Basic Cyber Attacks and Log Analysis

Instructor

Panuwat Phunsuk (Hugo)

Senior SOC Engineer

INET Managed Services Co. Ltd.

What is Log

Log file: In the context of computers and software, a "log" can also refer to a log file. A log file is a record of events, actions, or messages generated by a computer program, system, or device. These logs are often used for troubleshooting, debugging, monitoring, and auditing purposes. They can contain information about errors, warnings, and other events that occur during the operation of software or hardware.

```
Oct  5 15:30:45 Workstation01 WinSecurityLog: Successful logon by user JohnDoe from 192.168.1.100
Oct  5 16:45:20 Workstation02 WinSecurityLog: Failed logon attempt for user Admin from 192.168.2.10
Oct  6 09:20:15 DC1 WinSecurityLog: New user account created - User JaneSmith (Domain: MYDOMAIN) created by Administrator
```

```
May  5 11:15:06 localhost sshd: Failed password for root from 123.213.55.47 port 53151 ssh2
May  5 11:15:07 localhost sshd: Success password for root from 123.213.55.47 port 53156 ssh2
```

```
Date: 2023-10-01 08:45:20 | Log Type: Traffic | Action: Allow | Source IP: 192.168.1.10 | Source Port: 54321 | Destination IP: 203.0.113.5 | Destination Port: 80
Date: 2023-10-01 09:30:15 | Log Type: Traffic | Action: Deny | Source IP: 10.0.0.50 | Source Port: 56789 | Destination IP: 192.168.1.100 | Destination Port: 22 | Policy ID: 1234
Date: 2023-10-01 10:15:30 | Log Type: IPS | Action: Alert | Source IP: 172.16.0.5 | Signature: WEB-ATTACKS SQL injection attempt
Date: 2023-10-01 11:20:45 | Log Type: Web Filter | Action: Block | Source IP: 192.168.2.10 | URL: http://malicious-site.com
Date: 2023-10-01 12:10:55 | Log Type: App Control | Action: Allow | Source IP: 192.168.3.20 | Application: Skype
Date: 2023-10-01 13:05:10 | Log Type: Anti-Virus | Action: Block | Source IP: 192.168.4.10 | Virus Name: Trojan.Generic
```

Convert log to table format for easier analysis. (Network Log)

Date: 2023-10-01 08:45:20 | Log Type: Traffic | Action: Allow | Source IP: 192.168.1.10 | Source Port: 54321 | Destination IP: 203.0.113.5 | Destination Port: 80
Date: 2023-10-01 09:30:15 | Log Type: Traffic | Action: Deny | Source IP: 10.0.0.50 | Source Port: 56789 | Destination IP: 192.168.1.100 | Destination Port: 22 | Policy ID: 1234
Date: 2023-10-01 09:30:20 | Log Type: Traffic | Action: Allow | Source IP: 192.168.1.1 | Source Port: 54444 | Destination IP: 203.0.19.9 | Destination Port: 443
Date: 2023-10-01 09:30:25 | Log Type: Traffic | Action: Deny | Source IP: 12.3.65.22 | Source Port: 43562 | Destination IP: 65.34.5.6 | Destination Port: 22 | Policy ID: 1234
Date: 2023-10-01 10:15:30 | Log Type: IPS | Action: Alert | Source IP: 172.16.0.5 | Signature: WEB-ATTACKS SQL injection attempt
Date: 2023-10-01 11:20:45 | Log Type: Web Filter | Action: Block | Source IP: 192.168.2.10 | URL: http://malicious-site.com
Date: 2023-10-01 12:10:55 | Log Type: App Control | Action: Allow | Source IP: 192.168.3.20 | Application: Skype
Date: 2023-10-01 13:05:10 | Log Type: Anti-Virus | Action: Block | Source IP: 192.168.4.10 | Virus Name: Trojan.Generic

Time	Message	Remark	Source IP	Source Port	Destination IP	Destination Port	Action
2023-10-01 08:45:20	Traffic	-	192.168.1.10	54321	203.0.113.5	80	Allow
2023-10-01 09:30:15	Traffic	-	10.0.0.50	56789	192.168.1.100	22	Deny
2023-10-01 09:30:20	Traffic	-	192.168.1.1	54444	203.0.19.9	443	Allow
2023-10-01 09:30:25	Traffic	-	12.3.65.22	43562	65.34.5.6	22	Deny
2023-10-01 10:15:30	WEB-ATTACKS	SQL injection attempt	172.16.0.5	-	-	-	Alert
2023-10-01 11:20:45	Web Filter	Malicious URL	192.168.2.10	-	-	-	Block
2023-10-01 12:10:55	App Control	Skype	192.168.3.20	-	-	-	Allow
2023-10-01 13:05:10	Anti-Virus	Trojan.Generic	192.168.4.10	-	-	-	Block

Convert log to table format for easier analysis. (Network Log)

