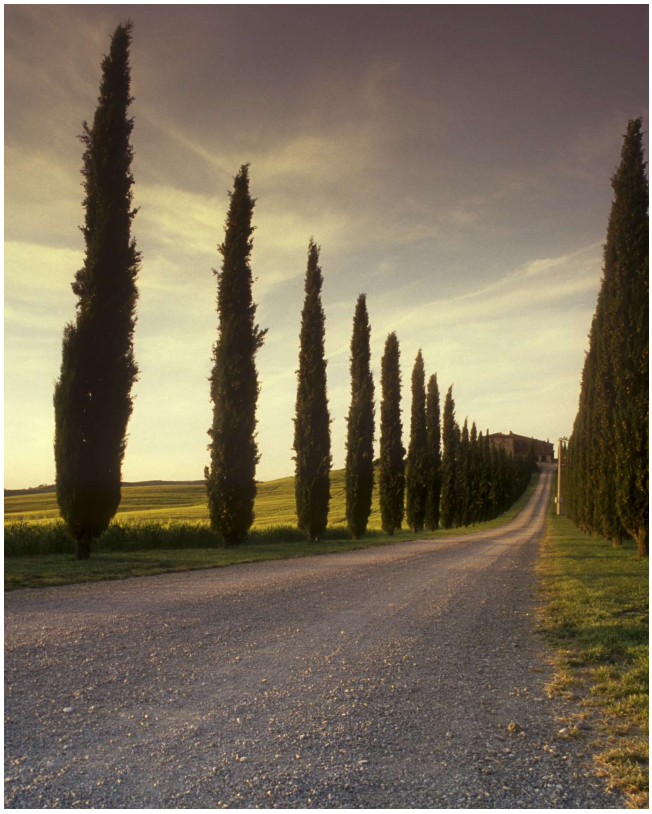
MRCO24 RECON METHODOLGY



hi!

i am mrco24

Admin at Gray Hat Hacker's Community

I am a security geek.

Love to explore the security faults.

I am in this field about 3 years.

So i have taken many from this field

now it's my time to give back ❤

contact us :

Fb id : https://web.facebook.com/MRCO24

page : https://web.facebook.com/mrco24n/

Gorup : https://web.facebook.com/groups/grayhathackerscommunity

youtube channel : https://www.youtube.com/channel/UCakzx9mgKjh9V2CjwCJ7kwA

MRCO24 RECON METHODOLGY

Recon বা ইনফর্মেশন গেদারিং বলতে আমাদের প্রথমে যেটা করতে হয় সেটা হলো

subdomain Enumeration

Subdomain ফাইন্ড করার জন্য আমরা নিচের টুলস গুলা ব্যবহার করবো ।

1. Subfinder
2. Assetfinder
3. Amass
4. Sublist3r

টুলস এর ব্যবহার কমান্ড :

Subfinder == subfinder -d tesla.com -o sub.txt

Assetfinder == assetfinder --subs-only tesla.com -o sub.txt

Amass == amass enum -d tesla.com -o sub.txt

Sublist3r == python3 sublist3r.py -d tesla.com -o sub.txt

website ব্যবহার করে subdomain ফাইন্ড করা।

1. https://dnsdumpster.com/
2. https://spyse.com/tools/subdomain-finder
3. https://www.nmmapper.com/sys/tools/subdomainfinder/
4. https://searchdns.netcraft.com/

এখন আপনাদের অনেক এর মনে হতে পারে যে আমরা উপরের টুলস গুলা থেকে subdomain ফাইন্ড করছি তাহলে ওয়েব সাইট দিয়ে কেন subdomain ফাইন্ড করব। কারণ এর মাধ্যমে আমরা উইনিক subdomain পেতে পারি এই জন্য।

