A diagram of a cyber attack

Description automatically generated

## Why are they red flags? What it means? How does it affect your security? How would you respond to it? What is the policy?

1. **Brute Force Attack:** A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

**What’s the motive behind a brute force attack?**

The most obvious is also the most common: privileged access to restricted data, applications, or resources of all kinds. Identity theft – stealing someone's identity to access their accounts, such as bank accounts or credit cards

**How Brute force affect security?**

These attacks can significantly consume network and system resources, causing performance degradation and potential service disruptions. Precursor to Larger Attacks and can be used to launch more sophisticated attacks, such as spreading malware, data exfiltration, or lateral movement within the network.

**Indicators of a brute force attack:**

* Unusual patterns of failed login attempts
* Failed login attempts from the same IP address into many accounts
* Logging into an account from an unusual IP address
* Successfully logging into an account followed by numerous failed login attempts
* Unusual use behaviour after a successful login
* Increased internet use after a successful login

**How to Prevent Brute Force Attacks**

* Enforce Strong Password Policy.
* Implement Multi-factor Authentication.
* Limit Login Attempts.
* Use a CAPTCHA.
* Monitoring and Incident Response for Brute Force Attacks.
* Secure Coding Practices to Prevent Brute Force Vulnerabilities.
* Intrusion Detection System (IDS)

1. **Activity from blacklisted geolocation:**Blacklisted geolocations are often associated with malicious activity, such as spamming, phishing, or malware distribution. When an IP address is blacklisted, it can lead to a reputation issue, making it difficult for users to access certain services or websites. They may be used by attackers to launch attacks, distribute malware, or steal sensitive information. This can put users’ devices and data at risk of compromise. Could potentially be an employee using a VPN, should be able to monitor which devices are being used. But it depends on the company’s policy regarding where you can access company data from (e.g. if you’re on holiday)
2. **HOW TO COUNTER ACTIVITY FROM A BLCAKLISTED GEOLOCATION?**

**Identify the Blacklisted Geolocation**-

Use geolocation tracking technology to identify the IP address and location associated with the suspicious activity. This will help you determine the region or country where the activity is originating from.

**Verify the Blacklist Status-**

Check the blacklisted IP or domain to confirm its status. This can be done by searching for the IP address or domain on blacklisting databases or contacting the relevant authorities.

**Block the IP Address-**

Immediately block the IP address to prevent further suspicious activity. This can be done by configuring your firewall or web application firewall (WAF) to block traffic from the blacklisted IP address.

**Monitor for Additional Activity-**

Continuously monitor your platform or website for any additional activity from the blacklisted geolocation. This will help you detect and respond to any potential threats in real-time.

**Investigate and Act-**

Investigate the source of the suspicious activity and take appropriate action. This may involve contacting the relevant authorities, reporting the incident to the blacklisting database, or taking legal action if necessary.

1. **Failed privilege escalation detected:** Privileges grant rights for accounts to perform privileged operations within the operating system: debugging, impersonation, etc. Defenders who understand privileges and how attackers may abuse them can enhance their detection and attack surface reduction capabilities.

The following are the most abused privilege constants in malicious software:

* **SeBackupPrivilege:** This privilege causes the system to grant all read access control to any file, regardless of the access control list (ACL) specified for the file.
* **SeDebugPrivilege:** Required to debug and adjust the memory of a process owned by another account.
* **SeLoadDriverPrivilege:** Required to load or unload a device driver.
* **SeRestorePrivilege**: Required to perform restore operations. This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file.
* **SeTakeOwnershipPrivilege:** Required to take ownership of an object without being granted discretionary access.
* **SeTcbPrivilege:** This privilege identifies its holder as part of the trusted computer base. Some trusted protected subsystems are granted this privilege.

To respond to these failed privileges, we will need to enable any auditing to receive event notifications when any tokens have been enabled or disabled. This will allow the analyzation of any escalated privileges to decide whether malicious, or not. Once the event log has been validated/audited the escalation can be removed to ensure only the specific users have the privilege. Following this there will need to be a security group created to monitor the systems and they will be the only ones who will have access to configure any assignees their privileges.

1. **Dormant service account reactivated:**

Even though the accounts are inactive they may still contain valuable personal information such as company data, passwords, financial data etc. By monitoring these accounts, we can promptly identify and deactivate this sensitive information, reducing the risk of exposure and identity theft. By keeping track of inactive accounts, we may detect unusual activity or unauthorized access attempts. This allows us to quickly intervene and take action to prevent possible attempts to compromise security and protect other accounts and associated systems. Monitoring inactive accounts becomes essential in the case of resignation of a user. If a user leaves the organization or gives up their account without deactivating it, that account can become a potential vulnerability. Through monitoring services, we may identify inactive accounts associated with former employees and disable their access to prevent misuse of accounts and protect the organization’s data and system. An additional reason for monitoring inactive accounts is to identify and prevent accounts that have been taken over by hackers to use as backdoor. Hackers can take over an inactive account (to not raise suspicions) and use this privileged access position after his initial malicious access to the corporate network was revoked.

1. **Unusual number of messages marked as unread:**

Unread messages could signal unauthorised access, data leaks, or compromised communication channels. Vigilance and prompt investigation are crucial to prevent further damage.