<190>May 4 11:48:00 Gateway device="AFC" date=2023-05-06 time=11:48:00 timezone="+07" device_name="AFCX86" device_id=C0100164TJXPW21 log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information duration=0 fw_rule_id=30 policy_type=3 user_name="" user_gp="" iap=0 ips_policy_id=8 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="PortB" out_interface="PortG.1731" src_mac=00:00:00:00:00:00 src_ip=64.62.197.92 src_country_code=USA dst_ip=210.33.44.51 dst_country_code=THA protocol="TCP" src_port=19246 dst_port=21 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip=172.1.11.111 tran_dst_port=0 srczonetype="WAN" srczone="WAN" dstzonetype="WAN" dstzone="WAN" dir_disp="" connevent="Start" connid="988956824" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature" app_is_cloud=0

<190>May 4 11:48:10 Gateway device="AFC" date=2023-05-06 time=11:48:02 timezone="+07" device_name="AFCX86" device_id=C0100164TJXPW21 log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Block" priority=Information duration=0 fw_rule_id=30 policy_type=3 user_name="" user_gp="" iap=0 ips_policy_id=8 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="PortB" out_interface="PortG.1731" src_mac=00:00:00:00:00:00 src_ip=11.42.27.65 src_country_code=USA dst_ip=210.33.44.51 dst_country_code=THA protocol="TCP" src_port=35621 dst_port=80 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip=172.1.11.111 tran_dst_port=0 srczonetype="WAN" srczone="WAN" dstzonetype="WAN" dstzone="WAN" dir_disp="" connevent="Start" connid="988956824" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature" app_is_cloud=0

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
4/5/2023 11:48:00	Traffic	64.62.197.92	210.33.44.51	19246	21	Allow
4/5/2023 11:48:10	Traffic	11.42.27.65	210.33.44.51	35621	80	Block

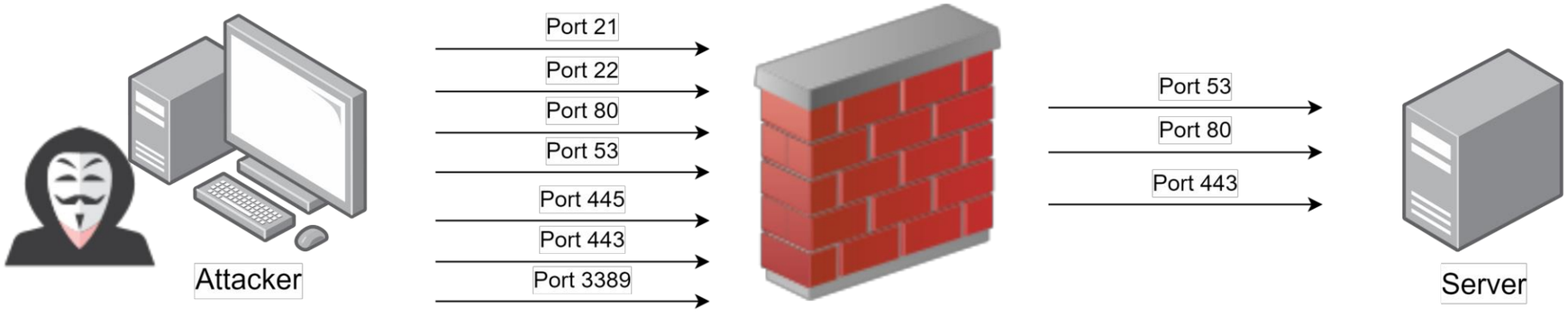
Convert log to table format for easier analysis. (System Log)

```
Oct  5 15:30:45 Workstation01 WinSecurityLog: Successful logon by user JohnDoe from 192.168.1.100
Oct  5 16:45:20 Workstation02 WinSecurityLog: Failed logon attempt for user Admin from 192.168.2.10
Oct  6 09:20:15 DC1 WinSecurityLog: New user account created - User JaneSmith (Domain: MYDOMAIN) created by Administrator
Oct  8 14:30:55 Server01 WinSecurityLog: Password reset for user JohnDoe (Domain: MYDOMAIN) by Administrator
Oct 15 09:55:20 Server01 WinSecurityLog: New security group created - GroupName "Sales Team" (Domain: MYDOMAIN) by Administrator
Oct 20 14:15:30 Server01 WinSecurityLog: Security group deleted - GroupName "Marketing Team" (Domain: MYDOMAIN) by Administrator
Oct 25 10:20:45 Server01 WinSecurityLog: User added to group - User JaneSmith (Domain: MYDOMAIN) added to group "Sales Team“ by Administrator
Oct 25 16:45:20 Workstation03 WinSecurityLog: Failed logon attempt for user James from 192.168.2.15
Oct 25 16:46:45 Workstation03 WinSecurityLog: Successful logon by user James from 192.168.1.100
```

Time	Message	Source IP	Source User	Destination User	Destination Group	Host Name	Action
2023/10/5 15:30:45	Successful logon	192.168.1.100	JohnDoe	-		Workstation01	Success
2023/10/5 16:45:20	Failed logon	192.168.2.10	Admin	-		Workstation02	Fail
2023/10/6 09:20:15	New user account created	-	JaneSmith	-		DC1	Success
2023/10/8 14:30:55	Password reset for user	-	JohnDoe	-		Server01	Success
2023/10/15 09:55:20	New security group created	-	Administrator	-	Sales Team	Server01	Success
2023/10/20 14:15:30	Security group deleted	-	Administrator	-	Marketing Team	Server01	Success
2023/10/25 10:20:45	User added to group	-	Administrator	JaneSmith	Sales Team	Server01	Success
2023/10/25 16:45:20	Failed logon	192.168.2.15	James	-		Workstation03	Fail
2023/10/25 16:46:45	Successful logon	192.168.1.100	James	-		Workstation03	Success

