ میگویند . کسانی که dork نویسی و گوگل هکینگ خوبی دارند، بسیار موفق تر هستند .

کلمات کلیدی برای انجام Google Hacking :

- Site
- inurl
- intext
- intitle
- filetype
- Related
- link
- cache
- info

ابزارهای دیگر در زمینه Footprinting

- Maltego
- Recon-ng
- FOCA
- Dmitry
- Wafwoof
- Prefix Whois
- Netmask
- Net Scan Tools Pro
- Binging
- Tctrace
- Search Bug

FOCA Free 3.0

Project | Tools | Options | TaskList | About | Donate

- Network
- Domains
- Roles
  - ActiveDirectory
  - Dns
  - Finger
  - Firewall
  - Ftp
  - Http
  - Https
  - InstantMessaging
  - IPS
  - Kerberos
  - LDAP
  - LoadBalancer
  - Mail
  - Proxy
  - RemoteDesktop
  - SSH
  - Telnet
  - VPN
  - VoIP
  - WAF
  - Whois
- Vulnerabilities
  - Backups
  - Directory listing
  - DNS Active Cache
  - .DS_Store
  - GHDB
  - Insecure Methods
  - Multiple choices
  - SQLi
  - Listing
  - Leaks
  - Proxy
  - Users
  - ZoneTransfer
- Metadata

Select search type

Web Searcher | DNS Search | Transfer Zone | Dictionary Search | IP Bing | PTR Scanning | Shodan & Robtex

Search IP in Bing

Bing allows search links located in a particular IP address.
This funcionalitty can be used to find domains that
share IP Address.

Select the web search engine to use:

BingWeb

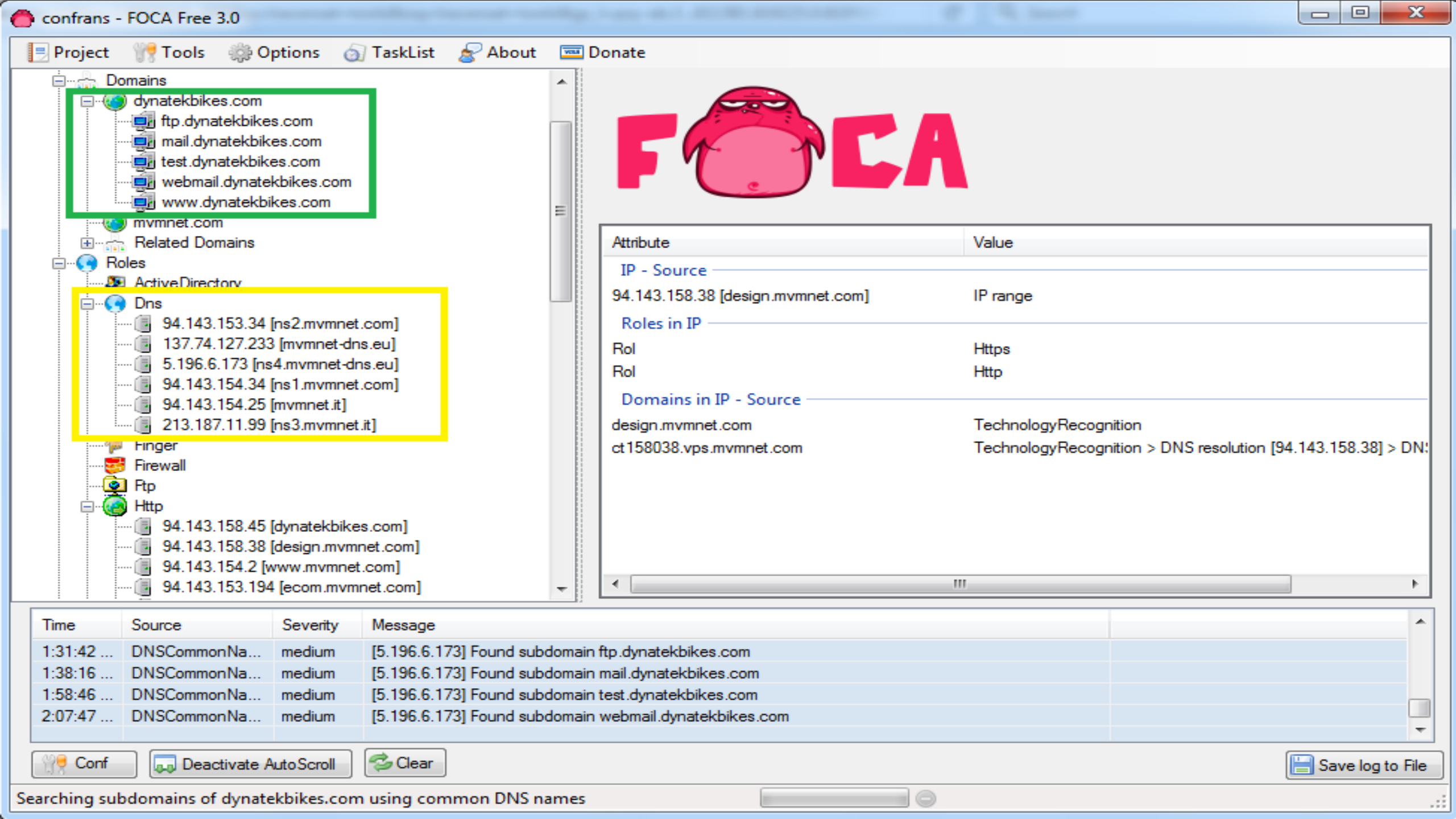
Bing Web limitations

-Max 1000 results for each search
-Max 49 words in a search string

Current search: None

Skip | Start

Conf | Deactivate AutoScroll | Clear | Save log to File


confrans - FOCA Free 3.0
Project
Tools
Options
TaskList
About
Donate
Domains
dynatekbikes.com
ftp.dynatekbikes.com
mail.dynatekbikes.com
test.dynatekbikes.com
webmail.dynatekbikes.com
www.dynatekbikes.com
mvmnet.com
Related Domains
Roles
ActiveDirectory
Dns
94.143.153.34 [ns2.mvmnet.com]
137.74.127.233 [mvmnet-dns.eu]
5.196.6.173 [ns4.mvmnet-dns.eu]
94.143.154.34 [ns1.mvmnet.com]
94.143.154.25 [mvmnet.it]
213.187.11.99 [ns3.mvmnet.it]
Finger
Firewall
Ftp
Http
94.143.158.45 [dynatekbikes.com]
94.143.158.38 [design.mvmnet.com]
94.143.154.2 [www.mvmnet.com]
94.143.153.194 [ecom.mvmnet.com]
FOCA
Attribute
Value
IP - Source
94.143.158.38 [design.mvmnet.com]
IP range
Roles in IP
Rol
Https
Rol
Http
Domains in IP - Source
design.mvmnet.com
TechnologyRecognition
ct158038.vps.mvmnet.com
TechnologyRecognition > DNS resolution [94.143.158.38] > DN
Time
Source
Severity
Message
1:31:42 ...
DNSCommonNa...
medium
[5.196.6.173] Found subdomain ftp.dynatekbikes.com
1:38:16 ...
DNSCommonNa...
medium
[5.196.6.173] Found subdomain mail.dynatekbikes.com
1:58:46 ...
DNSCommonNa...
medium
[5.196.6.173] Found subdomain test.dynatekbikes.com
2:07:47 ...
DNSCommonNa...
medium
[5.196.6.173] Found subdomain webmail.dynatekbikes.com
Conf
Deactivate AutoScroll
Clear
Save log to File
Searching subdomains of dynatekbikes.com using common DNS names

راه های مقابله با Footprinting

- محدود نمودن کارمندان برای دسترسی به سایت های شبکه های اجتماعی از طریقه شبکه سازمان
- پیکربندی صحیح وب سرور
- استفاده از IDS به منظور شناسایی ترافیک های مشکوک footprinting
- آموزش کارمندان برای استفاده از نام های مستعار برای عضویت در سایت ها و..
- ارزیابی اطلاعات قبل از انتشار در وب سایت
- رمزنگاری و محافظت با پسورد برای اطلاعات حساس
- اجرای عملیات footprinting و حذف اطلاعات حساس یافت شده

SCANNING

شناسایی داشته های سیستم

Scanning

به مجموعه ای از فرآیندهای مختلف برای شناسایی میزبان، پورت های باز وکشف آسیب پذیری های موجود در سایت هدف اشاره دارد.

