2021-2022

Q1ai)

- a keylogger

- physical keylogger

+ find the victims laptop

+ set up a keylogger on a victim’s laptop

- software key logger

- make user download it

- phishing

+ get emails of potential customers

+ create fake website redirecting them to your version of the page

- clickjacking

+ Create fake website with iframe over it, so user thinks they’re sending to real ite

+ send website to user and make them use it

- have bit or typo squatted site, so they might think it’s real

- gain access to database

- Get stuff physically from server

+ find geological location of server

+ steal the storage medium

+ do smart stuff

- SQLi

- XSS ?

- gain admin access

- social engineering

- bruteforce? / offline dictionary attack if you find the hashes

- intercept the requests between the user and the server

+ MITM

+ Network sniffing

Q1aii)

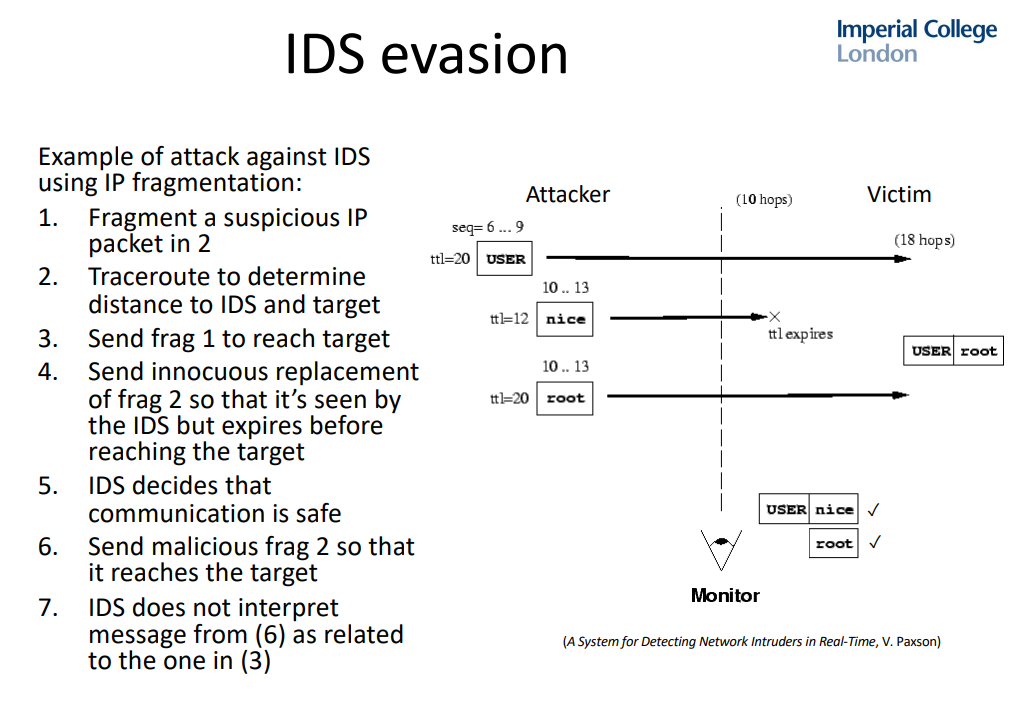
- Create a lot of fake accounts that look legit so it takes longer to process all of them

- Spoof requester IP + browser fingerprint to look like legitimate users

- Hide sus activity in a lot of normal activity, either when using the card or attacking the website

- Obfuscated injected code

- Send malicious code in small packets (ids evasion or something else)



- dynamic code generation so that it can’t detect the same payload

- random time in between payloads so it can’t detect a trend

Q1b. Nothing on the actual site, so no idea

Q2

a)i) TLS is sent over TCP, we can use the same IDS setup for the TCP packet filtering for the TLS filtering, so we only allow TLS to be sent to whitelisted domains.

We could decrypt the data, by intercepting the key initially, this might be too expensive to decrypt every TLS packet.

ii)

- compromise the DNS server of the organization, map a domain name to the ip that the attacker wants to access.

- DNSSEC

- or maybe we can use a proxy on one of the trusted domains, and forward the message

- Disallow any domains that could be used as a proxy

- or maybe we change the trusted whitelist

- Monitor the system for suspicious modifications such as to the whitelist

- DNS rebinding: bypass same origin policy(SOP) by resolving to a different IP address in the initial request, then switching to another IP address in subsequent requests

- DNS tunneling

Alternatively, the attacker can exfiltrate data over UDP – Mitigation: inspect UDP traffic as well

Q2b. No file, can’t do. See 2023 CW feedback for I and ii