Cybersecurity

Menemukan Inspirasi untuk dirimu sendiri

Whoami

Romi Syuhada a.k.a Ni’am Habibiy Sahid
Senior Security Consultant @ xtremax

Specialty on Offensive security – penetration test, red team

- Involved in security engineer day-to-day task (manage vault, EDR, siem, VA internal etc.)
- Involved in security operations : patch assessment, risk acceptance, Security Assesment of RFC documents, WAF/webserver log analyze
- Center of Excellence : presales activities, act as SME, estimate cost of vapt, document creation, etc.

Seperti apa sih aktifitas cybersecurity itu?

Kenyataannya

Banyak aktifitas Cybersecurity ranahnya tidak sampai membuat sesuatu

	Aktifitas	
	Patch Assesment	Melakukan analisa patching dan menghitung ulang resiko berdasarkan environment dari system pada organisasi
	Log Review	Review log pada organisasi dan memastikan tidak ada masalah, membuat laporan
	Security Event Analysis	Menganalisa email yang mencurigakan, memastikan apakah legitimate atau phishing Menganalisa log pada waf yang web nya di curigai ada serangan
	Security awareness	Membuat semua anggota organisasi lebih aware terhadap serangan atau pengamanan informasi pribadi.
	Etc.	dan yang lain lain, blue team activities banyak, dan kebanyakan Analisa itu memanfaatkan tools yang ada dan melakukan proses manajemen aktifitas nya.

Red team Activities

Banyak aktifitas Cybersecurity ranahnya tidak sampai membuat sesuatu

Aktifitas	Deskripsi	Objektif
Pentest	Testing keamanan aplikasi / infrastruktur.	- menemukan celah yang membuat pentester berhasil menguasai system - menemukan celah keamanan pada aplikasi (meskipun tidak dapat meng-compromise system) sebanyak mungkin -> checklist OWASP - mengidentifikasi resiko pada aplikasi - Tidak menemukan kerentanan apapun pada aplikasi setelah melakukan pentest
Vulnerability Assesment	Regular scanning menggunakan tools otomatis untuk celah keamanan yang sudah di publish (CVE)	- mengidentifikasi kerentanan - Melakukan penutupan celah tersebut
Red Teaming	Mensimulasikan serangan siber yang dilakukan oleh musuh sungguhan (misalnya, APT - Advanced Persistent Threat).	- Menguji efektivitas keamanan pada perusahaan/oranisasi dari perspektif penyerang (real-world attack simulation). - Mengungkap kelemahan dalam deteksi, pencegahan, dan respons organisasi. - Mengukur kinerja tim keamanan (Blue Team). - Menemukan jalur serangan yang tidak terduga untuk mencapai tujuan bisnis. Misal sudah memantau habis habisan jalur tertentu, eh tapi bisa di serang via wifi - Membuktikan dampak nyata dari celah keamanan pada aset krusial. Compromise laptop bos.

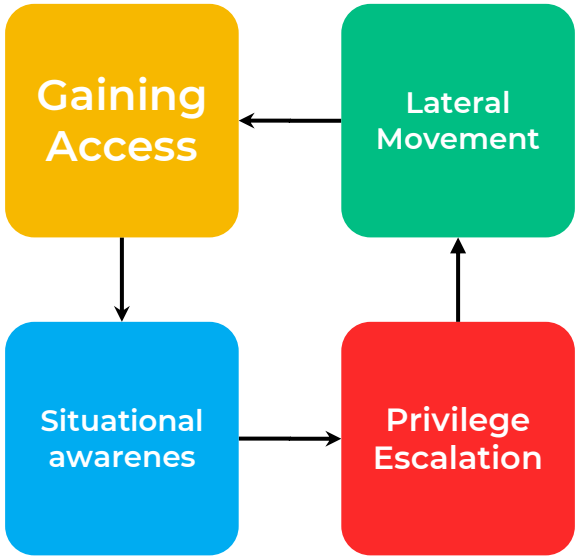
Tapi, semua selalu ada proses nya

Tapi, semua selalu ada proses nya

Compromise Machine – And move to other machine

Gaining Access

- Exploiting vulnerabilities
- Using leaked credentials



Lateral Movement

- Move to other machine
- Pivoting/tunneling to new network

Situational Awareness

- Checking user, system, files
- Checking security tools, AV, EDR,
- Checking if you on sandboxed machine