Network Attacks

Port Scanning



Description	A port scan is a common reconnaissance technique used by attackers to discover open ports on a target system or network. In a port scan, the attacker systematically sends connection requests to a range of network ports (or all ports) on a target system to determine which ports are open and listening for incoming connections. The information gathered from a port scan can be used to identify potential vulnerabilities and weaknesses in the target, helping the attacker plan further attacks.
Impact	Attackers can identify open ports and services, potentially discovering vulnerabilities that can be exploited in subsequent attacks.
Recommendations	- Add the source IP address to your firewall to block all traffic from that source. - Implement strong firewall rules to block or limit access to unnecessary ports and services. Only allow traffic to essential ports and services required for your organization's operations. - Deploy IDS/IPS solutions to detect and block suspicious port scanning activity in real-time.

Port Scanning Detection (Traffic Log)

At least 20 traffic event which following condition:

- Source IP are the same
- Destination IP are the same
- Destination port are different
- Occurs in 5 seconds

Can be detected from IDS/IPS, UTM

Severity: Low

vertical
high
medium
Low

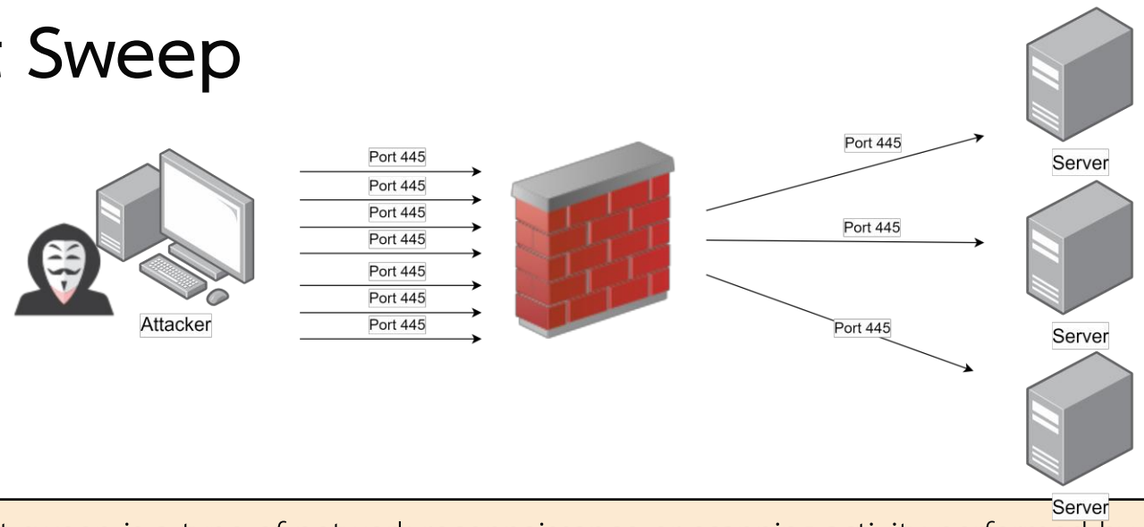
Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
4/5/2023 11:48:01	Traffic	64.62.197.92	210.33.44.51	19246	21	Allow
4/5/2023 11:48:01	Traffic	64.62.197.92	210.33.44.51	35621	443	Block
4/5/2023 11:48:01	Traffic	64.62.197.92	210.33.44.51	35677	80	Allow
4/5/2023 11:48:01	Traffic	64.62.197.92	210.33.44.51	35672	53	Block
4/5/2023 11:48:01	Traffic	64.62.197.92	210.33.44.51	35677	445	Block
4/5/2023 11:48:02	Traffic	64.62.197.92	210.33.44.51	35671	25	Allow
...	...	...	...	...	...	...

Port Scanning Detection (IDS/IPS, UTM log)

2023-10-04 15:30:45 - IPS Alert - Source: 192.168.1.100, Dest: 203.0.113.1, Protocol: TCP, Src Port: 52345, 52384 Dest Ports: 22, 80, 443, 8080, Description: Port Scan Detected, Severity: High, Action: Blocked (10m)
2023-10-04 15:35:45 - IPS Alert - Source: 64.62.197.92, Dest: 210.33.44.51, Protocol: TCP, Src Port: 52345, 35232 Dest Ports: 25, 22, 80, 808, Description: Port Scan Detected, Severity: High, Action: Blocked (10m)
2023-10-04 15:40:45 - IPS Alert - Source: 92.18.1.10, Dest: 203.5.13.1, Protocol: TCP, Src Port: 52345, 64325, 32562 Dest Ports: 21, 80, 43, 700, Description: Port Scan Detected, Severity: High, Action: Blocked (10m)
2023-10-04 15:43:45 - IPS Alert - Source: 12.68.78.10, Dest: 210.30.4.51, Protocol: TCP, Src Port: 52345, 44623, 45726 Dest Ports: 24, 20, 53, 3389, Description: Port Scan Detected, Severity: High, Action: Alert