এর পরও বুঝতে অসুবিধা হলে এই ভিডিও টা দেখে আসতে পারেন।

ভিডিও লিংক : https://youtu.be/JyUKafF2fjY

MRCO24 RECON METHODOLGY

SUBDOMAINS BURT-FORCING PureDNS USING

Subdomain বুর্টফোর্সিং। Subdomain বুর্টফর্সিং করার কারণ, আমরা যত বেশি subdomain পাবো তত বাগ পাওয়ার সম্ভাবনা বেড়ে যাবে। মূলত একটি ডোমেইন এর ৫/৬ টা লেয়ার থাকে এবং এই ব্রুটফোর্সিং এর মাধ্যমে এই লেয়ার এর ভিতরে থাকা subdomain গুলো পেতে সাহায্য করে থাকে।

Subdomain ব্রুটফোর্সিং করতে আমরা PureDNS টুলস ব্যবহার করবো।

(Optional) Optional রাখার কারন আমরা যারা বিগেনার তাদের ভক্স নেই এই জন্য এই টুলস টা আপনার পিসি তে ব্যবহার করলে আপনার নেটওয়ার্ক জ্যাম হয়ে যেতে পারে এবং এই টুলস টাই অনেক সমায় লাগে সে ক্ষেত্রে আপনার পিসি অফ বা বিদ্যুৎ চলে গেলে অফ হয়ে যাবে এই জন্য।

টুলস এর ব্যবহার কমান্ড : puredns bruteforce /root/wordlist/bitquark-subdomains-top100000.txt canva.com -r /root/wordlist/ resolvers.txt -w output.txt

cat subdomain.list | xargs -n1 puredns bruteforce /root/wordlist/50000sub.txt

টুলস এর কমান্ড এর যেখানে আমি canva.com দিয়েছি সেখানে আপনারা আপনাদের মাইন টার্গেট এর নাম দিবেন

এর পরও বুঝতে অসুবিধা হলে এই ভিডিও টা দেখে আসতে পারেন।

ভিডিও লিংক : https://youtu.be/9_DMeyj_mDA

MRCO24 RECON METHODOLGY

তারপর আমরা ব্যবহার করবো

Httprobe টুলস

Httprobe টুলস কেনো ব্যবহার করবো?

httprobe টুলস টা আমদের subdomain কে কিছুটা ফিল্টার করে লাইভ subdomain গুলা বাছাই করতে সাহায্য করবে এবং আরো বেশি subdomain ফাইন্ড করতে সাহায্য করবে।

Tools ব্যবহার এর কমান্ড : cat sub.txt | httprobe > sub1.txt

তার পর এই কমান্ড টা দিবেন sort sub.txt | uniq > main.txt

এই কমান্ড টা উপর থেকে যত গুলা subdomain পেয়েছেন তার ভিতরে যদি সেম subdomain দুইতা থাকে তাহলে তার ভিতর থেকে একটি subdomain রিমুভ করে দিবে ফলে কোন subdomain দুইটা থাকবে না আপনার ফাইল এর ভিতরে

এর পরও বুঝতে অসুবিধা হলে এই ভিডিও টা দেখে আসতে পারেন।

ভিডিও লিংক : https://youtu.be/ZjisOjNK4YA

MRCO24 RECON METHODOLGY

Subdomain Takeover

puredns / Httprobe ব্যবহার করে subdomain ফাইন্ড করা হয়ে গেলে| ফাইন্ড করা সকল subdomain গুলো এক সঙ্গে এবার subdomain takeover হয় নাকি সেটা দেখবো।

Subdomain takeover চেক করার জন্য আমরা

Sub 404 tools (এই টুলস টা আমি Prefer করবো ব্যবহার করার জন্য কারণ এটা ইনস্টল করা বা ব্যবহার করা দুটোই সহজ)

বা Nthim tools

টা ব্যবহার করবো

Tools ব্যবহার এর কমান্ড :

Sub 404 tools : python3 sub404.py -f /root/tools/sub.txt

NtHiM : NtHiM -f hostnames.txt

তার পর এই টুলস থেকে যে subdomain গুলো পাবো সেগুলো subdomain takeover হয় কি না সেটা দেখবো।

যাদের বুঝতে অসুবিধা হচ্ছে তাদের জন্য subdomain takeover এর

ভিডিও Link : https://youtu.be/NzvlHwLb1Gg

MRCO24 RECON METHODOLGY

web page screenshot :