Privilege Escalation

- Exploit vulnerability
- Used credentials found
- (Ab)used misconfiguration

Masing masing proses ada tools nya

Masih bahas compromise machine

Gaining Access 01

Vulnerabilities	Sqli, ssrf, code execution, command injection, upload file
Processes	Inject SQL, get cloud metadata, execute code system(), execute whoami, upload webshell
Tools	Sqlmap, ssrfmap, exploit-script, exploit-script, exploit-script

Situational Awareness 02

Purpose	Check system, check AV/EDR, check sandboxed machine
Processes	Systeminfo, get av information, get information indicate sandboxed machine
Tools	Reverse shell, edr-checker, Freeze sandbox-evasion checker

Lateral Movement 04

Purpose	Move to other machine, tunneling/pivoting
Processes	Rdp, ssh, pass-the-hash, via metasploit routing
Tools	Xfree-rdp, ssh, evil-winrm, metasploit

Privilege Escalation 03

Technique	Exploit vulnerability, Abuse Misconfiguration, Using credentials, dump credentials
Processes	Use exploit CVE, Use script to abuse the misconfig, Pass-the-hash, dump from lsass
Tools	CVE-xxx-xx exploit.py, PowerUp, rubeus, mimikatz

https://github.com/A-poc/RedTeam-Tools

Semua yang ada berkaitan security selalu ada yang bisa dibuat

- **Untuk menyelesaikan satu masalah ‘kecil’**. Exploit script sebagai proof of concept untuk melakukan exploitasi serangan.
- **Untuk mempermudah proses serangan**. Script untuk mengulang request, script checking files/folder exist untuk deteksi AV terinstall, script untuk membypass AV/EDR
- **Membuat tools lengkap dengan semua fiturnya**. Eg; sqlmap, mimikatz, Rubeus
- Ada tools yang dibuat untuk memastikan tools2 diatas dapat digunakan dan tidak terdeteksi AV/EDR. Eg; Powershell obfuscator, crypter, Pezor
- Atau **membangun infrastruktur yang tidak mudah di deteksi oleh threat analys**.

Batasannya ada pada bagaimana kamu bisa meyakinkan dosbing untuk membolehkan

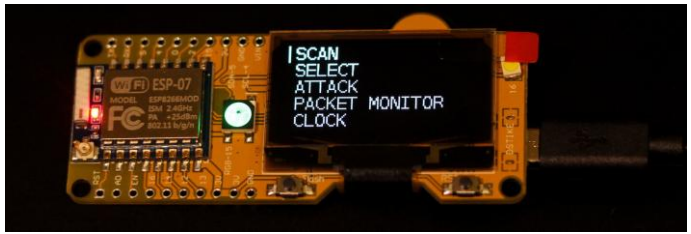
Mungkin bisa jadi Inspirasi

Hardware untuk pentest

- Wifi pineapple
- ESP8266 WIFI deauther

https://github.com/sujayadkesar/Wifi-Deauther

- buat hardware tools menggunakan raspberry pi
- membuat tools yang tidak hanya deauther saja
- Bad USB, USB Cable, dll.

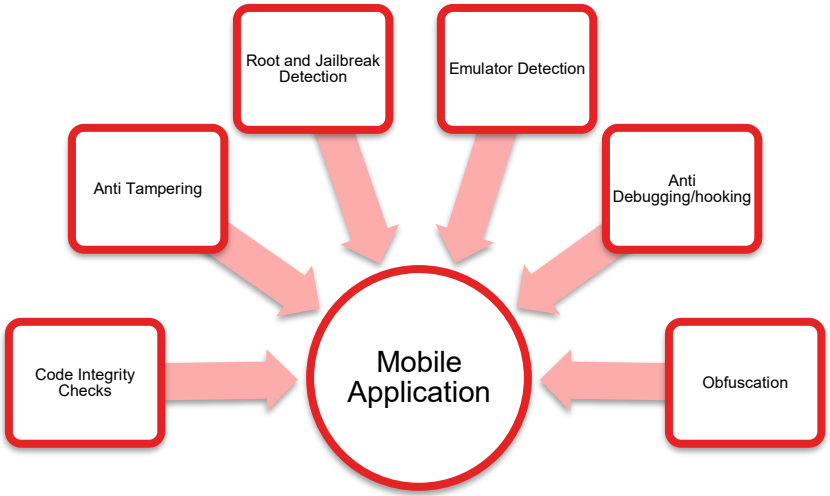


Mungkin Bisa jadi Inspirasi

Mobile Application Runtime Application Self Protection (RASP)

- Standard digunakan di aplikasi perbankan
- Bisa implementasi tools untuk RASP
https://github.com/talsec/Free-RASP-Flutter

- Ataupun sebaliknya, buat tools untuk bypass RASP nya
- Tools : Frida
- Script : Bypass Root detection, SSL pinning bypass, etc.