مراحل scanning :

- Ip Scanning
- Port Scanning
- Vulnerability Scanning

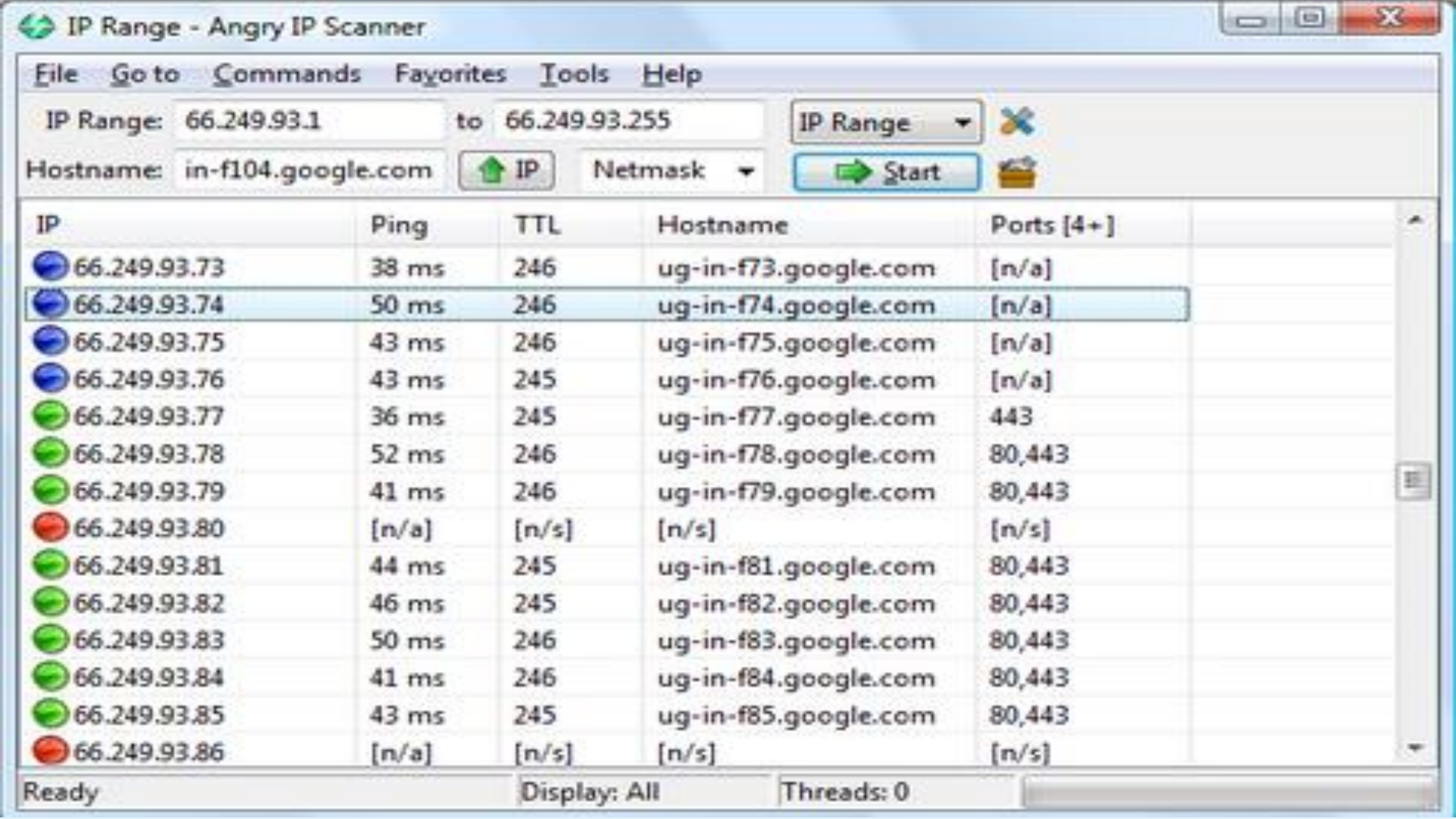
اهداف Scanning

- شناسایی میزبان های در دسترس و پورت های باز روی آن ها
- شناسایی سیستم عامل و معماری سیستم
- شناسایی سرویس های اجرا شده بر روی میزبان ها
- کشف آسیب پذیری های موجود روی سیستم میزبان

Ip Scanning

به تشخیص فعال بودن یا نبودن یک IP در شبکه عمل ip scanning میگویند.

با انجام عمل ping به سادگی می توان فعال بودن یک IP را تشخیص داد اما چک کردن مجموعه وسیعی از ip ها با این روش فرایندی زمان بر خواهد بود. از ابزارهای موجود در این زمینه برای سرعت دادن به کار می توان استفاده کرد.
یکی از ابزارهای قدرتمند موجود، ابزار Angry ip scanner هست.

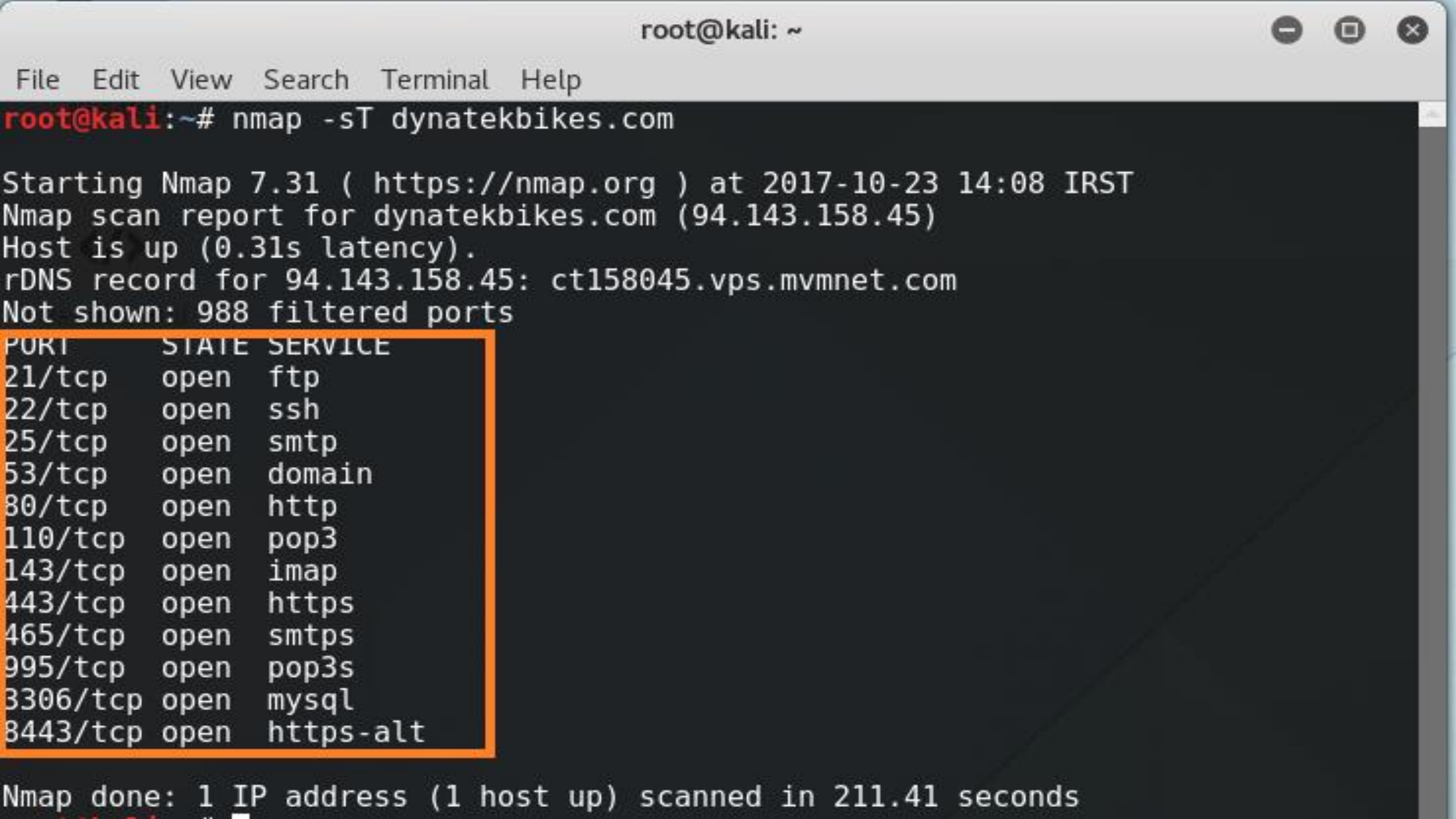

IP Range - Angry IP Scanner
File Go to Commands Favorites Tools Help
IP Range: 66.249.93.1 to 66.249.93.255
IP Range
Hostname: in-f104.google.com
IP
Netmask
Start
IP Ping TTL Hostname Ports [4+]
66.249.93.73 38 ms 246 ug-in-f73.google.com [n/a]
66.249.93.74 50 ms 246 ug-in-f74.google.com [n/a]
66.249.93.75 43 ms 246 ug-in-f75.google.com [n/a]
66.249.93.76 43 ms 245 ug-in-f76.google.com [n/a]
66.249.93.77 36 ms 245 ug-in-f77.google.com 443
66.249.93.78 52 ms 246 ug-in-f78.google.com 80,443
66.249.93.79 41 ms 246 ug-in-f79.google.com 80,443
66.249.93.80 [n/a] [n/s] [n/s] [n/s]
66.249.93.81 44 ms 245 ug-in-f81.google.com 80,443
66.249.93.82 46 ms 245 ug-in-f82.google.com 80,443
66.249.93.83 50 ms 246 ug-in-f83.google.com 80,443
66.249.93.84 41 ms 246 ug-in-f84.google.com 80,443