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
2023-10-04 15:30:45	Port Scan Detected	192.168.1.100	203.0.113.1	52345, 52384	22, 80, 443, 8080	Block
2023-10-04 15:35:45	Port Scan Detected	64.62.197.92	210.33.44.51	52345, 35232	25, 22, 80, 808	Block
2023-10-04 15:40:45	Port Scan Detected	92.18.1.10	203.5.13.1	52345, 64325, 32562	21, 80, 43, 700	Block
2023-10-04 15:43:45	Port Scan Detected	12.68.78.10	210.30.4.51	52345, 44623, 45726	24, 20, 53, 3389	Alert

Port Sweep



Description	A port sweep is a type of network reconnaissance or scanning activity performed by an attacker to identify which network ports on a target system or range of systems are open and listening for incoming connections. Unlike a full port scan, which checks all possible ports on a target, a port sweep typically focuses on a specific range or subset of ports. Attackers use port sweeps to gather information about potential entry points and vulnerabilities on target systems.
Impact	Attackers can identify open ports and services, potentially discovering vulnerabilities that can be exploited in subsequent attacks.
Recommendations	- Add the source IP address to your firewall to block all traffic from that source. - Implement strong firewall rules to block or limit access to unnecessary ports and services. Only allow traffic to essential ports and services required for your organization's operations. - Deploy IDS/IPS solutions to detect and block suspicious port sweep activity in real-time.

Port Sweep Detection (Traffic Log)

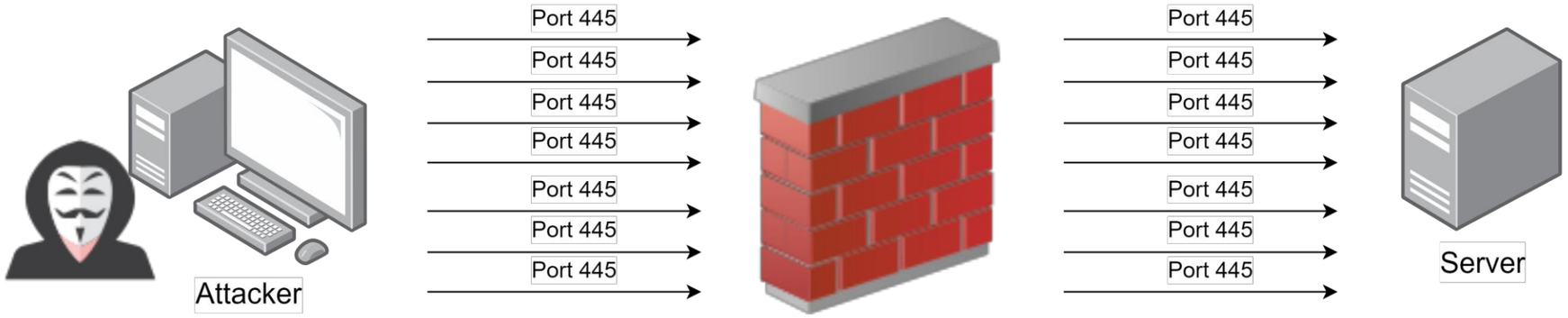
At least 5 traffic event which following condition:
- Source IP are the same
- Destination IP are different
- Destination port are the same
- Occurs in 2 seconds

Can be detected from IDS/IPS, UTM

Severity: Low

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
5/5/2023 23:48:23	Traffic	64.62.197.92	210.33.44.51	26296	445	Allow
5/5/2023 23:48:23	Traffic	64.62.197.92	210.33.44.63	26300	445	Block
5/5/2023 23:48:23	Traffic	64.62.197.92	210.33.44.32	26311	445	Block
5/5/2023 23:48:23	Traffic	64.62.197.92	210.33.44.89	26315	445	Allow
5/5/2023 23:48:23	Traffic	64.62.197.92	210.33.44.11	26321	445	Block
5/5/2023 23:48:24	Traffic	64.62.197.92	210.33.44.56	26327	445	Allow

Denial of Service Attack (DOS) - TCP SYN Flood



Description	A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a network, system, or service by overwhelming it with a flood of traffic, requests, or other disruptive activities. The goal of a DoS attack is to render the targeted resource unavailable to its intended users, thereby denying access or service. There are several variations and techniques associated with DoS attacks, including Distributed Denial of Service (DDoS) attacks, which involve multiple compromised systems working in concert to carry out the attack.
Impact	- The targeted service or system becomes unavailable, causing downtime and preventing legitimate users from accessing it. - A DoS attack can consume network bandwidth, server resources, and computing power, affecting overall network performance.
Recommendations	- Deploy traffic filtering and rate-limiting solutions to identify and block malicious traffic patterns. - Set up rate limits to restrict the number of requests a single IP address can make within a specific timeframe.

Denial of Service Attack (DOS) – TCP SYN Flood Detection (Traffic Log)

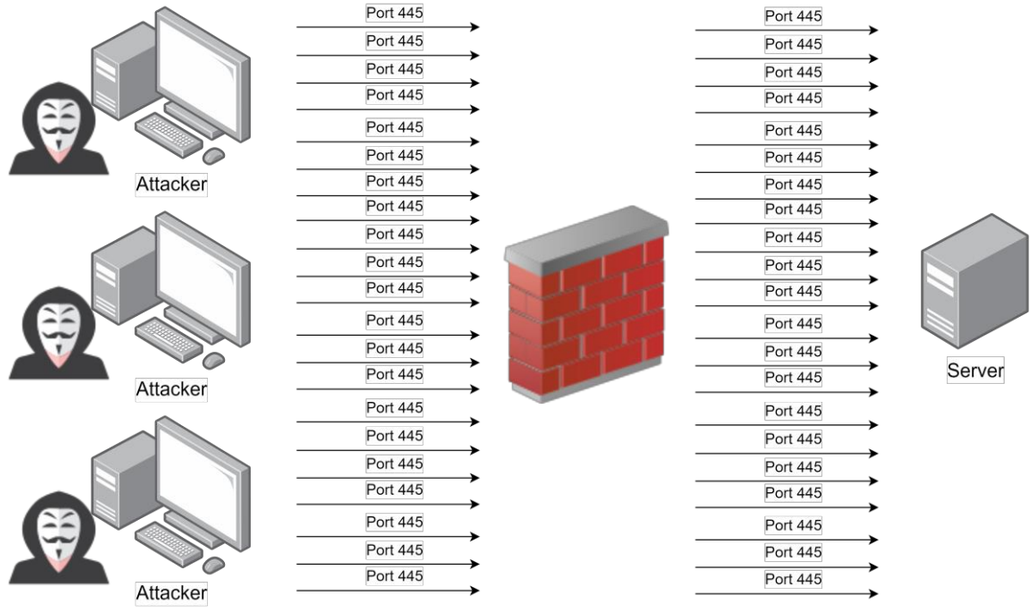
At least 100 traffic event which following condition:
- Source IP are the same
- Destination IP are the same
- Destination port are the same
- Source port are different
- Occurs in 5 seconds

Can be detected from IDS/IPS, UTM

Severity: High

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17898	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17901	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17902	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17905	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17908	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17910	443	Allow
...	...	...	...	...	...	...

Distributed Denial of Service Attack (DDOS) – TCP SYN Flood



Description	A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a network, service, or website by overwhelming it with a massive volume of traffic generated from multiple sources. Unlike a traditional DoS attack, which relies on a single source to flood a target, a DDoS attack leverages a network of compromised computers or devices (often called a botnet) to orchestrate the attack. These coordinated efforts make DDoS attacks more challenging to mitigate.
Impact	- The targeted service or system becomes unavailable, causing downtime and preventing legitimate users from accessing it. - A DDoS attack can consume network bandwidth, server resources, and computing power, affecting overall network performance.
Recommendations	- Deploy traffic filtering and rate-limiting solutions to identify and block malicious traffic patterns. - Set up rate limits to restrict the number of requests a single IP address can make within a specific timeframe.

Distributed Denial of Service Attack (DDOS) – TCP SYN Flood Detection (Traffic Log)

At least 200 traffic event which following condition:

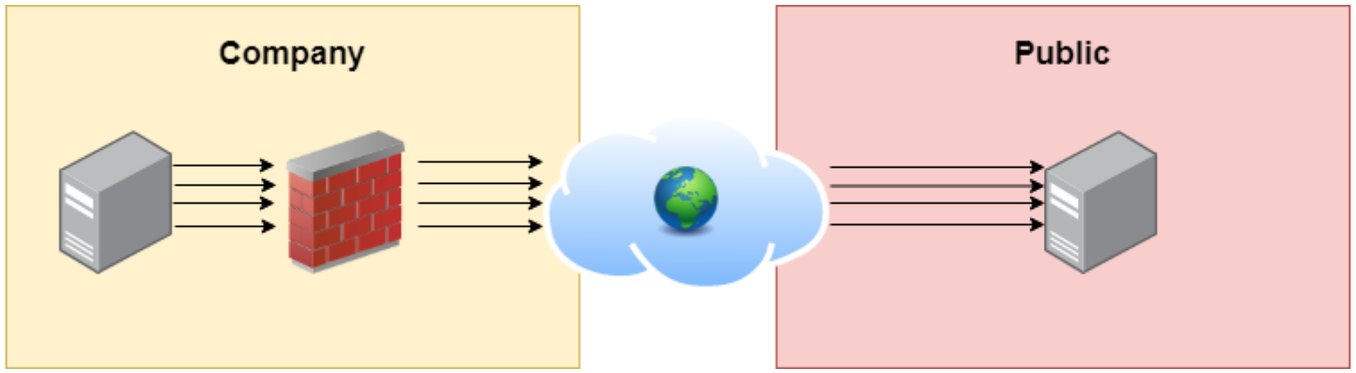
- At least 2 source IP are different
- Destination IP are the same
- Destination port are the same
- At least 100 source port are different
- Occurs in 5 seconds

Can be detected from IDS/IPS, UTM

Severity: Critical

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17898	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17901	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17902	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17905	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17908	443	Allow
6/5/2023 23:48:00	Traffic	213.34.163.254	210.33.44.51	17910	443	Allow
...	...	...	...	...	...	...

Outbound Flood Traffic



Description	Outbound flood traffic is a cybersecurity threat scenario where a large volume of network traffic originating from within an organization's network overwhelms the network infrastructure or external resources, such as a website or server. This type of traffic flood is typically unintentional and can result from various factors, including malware infections, misconfigurations, or legitimate but unexpectedly high traffic loads.
Impact	- The excessive outbound traffic can congest the organization's network, leading to reduced network performance and potential service disruptions. - Outbound flood traffic directed at external resources, such as a website or server, can cause service interruptions or downtime, affecting the availability of online services.
Recommendations	- Deploy traffic filtering and rate-limiting solutions to identify and block malicious traffic patterns. - Set up rate limits to restrict the number of requests a single IP address can make within a specific timeframe. - Deploy and regularly update endpoint security solutions (antivirus, anti-malware, etc.) to detect and prevent infections on devices within your network. - Ensure that all systems and software are up to date with the latest security patches to minimize vulnerabilities.

Outbound Flood Traffic Detection (Traffic Log)

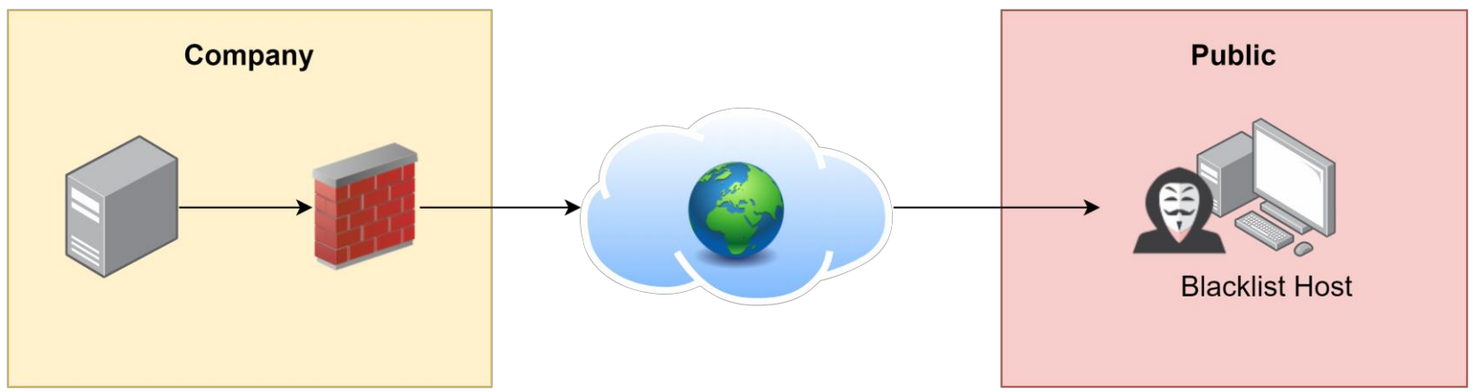
At least 100 traffic event which following condition:
- Source IP are the same
- Source IP are private IP or IP of organization
- Destination IP are the same
- Destination port are the same
- Occurs in 5 seconds

Can be detected from IDS/IPS, UTM

Severity: High

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
6/5/2023 23:48:00	Traffic	192.168.45.37	42.71.46.88	17898	443	Allow
6/5/2023 23:48:00	Traffic	192.168.45.37	42.71.46.88	17901	443	Block
6/5/2023 23:48:00	Traffic	192.168.45.37	42.71.46.88	17902	443	Allow
6/5/2023 23:48:00	Traffic	192.168.45.37	42.71.46.88	17905	443	Block
6/5/2023 23:48:00	Traffic	192.168.45.37	42.71.46.88	17908	443	Allow
6/5/2023 23:48:00	Traffic	192.168.45.37	42.71.46.88	17910	443	Allow
...	...	...	...	...	...	...

Outbound Communication to Blacklist IP Address



Description	Outbound communication to a blacklist IP address occurs when a device or system within your network initiates connections or sends data to an IP address that has been identified as malicious, untrustworthy, or part of a known blacklist. This threat scenario can indicate that a device within your network has been compromised or that a legitimate application is inadvertently communicating with a malicious IP address.
Impact	The target is high risk of being cyber-attacked.
Recommendations	- Deploy and regularly update endpoint security solutions (antivirus, anti-malware, etc.) to detect and prevent infections on devices within your network. - Configure firewalls to restrict outbound traffic to only necessary and trusted destinations. Implement egress filtering rules to block connections to known blacklist IP addresses. - Deploy and regularly update endpoint security solutions (antivirus, anti-malware, etc.) to detect and prevent infections on devices within your network. - Ensure that all systems and software are up to date with the latest security patches to minimize vulnerabilities.

Outbound Communication to Blacklist IP Address Detection (Traffic Log)

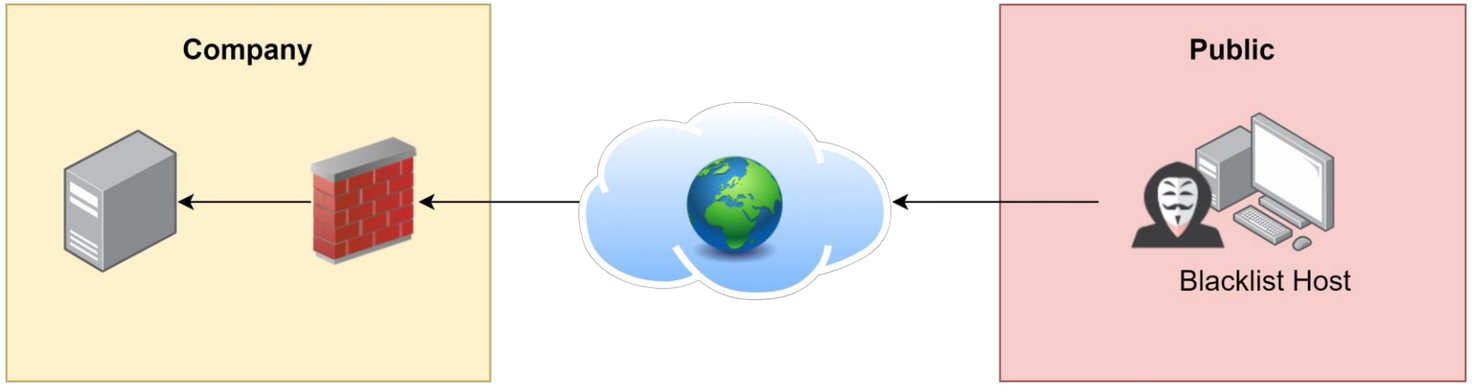
At least 1 traffic event which following condition:
- Destination IP is the suspicious or malicious
- Source IP is private IP or IP of organization
- Occurs in 1 seconds

Can be detected from IDS/IPS, UTM

Severity: Critical

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
5/5/2023 06:47:21	Traffic	192.168.10.10	213.34.163.254	36602	50239	Allow
5/5/2023 23:50:01	Traffic	192.168.10.10	213.34.163.254	36604	50239	Allow
5/5/2023 23:54:02	Traffic	192.168.10.10	213.34.163.254	36608	50239	Allow
5/5/2023 23:59:04	Traffic	192.168.10.10	213.34.163.254	36612	50239	Allow
6/5/2023 00:15:06	Traffic	192.168.10.10	213.34.163.254	36615	50239	Allow
6/5/2023 01:00:07	Traffic	192.168.10.10	213.34.163.254	36619	50239	Allow

Inbound Communication from Blacklist IP Address



Description	Inbound communication from a blacklist IP address refers to network traffic originating from an IP address that has been previously identified as malicious or untrustworthy. This threat occurs when a system or network receives data packets or requests from an IP address that has been blacklisted due to its association with cybercriminal activities, such as spamming, malware distribution, hacking attempts, or other malicious actions.
Impact	The target is high risk of being cyber-attacked.
Recommendations	- Setup robust firewall rules to block traffic from known blacklist IP addresses. Utilize threat intelligence feeds and regularly update firewall rules to stay current with emerging threats. - Implement IDS/IPS solutions to monitor and analyze incoming traffic for suspicious patterns or behavior, automatically blocking or alerting on traffic from blacklisted IPs.

Inbound Communication from Blacklist IP Address Detection (Traffic Log)

At least 1 traffic event which following condition:
- Destination IP is private IP or IP of organization
- Source IP is the suspicious or malicious
- Occurs in 1 seconds

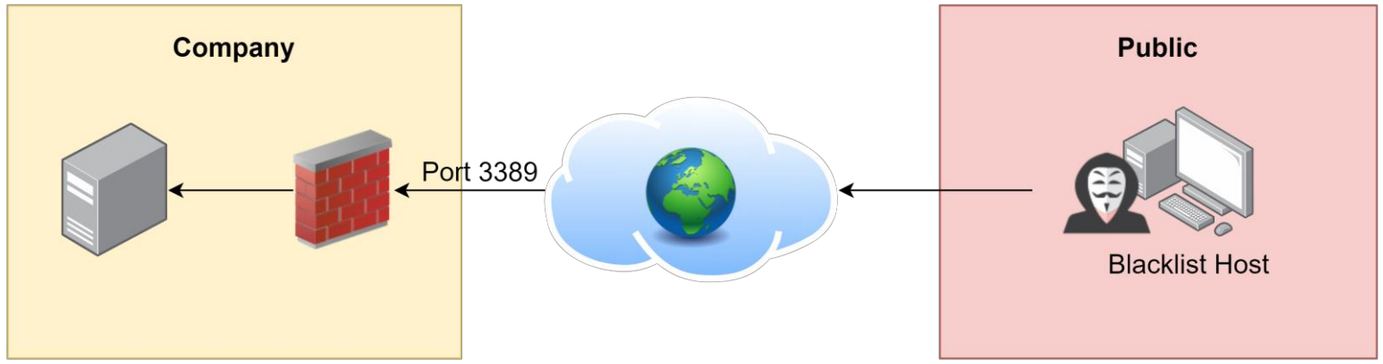
Can be detected from IDS/IPS, UTM

Severity: Medium

← the owner of blacklist may change to other

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
5/5/2023 23:48:00	Traffic	64.62.197.92	210.33.44.51	26296	445	Allow
5/5/2023 23:50:01	Traffic	64.62.197.92	210.33.44.51	26300	445	Allow
5/5/2023 23:54:02	Traffic	64.62.197.92	210.33.44.51	26311	445	Allow
5/5/2023 23:59:04	Traffic	64.62.197.92	210.33.44.51	26315	445	Block
6/5/2023 00:15:06	Traffic	64.62.197.92	210.33.44.51	26321	445	Allow
6/5/2023 01:00:07	Traffic	64.62.197.92	210.33.44.51	26327	445	Allow