এবার ওয়েবসাইট স্ক্রিনশট নেওয়ার পালা যার মাধ্যমে আমরা subdomain এ ভিজিট না করেই subdomain এর সব কিছু দেখতে পারবো। কোন subdomain এর কোন কোন অপশন আছে এটা জানতে পারবো এবং এটার মাধ্যমে ওই অপশন গুলাই কি কি Attack Perform করতে পারবো তার একটা ধারণা পেয়ে যাবো।

এর জন্য আমরা Acuatone টুলস ব্যবহার করবো

টুলস এর কমান্ড : cat sub.txt | aquatone

এর পরও বুঝতে অসুবিধা হলে এই ভিডিও টা দেখে আসতে পারেন।

ভিডিও লিংক :

Live subdomain Find

এবার আমরা লাইভ বা ভালো subdomain গুলো বাছাই করবো কারণ উপর থেকে আমার যতগুলা subdomain ফাইন্ড করেছি তার ভিতরে অনেক subdomain ডেড বা নষ্ট। লাইভ subdomain বাছাই করার জন্য আমার দুটি টুলস ব্যবহার করতে পারি।

১. massdns (Recommended)

২. httpx

MRCO24 RECON METHODOLGY

এই টুলস এর ভিতরে যেকোনো টুলস ব্যবহার করতে পারেন এই টুলস গুলা আপনার all subdomain থেকে লাইভ subdomain গুলা বাছাই করে দিবে কারণ যে subdomain গুলা ডেড, সে subdomain গুলো তে আপনি হান্টিং করতে পারবেন না বা ডেড subdomain কোন কাজেও আসবে না এবং এর মাধ্যমে আপনি ভালো subdomain গুলো বাছায় করে সে গুলাই তে হান্টিং করতে পারবেন।

Tools ব্যবহার এর কমান্ড :

massdns -r /root/wordlist/resolvers.txt -t A -o S -w results.txt sub.txt

বিদ্রোহী উপরের কমান্ড এর ভিতরে যেখানে sub.txt দেখছেন সেখানে আমাদের সব subdomain আছে। আর results.txt এর ভিতরে আমাদের লাইভ subdomain গুলো আছে

আর আমাদের লাইভ subdomain গুলা ফাইন্ড করা হয়ে গেলেও দেখবেন সেখানে অনেক অতিরিক্ত জিনিস subdomain গুলাই অ্যাড করা আছে সেগুলা রিমভ করতে আমরা এই কমান্ড ব্যবহার করব cat results.txt | sed 's/A.*// ; s/CN.*// ; s/\..$//' এই কমান্ড ব্যবহার করার পর আপনার গুলা subdomain সুন্দর ভাবে শো করবে।

এর পরও বুঝতে অসুবিধা হলে এই ভিডিও টা দেখে আসতে পারেন।

ভিডিও লিংক : https://youtu.be/Pi6UN5G5i7s

Open Port Checking

উপর থেকে আমরা যে লাইভ subdomain পেয়েছি সেগুলার open Port check করবো

Tools:

১. Naabu (Recommended)

২. Nmap

MRCO24 RECON METHODOLGY

ওপেন port আমরা কেন চেক করবো? ওপেন port চেক করার কারণ। অনেকে এই ওপেন port টা চেক করেনা কিন্তু ওপেন port গুলা চেক করার মাধ্যমে আমরা খুব সহজে অনেক ক্রিটিক্যাল বাগ পেতে পারি যেমন Port 21 এর Ftp Login ইত্যাদি।

Tools এর কমান্ড :

Nabbu : naabu -list sub.txt

naabu -p 21 -list canva.txt

Nmap : nmap –iL sub.txt

এর পরও বুঝতে অসুবিধা হলে এই ভিডিও টা দেখে আসতে পারেন।

ভিডিও লিংক : https://youtu.be/dHU_ZgZnVA0

OSINT:

Credentials Stuffing:

এটার মাধ্যমে আমরা আমাদের টার্গেট এর কোনো ডাটা লিক হলে সেখান থেকে আমরা Gmail, Password, Credit Card ইত্যাদি সংগ্রহ করতে পারি।

