Reconnaisance   pentest methodology

OSINT - open source intelligence

Virus total - website এর কাজ.

200 MB এর কোনো link malicious কিনা, কোন ধরনের
নিচে হলে ভালো

কোন anti virus best — কোম্পানিটাও না.

total 80+ antivirus আছে - sophos, Dr.web

Riskware. dropper. VT.

Virus total নিয়ে কাজ.

Poe.com - poe

অনেক AI integrated আছে

Claude - এ সমস্যা. VPN লাগে.

accurate বেশি

app.any.run — malicious file check করতে পারি

ছবি থেকে location

Phorensic এর part থেকে

Properties check করো

OSINT - Find the cat location from the disk file.

disk

testdisk ch9 —

apt install testdisk

C to copy

I — quit

file select ... 2 ... C click ...

latitude

longitude — |

exiftool

apt install exiftool

cd /media/st_CS_OS/Files/reverdicatia/

exiftool ... info ...

username , email

intitle: index. of ? pdf hacking

mkv

doc ... all

DorkGPT

Dork ... search

doc ... command

ss

wappa

google-hacki

exploit-db.com / google-hacking Database

exploit ... data ...

site:.uni.edu ... link ...

filetype

apache flink

worldwide এর CCTV গুলোতে access
free তে পাবো

user pass মানে default pass

Dorks

shared folder এর - step

2-assign - OSINT (এর পেছনে যা)

learn - threat intelligence tool

operational powers → tactical কে help করে

↓

tactical ← technical "

↓

technical - evidence and artefacts analyse and develop defence

↓

strategic intel - management / উপরের level এর যারা decision নিবে.

MD, CEO

job sector operational level এ বেশি হবে

talos intelligence -

ABuse ch - যত ঝামেলার ফাইল file

আছে

database

Security policy — large doc
sub doc তৈরি

সবার জন্য enforceable.

Subsection বা part (I) Overview — password কেন দরকার

(II) Scope — কাদের জন্য policy তে

(III) Policy — মূল doc.
Subsection
আকারে
do's and don'ts লিখতে

(IV) Enforcement — consequence লিখতে

(V) Definitions:

(VI) Revision History: date of change,
who made change
maybe কোন authorized ছিল
change

Identifying types of policies

(I) Standard — must be followed. it covered
specific area of security

(II) Guidelines; ~~penalty~~ (NSA)
National security agency

যেমন আগের মতো guideline

Procedure — SOP — Standard operating procedure (SOP)
step by step procedure

Security control — firewall, antivirus

AUP — acceptable use policy — ...

password policy — minimum length
password history — 12 or 24 passwords
maximum password age
min password age —
password complexity —

policies affecting personnel management

(I) Non disclosure agreement (NDA): confidential info leak ...
working or after few work engagement was completed.

(II) Onboarding: specific training ...

(III) Offboarding: ...

(IV) continuing education: