TASK 1A

What does the "Not Secure" warning mean in the first picture and what risks does visiting sites with the warning pose?

The "Not Secure" warning indicates that the website does not use HTTPS and instead relies on HTTP. Visiting such sites has risks because the data transmitted between the browser and the server is not encrypted, making it susceptible to interception by attackers. Personal data, login credentials, and any sensitive information entered on such sites can be stolen via man-in-the-middle attacks.

Why does the second site show up as "trusted" to the browser?

The second site is using HTTPS, as indicated by the padlock icon. This means that the site has a valid SSL/TLS certificate, ensuring that the data exchanged between the user and the server is encrypted. It also implies that the identity of the website has been verified by a trusted Certificate Authority (CA), which is why the browser marks it as "trusted."

What other ways are there to detect a phishing/scam site? Are there any tools available online?

Methods to detect phishing/scam sites:

Look for misspellings or suspicious URLs that mimic legitimate sites.

To check for the padlock icon to ensure the site is secure (HTTPS).

To be cautious of unsolicited emails or pop-ups asking for sensitive information.

To inspect the site's domain to ensure it's the official one.

To check for poor grammar or odd design elements, as phishing sites often have these.

Tools available online:

Google Safe Browsing: Can identify potentially unsafe websites.

VirusTotal: Provides a URL scanner to check if a site is safe.

PhishTank: A community-driven site that verifies phishing URLs.

Browser-based phishing filters like those in Google Chrome, Firefox, and Microsoft Edge.

What is typosquatting and how does it relate to the pictures?

Typosquatting is a form of cyberattack where attackers register domain names that are very similar to legitimate domains, often relying on users mistyping the address. For example, instead of "danskebank.fi," a typosquatter might register "danskbak.fi" or "danskebnk.fi" to trick users into visiting the malicious site.

Relation to the pictures: In the second picture, we see "danskebank.io" instead of the expected ".fi" domain, which might be a sign of typosquatting, where a slight variation in the domain name could lead users to a fraudulent website.

What is UDRP and how does it help with combating typosquatting?

The Uniform Domain-Name Dispute-Resolution Policy (UDRP) is a process established by ICANN for resolving disputes regarding the registration of internet domain names, particularly those that are identical or confusingly similar to a trademark or service mark. UDRP allows trademark holders to take action against individuals who register domains similar to their trademarks, thus combating typosquatting.

If you were to own the domain oupsg.org and would be running your crypto banking application at bank.ouspg.org, what domains could you monitor for warning signs of possible phishing attempts against your customers?

You should monitor domains that are visually or phonetically similar to legitimate domain. Examples include:

Typo Variants: bank.ousgp.org, bank.ouspg.com, bnak.ouspg.org

Homograph Attacks: Domains that replace similar-looking characters like "ouspg.org" (with Cyrillic characters).

Different TLDs: bank.ouspg.net, bank.ouspg.co, ouspg-bank.org

Addition/Removal of Words: secure-bank.ouspg.org, ouspgbank.org, oupsg-finance.org

Monitoring tools like WHOIS alerts, DNS monitoring services, and phishing domain tracking tools can help us stay aware of potential phishing attempts targeting your domain.

TASK 2

Questions: Payments

Why do modern payment cards use a chip and not a magnetic stripe?

Modern payment cards use EMV chips (Europay, MasterCard, and Visa) instead of magnetic stripes because chips provide better security. While magnetic stripe cards store static data that can easily be copied or cloned, chip cards generate a unique transaction code for each purchase, making it much harder for fraudsters to reuse stolen data.

What are EMV Certificates and why are they relevant for payment protection?

EMV certificates are cryptographic keys stored on the chip of the card. They are used to authenticate transactions securely by generating a one-time code that can only be used for that specific transaction. This encryption helps protect against card cloning and fraud.

What attacks exist against payment cards?

Card-not-present (CNP) attacks: These occur during online or phone transactions where the cardholder does not physically present the card. Attackers often obtain card details through phishing, skimming, or data breaches and then use the stolen information for fraudulent transactions.