এটার জন্য আমরা যে টুলস ইউজ করবো :

টুলস নাম :

১. Breach Parse (সার্ফেস ওয়েব)

২. Pwndb (ডার্ক ওয়েব ডাটা লিক) (এই টুলস টা ব্যবহার করতে হলে আপনার পিসি তে টর ইন্সটল থাকতে হবে)

Breach Parse commnd: ./breach-parse.sh @tesla.com tesla.txt

Pwndb commnd: pwndb.py --list teslasub.txt --output 127.0.0.1:9150 --proxy

MRCO24 RECON METHODOLGY

এই টুলস গুলা আসলে করবে কি?

এই টুলস গুলা আপনার টার্গেট এর Leaked Data গুলা আপনাদের খুঁজে এনে দিবে। ধরুন এক সপ্তাহ আগে আপনার টার্গেট এর ডাটা লিক হয়েছে এবং সেটা ব্ল্যাক হ্যাট কোনো না কোনো জায়গায় এটা শেয়ার করেছে। সেখান থেকে আপনাকে ডাটা গুলা কালেক্ট করে দিবে এবং এই ডাটা গুলার মাধ্যমে আপনি আপনার টার্গেট এর ইউজার বা Employee দের একাউন্ট এ অ্যাক্সসেস পেয়ে যেতে পারেন।

All Subdomain CloudFlare Check :

এবার আমরা উপর থেকে যতগুলা subdomain ফাইন্ড করলাম, সব গুলার ভিতরে কোন গুলাই CloudFlare আছে আর কোন গুলাই নাই সেটা দেখবো।

এটার জন্য আমরা নিচের টুলস ব্যবহার করবো

Tools এর নাম : cf-check

Command Line : cf-check -d livesub.txt

CloudFlare চেক করা হয়ে গেলে আমরা দেখবো কোন গুলাই CloudFlare নেই তার ভিতর থেকে একটা ইউনিক subdomain কে বেছে নিবো এবং খেয়াল রাখবেন সেই subdomain টা যেনো http হয়। আশা করি আপনারা সবাই জানেন যে http,HTTPS এর তুলনায় সিকিউরিটি অনেক কম হয়ে থাকে।

এর পরও বুঝতে অসুবিধা হলে এই ভিডিও টা দেখে আসতে পারেন।

ভিডিও লিংক : https://youtu.be/GVePkfduzcQ

এখন তাহলে আমরা সিঙ্গেল subdomain এ হান্টিং করবো কারণ উপর থেকে আমরা একটি সিঙ্গেল subdomain কে বাছায় করে নিয়েছি।

MRCO24 RECON METHODOLGY

Critical File / Sensitive Information Disclosure Bug find

এই Bug টা Find করার জন্য আমরা ব্যবহার করতে পারি

১. Ffuf

২. Burpsuite

Ffuf টুলস এর কমান্ড : ffuf -c -w /root/wordlist/Critical.txt -u https://canva.com/FUZZ -mc 200,302,301,403,401,500 2>/dev/null

Wordlist ডাউনলোড লিংক : https://github.com/mrco24/Critical-word/blob/main/Critical%20word

এটার মাধ্যমে আমরা আমাদের সিঙ্গেল টার্গেট এর Critical বাগ পেতে পারি খুব সহজে।

ভিডিও লিংক : https://youtu.be/DwnaC_mFJ04

Github Droking :

এটার মাধ্যমে আমারা আমাদের টার্গেট এর খুব সহজে বাগ পেতে পারি এটার জন্য আমরা GitDorker টুলস ব্যবহার করব এই টুলস টা অটোমেটিক Github Dorking করে তার রেজাল্ট আপনাকে শো করবে আপনাকে মানুলায় করতে হবে না

টুলস এর command : python3 GitDorker.py -tf *tokensfile* -org canva

এবং নিচের ওয়েবসাইট এ গেলে টুলস এর সকল ব্যবহার বুঝতে পারবেন

ওয়েবসাইট লিংক : shorturl.at/beoCM

MRCO24 RECON METHODOLGY

Manual target checking using advanced search engine

ম্যানুয়ালি টার্গেট চেকিং :