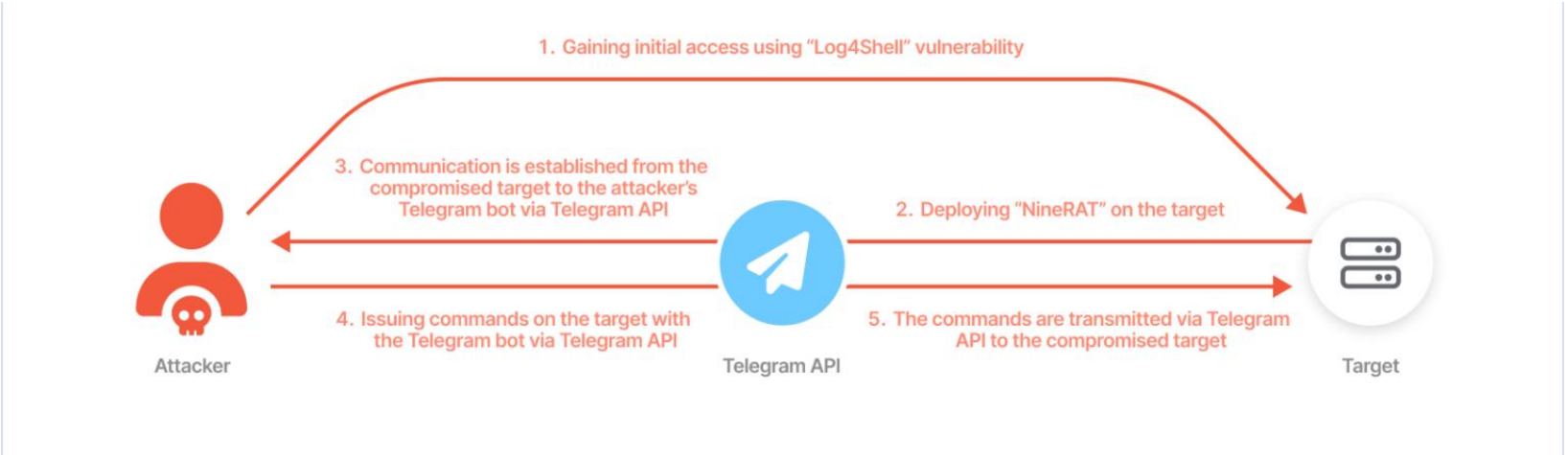
Mungkin Bisa jadi Inspirasi

- Mengontrol via telegram eg; apk undangan nikah
- Mengontrol via google calendar

- Atau menggunakan channel control yang lain :

Whatsapp, google drive, aws lambda, semua yg bisa di program

Command n control (C2)