66.249.93.85 43 ms 245 ug-in-f85.google.com 80,443
66.249.93.86 [n/a] [n/s] [n/s] [n/s]
Ready
Display: All
Threads: 0

Port Scanning

به عمل کشف و شناسایی پورت های باز و بسته یک سرور عمل port scanning میگویند.

با انجام عمل telnet به سادگی می توان باز بودن یک port را تشخیص داد اما چک کردن حالت همه ۶۵۵۳۵ پورت موجود با این روش فرایندی زمان بر خواهد بود.

استفاده از nmap راه حل بهتری است.


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sT dynatekbikes.com
Starting Nmap 7.31 (https://nmap.org) at 2017-10-23 14:08 IRST
Nmap scan report for dynatekbikes.com (94.143.158.45)
Host is up (0.31s latency).
rDNS record for 94.143.158.45: ct158045.vps.mvmnet.com
Not shown: 988 filtered ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
995/tcp open pop3s
3306/tcp open mysql
8443/tcp open https-alt
Nmap done: 1 IP address (1 host up) scanned in 211.41 seconds

Vulnerability Scanning

Vulnerability :

هرگونه ضعف نرم افزاری که قابل سوءاستفاده باشد.

Vulnerability scanner :

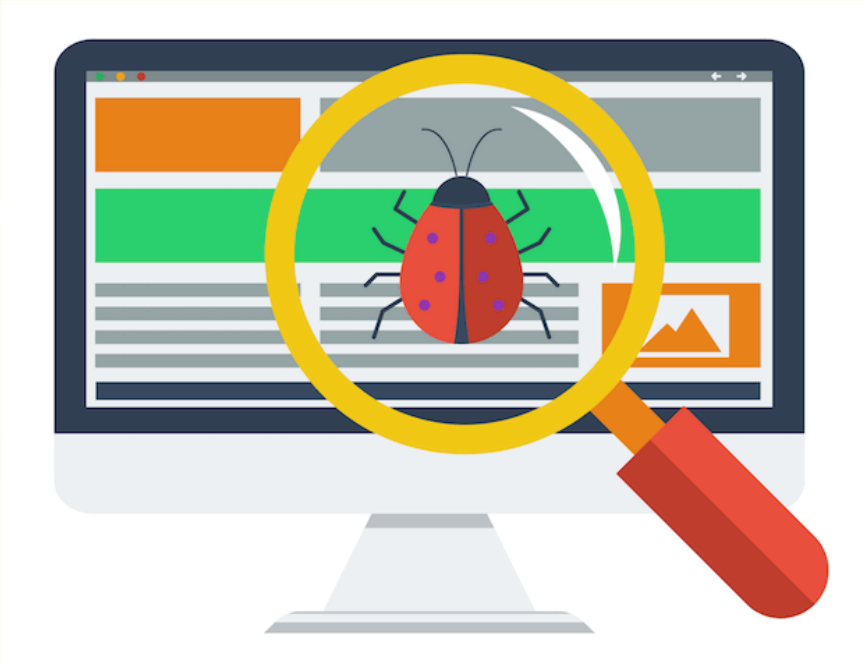
ابزاری است که به کمک آن می توان کامپیوترهای شبکه را از نظر وجود حفره های امنیتی تست کرد.