১. Shodan

২. Censys

৩. Google Dorking

এবার আমরা আমাদের সিঙ্গেল টার্গেট কে উপরের সার্চ ইঞ্জিন গুলো ব্যবহার করে ম্যানুয়ালি চেক করবো।

Shodan এর ব্যবহার : shorturl.at/eDGH3

Censys এর ব্যবহার : https://gbhackers.com/shoda-censys-internet/

Google droks এর ব্যবহার : https://github.com/mrco24/Google-Droks/blob/main/dork.txt

OSINT এর ব্যবহার : https://gbhackers.com/theharvester-information-gathering-tool/

এগুলোর মাধ্যমে ভালনারেবল subdomain বা টার্গেট কোম্পানির subdomain গুলার ব্যবহৃত টেকনোলজির ভার্সন শো করবে তখন সেই ভার্সন অনুযায়ী CVE খুঁজে দিবে এবং ।। আপনাকে আর আপনার টার্গেট এর সেনসিটিভ ডাটা খুজে বের করতে সাহায্য করবে যার মাধ্যমে আমরা বাগ ফাইন্ড করতে পারি।

MRCO24 RECON METHODOLGY

How to Web Technology Find

ওয়েব টেকনোলজি ফাইন্ড :

ওয়েব টেকনোলজি ফাইন্ড করার জন্য আমারা

Wappalyzer এই Browser Extension টা ব্যবহার করবো যার মাধ্যমে আমরা ওয়েবসাইট এর ওয়েব টেকনোলজি বা ফ্রেমওয়ার্ক বা ওয়েব ভার্শন সম্পর্কে জানতে পারবো যা আমাদেরকে CVE ফাইন্ড করতে সাহায্য করবে এবং বাগ ফাইন্ড করতে সাহায্য করবে

Wappalyzer Browser Extension Link :
https://chrome.google.com/webstore/detail/wappalyzer/gppongmhjkpfnbhagpmjfkannfbllamg?hl=en

হান্টিং এ নতুনদের এর জন্য কিছু টিপস ঃ

১। যে পগ্রাম বা যে ওয়েবসাইট এই হান্টিং করেন না কেন সর্ব প্রথম সেখানে একটি অ্যাকাউন্ট করে নিবেন

এতে আপনি রিকন বা হান্টিং এর সময় বেশি উরলস বা বেশি প্যারামিটার পাবেন যেটা আপনাকে বাগ পেতে সাহাজ করতে পারে। এবং আপনার অ্যাকাউন্ট খুলার সময় সেখানে আপনি অনেক গুলা অ্যাটাক পারফ্রমে করে ফেলতে পারবেন এই যেমন ধরুন

১। sqli

২। account takeover

৩। xss

৪। otp baypass

৫। gmail verify baypass

MRCO24 RECON METHODOLGY

Etc

২। যে প্রোগ্রাম বা যে ওয়েবসাইট এ হান্টিং করবেন সেই পগ্রাম এ নুন্নতম ১০ দিন সমায় দিন

কারণ দুই এক দিন সমায় দিয়ে কখন ও ওই পগ্রাম বাগ পাবেন না কারণ ওই পগ্রাম এ হান্টিং করে চলে গেছে কোন বাগ না পেয়ে । কারণ গাছে থাকা উপর উপর আম সবাই দেখে ভিতর এর আম সুধু তারাই দেখে যারা সমায় দিয়ে গাছের পাতা সরাই খুজে বের করে। কম সমায় এ হান্টিং করে বাগ নাও পেতে পারেন তাই হাল না ছেরে দিয়ে লেগে থাকবেন এতে করে ওই একটি প্রোগ্রাম এ আপনি যত সমায় দিবেন তত ওই প্রোগ্রাম এর গভিরে আপনি যেতে পারবেন এবং আসা করে যায় আপনি ইউনিক বাগ পেতে সক্ষম হবে ইনশাল্লাহ