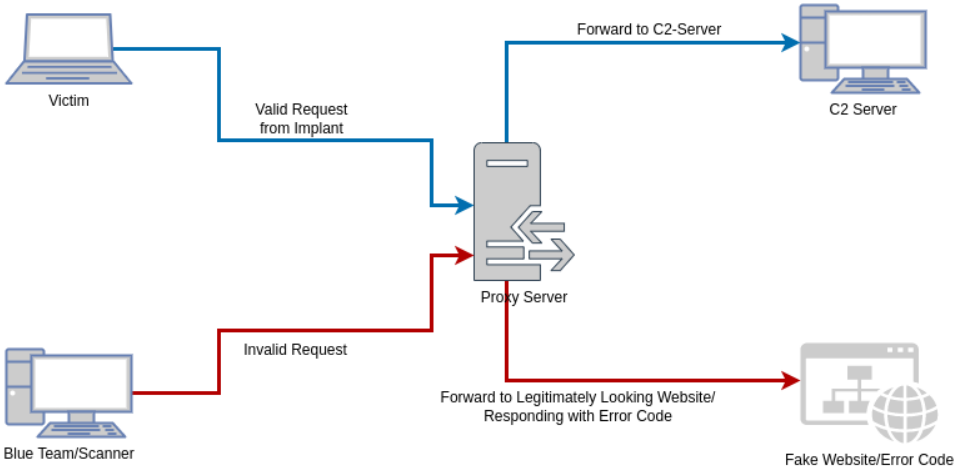


https://www.activecountermeasures.com/threat-hunting-a-telegram-c2-channel/
https://www.netskope.com/fr/blog/telegram-abused-as-c2-channel-for-new-golang-backdoor
https://csirt.or.id/berita/golang-malware-telegram-c2
https://maxlikessecurity.medium.com/hacking-tutorial-google-sheets-command-and-control-c2-server-999e4dbc89fc
https://www.upwind.io/feed/how-adversaries-use-telegram-to-evade-detection

Mungkin Ga boleh jadi skripsi

Red team infrastruktur

- Tujuannya adalah melewati deteksi sistem keamanan dan memperlama umur infrastruktur.
- **Domain Penyamaran** - Menggunakan situs web normal sebagai "tampang depan" untuk menyembunyikan server C2 asli.
- **Parameter Unik** - Manfaatkan parameter URL atau header HTTP khusus sebagai "kunci" komunikasi.
- **Redirector Aktif** - Server perantara akan memfilter semua lalu lintas yang masuk. Hanya permintaan dari agen dengan kriteria unik yang akan diteruskan ke C2.
- **Tampilan Normal** - Blue team akan melihat situs yang tidak mencurigakan saat dikunjungi langsung.
- **Domain Fronting** - Sembunyikan lalu lintas berbahaya di balik layanan tepercaya seperti Cloudflare.



https://medium.com/@frsfaisall/mastering-modern-red-teaming-infrastructure-part-2-building-stealthy-c2-infrastructure-with-312aec7e1e48
https://www.ired.team/offensive-security/red-team-infrastructure/automating-red-team-infrastructure-with-terraform

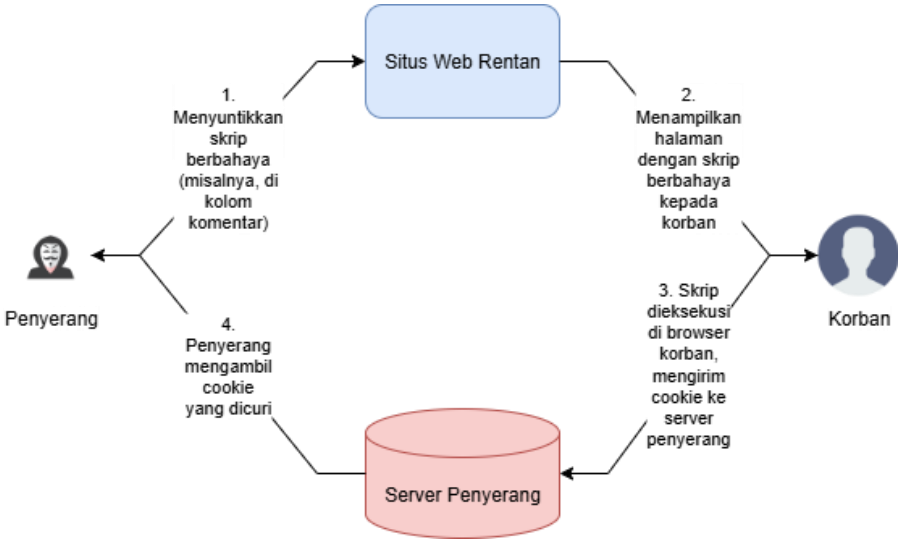
Mungkin Bisa jadi Inspirasi

Website exploitation

- Bikin dashboard stealer untuk proof of concept stealing cookie dari XSS

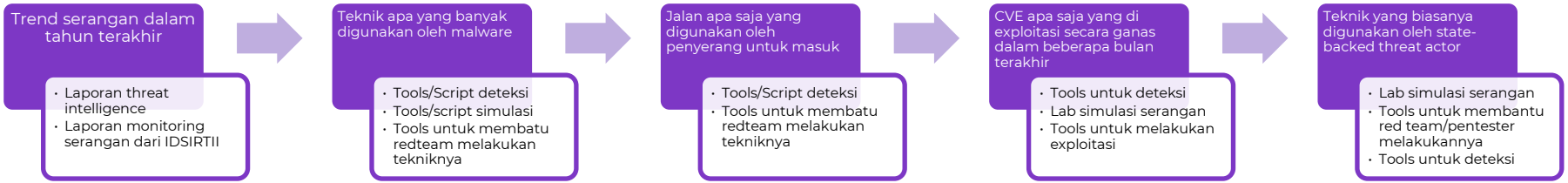
- **very simple POC**
https://github.com/noxvix/Xss-Exploitation

- Apapun Teknik yang kamu baca di internet, coba terjemahkan jadi tools



Berangkat darimana?