به استفاده از ابزارهای موجود یا بررسی دستی برای کشف آسیب پذیری ها عمل vulnerability scanning می گویند.

ها Vulnerability scanner

ابزارهای قدرتمند زیادی در این زمینه موجود هست که در این قسمت به بخشی از آن ها اشاره می شود:

- Accountix
- Nikto
- Netsparker
- Nessus
- X-scan
- Openvas
- Owasp zap
- و ...



Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition)

File Actions Tools Configuration Help

New Scan

Tools Explorer

- Web Vulnerability Scanner
  - Web Scanner
  - Tools
    - Site Crawler
    - Target Finder
    - Subdomain Scanner
    - Blind SQL Injector
    - HTTP Editor
    - HTTP Sniffer
    - HTTP Fuzzer
    - Authentication Tester
    - Compare Results
  - Web Services
    - Web Services Scanner
    - Web Services Editor
  - Configuration
    - Application Settings
    - Scan Settings
    - Scanning Profiles
  - General
    - Program Updates
    - Version Information
    - Licensing
    - Support Center
    - Purchase
    - User Manual
    - AcuSensor

Report | Start URL: http://www.[redacted]:80/ | Profile: Default | Stop | Pause

Scan Results	Status
Scan Thread 1 (http://www[redacted] ..	Scanning
Web Alerts (16)	
Blind SQL Injection (4)	
Cross site scripting (verified) (5)	
HTML form without CSRF protection ...	
User credentials are sent in clear te...	
Clickjacking: X-Frame-Options heade...	
Cookie without HttpOnly flag set (1)	
Password type input with auto-comp...	
Network Alerts	
Port Scanner (12)	
Open Port 22/ssh	
Open Port 25/smtp	
Open Port 21/ftp	
Open Port 53/domain	
Open Port 80/http	
Open Port 110/pop3	
Open Port 143/imap	
Open Port 443/https	
Open Port 465/smtps	
Open Port 995/pop3s	
Open Port 3306/mysql	
Open Port 8443/https-alt	
Knowledge Base	
Site Structure	

Alerts summary 16 alerts

acunetix threat level

Level 3: High

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Total alerts found 16

- High 9
- Medium 4
- Low 2
- Informational 1

Target information http://www[redacted]80/

Statistics 12360 requests

Progress 9.33%

Activity Window

```
10.23 13:04.54, [high] Blind SQL Injection "/product_category.php" on parameter "status"
10.23 13:05.48, [high] Blind SQL Injection "/news.ajax.php" on parameter "id"
10.23 13:06.05, [high] Cross site scripting (verified) "/news.ajax.php" on parameter "id"
10.23 13:08.07, Open port 3306 - mysql
10.23 13:14.49, Open port 8443 - https-alt
```

Application Log | Error Log

Web Scanner | Scanning 1 website(s) ... | Number of websites left to scan : 1

اسکن اتوماتیک سایت کافیست؟

نکته مهم راجع به اسکنرها این است که حتی اگر یک اسکنر نتواند برای یک کامپیوتر vulnerability پیدا کند, دلیل بر امن بودن آن کامپیوتر نیست چون هر vulnerability scanner از یک database استفاده می کند که الزاما همه آسیب پذیری ها را پوشش نمی دهد.

نتیجه

ارزیابی امنیتی انجام شده توسط متخصصین، می تواند جلوی بسیاری از مشکلات محتمل در آینده را گرفته و امنیت را برای سازمان ها به ارمغان آورد.

منابع

- Tutorialspoint.com
- Incapsula.com
- Owasp.org
- …

از توجه تان متشکریم