৩। সঠিক প্রোগ্রাম বাছায় করা

একটি সঠিক প্রোগ্রাম আপনাকে এক এ একাধিক বাগ এবং ভালো দিতে পারে সুতরাং প্রোগ্রাম ঠিক করার সমায় এটা মাথায় রাখুন

উপরে ব্যবহার করা সকল টুলস এর ইন্সটল কমান্ড দেও হল আপনাদের সুবিধার জন্য

```
git clone https://github.com/mrco24/install-tools.git

cd install-tools

chmod 777 *

./installation.sh
```

```
git clone https://github.com/JoyGhoshs/0install.git

cd 0install

chmod 777 *

./0install
```

MRCO24 RECON METHODOLGY

এই টুলস দুটি ইন্সটল দিলে আপনাদের উপরে ব্যবহার করা বেসির ভাগ টুলস হয়ে যাবে। এবং টুলস রান করার পূর্বে go lang টা download করে নিবেন এই Link : https://go.dev/dl/ থেকে তার পর এক্সট্রা হেয়ার করে নিবেন নাহলে অনেক সমস্যার সম্মুখিন হতে পারেন

---------->>>

go *1.15, 1.16*

GO111MODULE=on go get github.com/d3mondev/puredns/v2

go 1.17+

go install github.com/d3mondev/puredns/v2@latest

যদি আপনার go ভার্সন 1.15, 1.16 তাহলে উপরের তা ইন্সটল দিবেন আর 1.17+ হলে নিচের টা ইন্সটল দিবেন ইন্সটল দেও হয়ে গেলেও আপনার puredns টুলস কাজ করবে না ।। সে জন্য আপনাকে এখন আপনার লিনাক্স এর ফাইল ম্যানেজার এ গিয়ে go ফাইল এ জেতে হবে তার পর bin ফাইল যেতে হবে| ওখানে গেলে দেখতে পাবেন puredns আছে তখন ওখানে মাওইস এর রাইট বাটন এ ক্লিক করে টার্মিনাল ওপেন করবেন এবং ও খানে কমান্ড দিবেন chmod 777 * । তার পর আবার ফাইল ম্যানেজারে গিয়ে বিন ফোল্ডার ভিতরে থেকে puredns কে কপি করে ফাইল system এর ভিতর থেকে প্রথমে user তারপর local তারপর bin ফোল্ডার যেতে হবে সেখানে আপনার কপি করা puredns কে পেস্ট করে দিবেন তার পর সেখানে উপরের নেই টার্মিনাল ওপেন করবেন এবং আবার ও chmod 777 * command দিবেন এখন আপনি আপনার টার্মিনাল এর যেকোনো জায়গা থেকে puredns ব্যবহার করতে পারবেন

MassDns :

git clone https://github.com/blechschmidt/massdns.git

cd massdns

make

sudo make install

MRCO24 RECON METHODOLGY

subdomain resolvers.txt Download Link :

https://github.com/blechschmidt/massdns/blob/master/lists/resolvers.txt

subdomain brute force wordlist Download Link :

https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/DNS/bitquark-subdomains-top100000.txt

subdomain takeover /sub404 tools

git clone https://github.com/r3curs1v3-pr0xy/sub404.git

install dependencies: pip install -r requirements.txt

cd sub404

pip3 install -r requirements.txt

NtHiM/ tools

cargo install NtHiM

MRCO24 RECON METHODOLGY

git clone https://github.com/TheBinitGhimire/NtHiM

cd NtHiM

cargo build

cd target/debug

apt-get update --fix-missing

aquatone-tool এই লিংক এ গেলে সুন্দর ভাবে aquatone-tools ইন্সটল করার নিয়ম ও কমান্ড দেও আছে

https://www.geeksforgeeks.org/aquatone-tool-for-domain-flyovers/

cf-check:

go get -u github.com/dwisiswant0/cf-check

Breach Parse:

https://github.com/hmaverickadams/breach-parse

pwndb

https://github.com/davidtavarez/pwndb

আমার লেখার ভিতরে যদি কোন ভুল ত্রুটি হয়ে থাকে তাহলে ক্ষমা দৃষ্টি তে দেখবেন ধন্যবাদ আসসালামুয়ালাইকুম সবাইকে