Contactless payment attacks: These include relay attacks, where a malicious device intercepts the communication between the card and the payment terminal to conduct unauthorized transactions. Skimming is another attack where attackers use hidden devices to steal card data wirelessly.

Questions: MFA

How is multi-factor authentication (MFA) used in banking?

MFA is used in banking to provide an extra layer of security. After the user enters their username and password, they must provide another piece of information (such as a one-time password, biometric verification, or a security token) to confirm their identity. This reduces the risk of fraud because even if a password is compromised, the attacker would still need access to the second factor to complete the login.

How does multi-factor authentication increase payment security?

MFA adds an additional layer of protection by requiring users to provide two or more forms of verification before completing a payment transaction. Even if one form (like a password or card number) is compromised, the second factor (such as a one-time password or fingerprint) helps prevent unauthorized access.

What MFA methods are you using in your daily life?

Time-based One-Time Passwords (TOTP): Microsoft Authenticator that generate a time-sensitive code in my university account.

Text Message (SMS): Receiving a code via SMS for login or transaction authorization in my facebook account.

Biometrics: Fingerprint or facial recognition, on my smartphones.

Security Tokens: Physical tokens that generate one-time passwords in my banking account.

What attacks exist against different forms of 2FA?

Time-based One-Time Password (TOTP) attacks:

Phishing attacks: An attacker might trick a user into revealing the TOTP by pretending to be a legitimate service.

Text Message (SMS) attacks:

SIM swapping: Attackers convince the telecom provider to transfer the victim’s phone number to a new SIM card under their control. This allows them to intercept SMS-based codes.

Man-in-the-middle attacks: Hackers intercept SMS codes in transit through vulnerabilities in the cellular network.

TASK 3

1. What kinds of card fraud exist?

Card fraud can take multiple forms:

Card-not-present (CNP) fraud: Occurs when the physical card is not required for the transaction, such as in online or telephone transactions.

Card-present fraud: This involves physical card theft or cloning to make fraudulent transactions.

Contactless payment fraud: This involves exploiting contactless payment systems (NFC), where criminals may use wireless skimming devices to steal card information.

Geographic Prevalence:

Card fraud tends to differ in prevalence based on the region. Countries with advanced EMV (Europay, Mastercard, Visa) chip implementations have seen reduced card-present fraud but increased card-not-present fraud due to a shift in attacker focus.

2. How has the fraud landscape changed between 2008–2019?

During this period, the global fraud landscape has shifted significantly:

Increase in online fraud: With the rise of e-commerce, card-not-present fraud has seen a notable increase as fraudsters target online transactions.

Technologies or regulations impacting card fraud:

EMV Implementation: The rollout of EMV chip technology has reduced card-present fraud, especially in regions with widespread adoption.

Strong Customer Authentication (SCA): Introduced through the EU's Payment Services Directive (PSD2), it has made it more difficult for fraudsters to impersonate legitimate cardholders during online transactions.

3. How has the transaction landscape changed in the same period?

Increased Popularity of Contactless Payments: Contactless payments became more common in this period, especially in retail and transportation sectors.

Rise in Online Transactions: The growth of e-commerce has made online transactions a preferred method for consumers, which has increased the risk of card-not-present fraud.

High-risk Transactions: Transactions without physical verification, such as online purchases, are more susceptible to fraud. This risk has remained consistent from 2008–2019 but has been mitigated somewhat by the introduction of tokenization and MFA.

4. What effect has the internet and e-commerce had on card fraud?

The rise of e-commerce has exponentially increased opportunities for fraudsters. Card-not-present fraud became more prominent as consumers started making more online purchases. The anonymity of online environments and the global nature of e-commerce have made it harder to track and prevent fraud.

5. Why is preventing data breaches important in preventing card fraud?

Data breaches can lead to large-scale theft of cardholder data, which is then used in fraudulent transactions. Preventing data breaches reduces the pool of compromised information available to fraudsters.

Payment card tokenization: Tokenization replaces sensitive card information with a unique identifier or token. This helps to ensure that even if the transaction data is intercepted or stolen, it cannot be reused for fraudulent purposes.