* Phishing Campaigns:  Cybercriminals often use mass phishing emails to distribute malware or steal sensitive information. If you receive many unread messages with suspicious subject lines or attachments, it could be part of a phishing campaign.
* Malware Distribution: Attackers may flood your inbox with malicious attachments or links. These unread messages could contain malware, such as ransomware or keyloggers, waiting to be activated when opened.
* Credential Stuffing: If you notice numerous unread login-related messages (e.g., password reset requests, failed login attempts), it might indicate attackers trying to gain access to your accounts using stolen credentials.
* Account Takeover Attempts: A sudden influx of unread messages related to account security (e.g., “Your account was accessed from an unfamiliar location”) could signal unauthorised access attempts.
* Data Exfiltration: Attackers might use unread messages to exfiltrate sensitive data. For instance, they could send themselves confidential files or messages containing critical information.
* Denial-of-Service (DoS) Attacks: Overwhelming your inbox with unread messages could be part of a DoS attack, disrupting your communication and potentially masking other malicious activities.

1. **Unusual number of GDPR files deleted**

By deleting GDPR (general data protection regulation) files, users have a denial of access as attackers can deny access to critical personal data and services that are dependent on this data. Can be an indication of a ransomware attack. The deletion of these files can be used as a leverage tactic as attackers may threaten to delete or delete files until the ransom is paid. Also deleting these files extends the damage of the attack even when the attack stops as the data is still lost. This could also happen because of the attackers' attempt to cover their tracks which then even if the systems are restored the organisation is still facing difficulty due to the lost files. There are also legal and regulatory requirements surrounding the impact of the loss of personal data which can put regulatory pressure on the affected organisation.

1. **Unusual amount of data uploaded external websites**

Signals of unusual data activity:

* Off-hour activity: When a given user’s endpoint file activity takes place at unusual times.
* Untrusted domains: When files are emailed or uploaded to domains and URLs that are not considered trusted, as established by the company.
* Suspicious file mismatch: When the MIME/Media type of a high-value file, such as a spreadsheet, is disguised with the extension of a low-value file type, such as a JPEG — typically indicative of attempts to conceal data exfiltration.
* Remote activity: Activity taking place off-network may indicate increased risk.
* User attributes: Attributes like name, title, department, manager, and employment type (full-time, part-time, contractor) from a company’s identity management system.
* File categories: Categories, as determined by analysing file contents and extensions, that help signify a file’s sensitivity and value.
* Employee departure: Employees who are leaving the organisation — voluntarily or otherwise.
* Employee risk factors: Risk factors such as contract employees, high-impact employees, flight risk, performance concerns, and elevated access privileges.
* ZIP / compressed file movement: File activity involving .zip files since they may indicate an employee is attempting to take many files or hide files using encrypted zip folders.
* Shadow IT apps: Unusual data activity happening on web browsers, Slack, Airdrop, FileZilla, FTP, cURL, as well as commonly unauthorised [Shadow IT](https://www.code42.com/glossary/shadow-it/) apps like WeChat, WhatsApp, Zoom, and Amazon Chime.
* Public cloud sharing links: When files are shared with untrusted domains or made publicly available incorporate Google Drive, OneDrive, and Box systems.

1. **Abnormal DNS reverse lookup requests**

Traditionally, DNS lookup requests are done in a forward manner, whereby the domain name is translated into an IP address. Reverse DNS lookup requests do the opposite, using an IP address and mapping it to a domain name, allowing the user to identify the host name belonging to an IP address. The reason this is done can be for verification (confirms the identity of the server or client connecting to the network) troubleshooting (when investigating problems or suspicious activity, administrators can use reverse DNS to identify the source of the incoming traffic) and security (helping to detect and prevent malicious activities i.e. spamming, phishing or unauthorised access by verifying the reverse DNS of incoming connections to filter out potentially harmful traffic.)

**Common causes of reverse DNS lookup errors can involve the following:**

* Misconfigured DNS records: Incorrect PTR records: One of the most common causes. This is where the PTR record (the thing that records map IP addresses to domain names) is misconfigured or points to an incorrect domain, causing the reverse DNS lookup to fail.
* Mismatched forward/reverse DNS: In some cases, forward DNS and reverse DNS won’t match up. When verifying the authenticity of a connection, this can cause an error.
* Missing or Incomplete PTR records: Lack of PTR records: Every IP address should have a PTR record corresponding with it. If it doesn’t have one, it’ll fail.
* Incomplete PTR records: If only a subset of IPs have PTR records within a network range, the reverse DNS lookup will also fail.
* Outdated DNS Information: Stale Cache or Zone Files: If they’re outdated, they can cause errors when performing lookups. Regular updates and maintenance are needed to prevent these errors.

Network Connectivity Issues: Issues with network connectivity due to problems with the routing. Firewalls can block DNS requests which creates issues with network connectivity

ISP or DNS Provider Problems:

* DNS server outages: Problems with the DNS infrastructure of Internet Service Providers (ISPs) or DNS providers, such as server downtime or maintenance, can cause reverse DNS errors.
* DNS misconfigurations: Errors in the configuration of ISP or DNS provider DNS servers can also lead to reverse DNS lookup failures. These misconfigurations may include incorrect zone configurations or DNS server settings.

IP address ownership changes:

* Updated PTR Records: When the ownership of an IP address changes, such as during network reconfigurations or IP address reassignments, corresponding PTR records may not be updated accordingly. This discrepancy can cause reverse DNS errors when performing lookups for the affected IP addresses.
* Misconfigured DNS Settings: Incorrect DNS settings on network devices, such as routers, switches, or servers, can lead to reverse DNS errors. These misconfigurations may result in DNS queries being directed to incorrect DNS servers or failing to resolve DNS queries properly.