Apa dasarnya biar saya bisa angkat tema implementasi atau develop tools ini pas ngomong sama dosen?



https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html
https://www.trendmicro.com/vinfo/id/security/research-and-analysis/threat-reports
https://attack.mitre.org/groups/G0087/

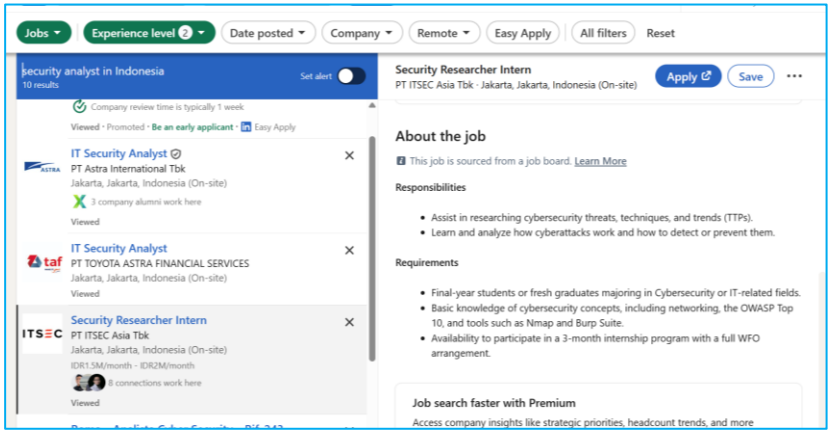
Wajib untuk di cek

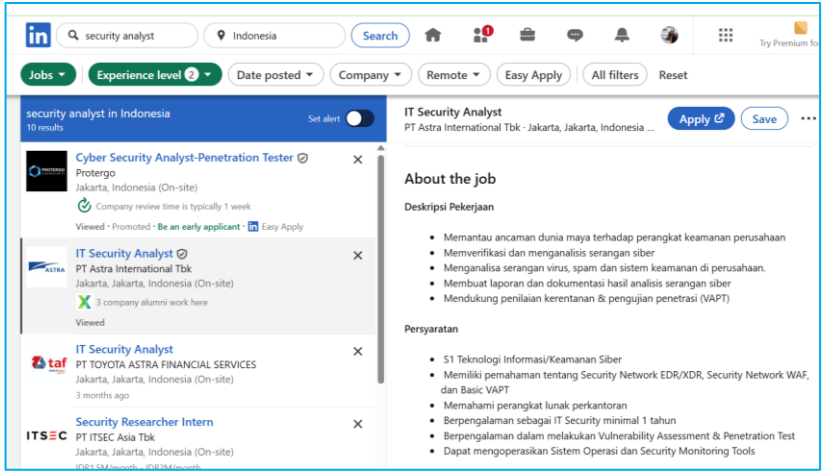
- **Defcon video**
https://www.youtube.com/@DEFCONConference/playlists

- **Blackhat**
https://www.youtube.com/@BlackHatOfficialYT/playlists

Habis lulus, posisi apa yang bisa di kejar?

- Junior penetration tester
- IT Security analyst
- SOC level 1
- Security engineer – product security
- Security researcher - intern





Feeder Role career path

- Security itu ada di level advanced. Ada fondasi ilmu terkait Network/Infra, Programming, dan Operations.
- Bisa juga untuk masuk ke ranah IT yang bukan security terlebih dahulu untuk memperkuat pondasinya.

- Network / Infra : Cloud engineer, Network Administrator
- Programming : Software developer, software engineer, front-end dev, back-end dev, mobile developer
- Operations : IT support, Devops Engineer, Product Engineer

- Setelah cukup pengalaman dan bisa lompat ke security, bisa mengarah ke spesifik teknologi seperti Cloud security engineer / cloud penetration tester

QnA

Waktunya bincang bebas. Bertanyalah sebelum bertanya itu dilarang.