Example: Apple Pay and Google Pay use tokenization to ensure card details are never exposed during transactions.

Summary:

Between 2008 and 2019, the evolution of card fraud was significantly impacted by both technological advancements and the rise of e-commerce. While EMV chip adoption drastically reduced card-present fraud, online transactions became the primary target for fraudsters, resulting in a notable increase in card-not-present fraud. The rise of contactless payments also presented new opportunities for fraud. In response, regulators introduced stronger authentication measures, such as SCA under PSD2, and industries adopted solutions like tokenization to protect against data breaches.

The transaction landscape saw a shift toward online and contactless payments, increasing the need for enhanced security protocols. The global push for data protection, particularly preventing data breaches, became critical in mitigating fraud risks as compromised data could easily be exploited. Technologies like tokenization have helped safeguard sensitive card information, reducing the likelihood of fraud even in the event of a breach.

TASK4

1. What rule descriptions did you get?

When an event is triggered in Wazuh, it associates a rule based on its rule set. The rule look like the following:

Rule ID 554: File integrity event triggered (file creation, modification, or deletion).

Description: Wazuh has detected a file or directory modification in the monitored directory.

Severity Level: High/Medium depending on the nature of the file change.

Details: The integrity of monitored files or directories was altered, triggering the FIM system.

2. What are the MITRE ATT&CK techniques (include ID) Wazuh reports for these events?

Wazuh integrates with the MITRE ATT&CK framework to provide relevant techniques when certain events are triggered. For file integrity monitoring, typical techniques might include:

T1070.004: Indicator Removal on Host: File Deletion.

Description: Adversaries may delete files left behind by the actions they perform to remove evidence of their presence.

T1027: Obfuscated Files or Information.

Description: Adversaries may attempt to conceal their activities by modifying file contents or metadata.

T1107: File Deletion.

Description: Adversaries may delete files to cover their tracks.

3. What is the reported MITRE technique for deleting files or directories inside monitored directories?

When a file or directory is deleted inside a monitored directory, the MITRE ATT&CK technique reported could be:

T1070.004: Indicator Removal on Host: File Deletion.

Description: This technique indicates that adversaries may attempt to delete log files, system files, or other important records to cover their tracks.

This is commonly detected by the Wazuh FIM system as it monitors and logs file changes, including deletions.

4. Explain in your own words where, when, and why should these systems be used. Would they be helpful in banking?

File Integrity Monitoring (FIM) systems like Wazuh should be used in environments where security and integrity of files are critical. These systems are commonly implemented to monitor sensitive directories such as those containing system configuration files, audit logs, customer data, or critical application files.

Where:

In banking environments, especially where sensitive financial data is stored or transmitted.

On servers that host critical financial services applications.

When:

FIM should be used continuously to detect unauthorized changes in files.

It is essential when auditing compliance with regulatory standards such as PCI-DSS or when monitoring security-sensitive environments.

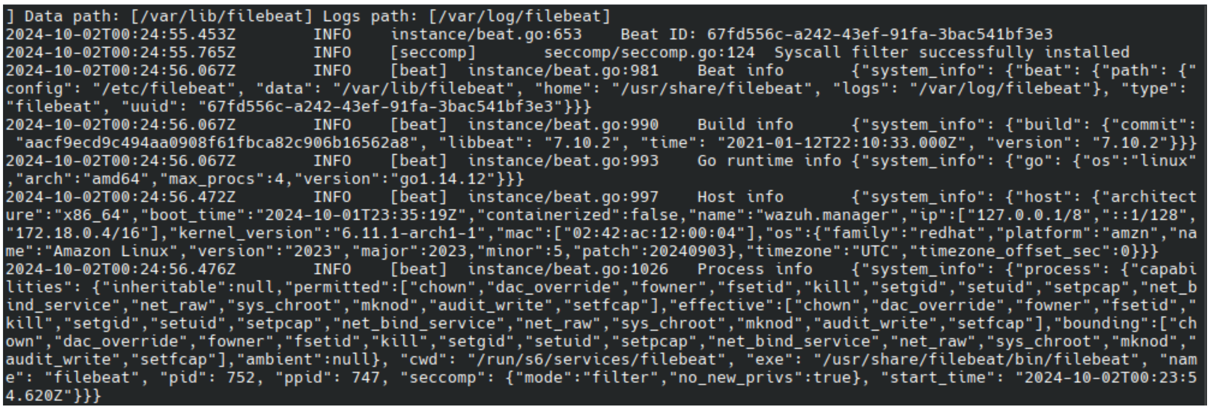
Why:

It helps detect unauthorized file changes that could indicate security breaches, malware infections, or insider threats.

In banking, where customer data and transaction records must remain confidential and unaltered, FIM can alert administrators to potential data manipulation or exfiltration.

Additionally, FIM provides an audit trail for changes, which is invaluable for post-incident forensic analysis.

In the banking sector, Wazuh's FIM can be extremely helpful in ensuring that critical financial data remains untouched and secure, detecting any unauthorized access or tampering.



```
] Data path: [/var/lib/filebeat] Logs path: [/var/log/filebeat]
2024-10-02T00:24:55.453Z        INFO    instance/beat.go:653    Beat ID: 67fd556c-a242-43ef-91fa-3bac541bf3e3
2024-10-02T00:24:55.765Z        INFO    [seccomp]       seccomp/seccomp.go:124  Syscall filter successfully installed
2024-10-02T00:24:56.067Z        INFO    [beat]  instance/beat.go:981    Beat info       {"system_info": {"beat": {"path": {"
config": "/etc/filebeat", "data": "/var/lib/filebeat", "home": "/usr/share/filebeat", "logs": "/var/log/filebeat"}, "type":
"filebeat", "uuid": "67fd556c-a242-43ef-91fa-3bac541bf3e3"}}}
2024-10-02T00:24:56.067Z        INFO    [beat]  instance/beat.go:990    Build info      {"system_info": {"build": {"commit":
 "aacf9ecd9c494aa0908f61fbca82c906b16562a8", "libbeat": "7.10.2", "time": "2021-01-12T22:10:33.000Z", "version": "7.10.2"}}}
2024-10-02T00:24:56.067Z        INFO    [beat]  instance/beat.go:993    Go runtime info {"system_info": {"go": {"os":"linux"
,"arch":"amd64","max_procs":4,"version":"go1.14.12"}}}
2024-10-02T00:24:56.472Z        INFO    [beat]  instance/beat.go:997    Host info       {"system_info": {"host": {"architect
ure":"x86_64","boot_time":"2024-10-01T23:35:19Z","containerized":false,"name":"wazuh.manager","ip":["127.0.0.1/8","::1/128",
"172.18.0.4/16"],"kernel_version":"6.11.1-arch1-1","mac":["02:42:ac:12:00:04"],"os":{"family":"redhat","platform":"amzn","na
me":"Amazon Linux","version":"2023","major":2023,"minor":5,"patch":20240903},"timezone":"UTC","timezone_offset_sec":0}}}
2024-10-02T00:24:56.476Z        INFO    [beat]  instance/beat.go:1026   Process info    {"system_info": {"process": {"capabi
lities": {"inheritable":null,"permitted":["chown","dac_override","fowner","fsetid","kill","setgid","setuid","setpcap","net_b
ind_service","net_raw","sys_chroot","mknod","audit_write","setfcap"],"effective":["chown","dac_override","fowner","fsetid","
kill","setgid","setuid","setpcap","net_bind_service","net_raw","sys_chroot","mknod","audit_write","setfcap"],"bounding":["ch
own","dac_override","fowner","fsetid","kill","setgid","setuid","setpcap","net_bind_service","net_raw","sys_chroot","mknod","
audit_write","setfcap"],"ambient":null}, "cwd": "/run/s6/services/filebeat", "exe": "/usr/share/filebeat/bin/filebeat", "nam
e": "filebeat", "pid": 752, "ppid": 747, "seccomp": {"mode":"filter","no_new_privs":true}, "start_time": "2024-10-02T00:23:5
4.620Z"}}}
```