RDP Access from Blacklist IP



Description	RDP (Remote Desktop Protocol) access from a suspicious IP address refers to a cybersecurity threat scenario where an attempt is made to establish a remote desktop connection to a system or server from an IP address that is considered suspicious or untrusted. Remote desktop services are commonly targeted by attackers attempting to gain unauthorized access to systems for malicious purposes.
Impact	- The target is high risk of being cyber-attacked. - If the RDP connection is successful, the attacker gains unauthorized access to the targeted system, potentially compromising sensitive data and resources.
Recommendations	- Configure firewall rules and ACLs to restrict RDP access to known, trusted IP addresses or authorized remote networks. - Enforce Network-Level Authentication (NLA) for RDP sessions to require users to authenticate before establishing a remote desktop connection. - Setup robust firewall rules to block traffic from known blacklist IP addresses. Utilize threat intelligence feeds and regularly update firewall rules to stay current with emerging threats. - Implement IDS/IPS solutions to monitor and analyze incoming traffic for suspicious patterns or behavior, automatically blocking or alerting on traffic from blacklisted IPs. - Use a strong password. (Minimum 8 characters long, including uppercase/lowercase letters, numbers, and special characters)

RDP Access from Blacklist IP (Traffic Log)

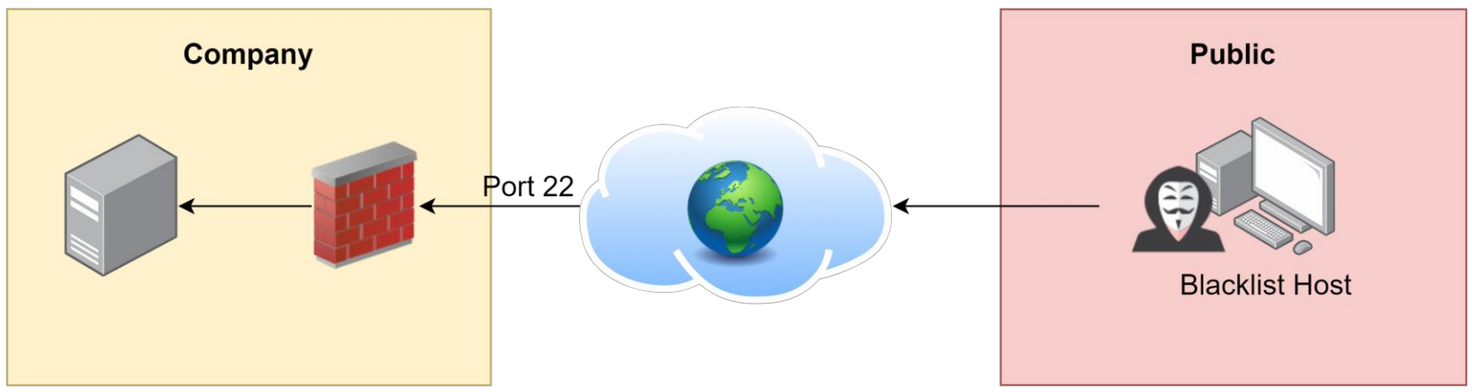
At least 1 traffic event which following condition:
- Destination IP is private IP or IP of organization
- Source IP is the suspicious or malicious
- Destination port is 3389
- Occurs in 1 seconds

Can be detected from IDS/IPS, UTM

Severity: Medium

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
5/5/2023 23:48:00	Traffic	64.62.197.92	210.33.44.51	26296	3389	Allow
5/5/2023 23:50:01	Traffic	64.62.197.92	210.33.44.51	26300	3389	Allow
5/5/2023 23:54:02	Traffic	64.62.197.92	210.33.44.51	26311	3389	Allow
5/5/2023 23:59:04	Traffic	64.62.197.92	210.33.44.51	26315	3389	Block
6/5/2023 00:15:06	Traffic	64.62.197.92	210.33.44.51	26321	3389	Allow
6/5/2023 01:00:07	Traffic	64.62.197.92	210.33.44.51	26327	3389	Allow

SSH Access from Blacklist IP



Description	SSH (Secure Shell) access from a suspicious IP address refers to a cybersecurity threat scenario where an attempt is made to establish an SSH connection to a system or server from an IP address that is considered suspicious or untrusted. SSH is a widely used protocol for secure remote administration, and unauthorized access attempts can pose a significant security risk.
Impact	- The target is high risk of being cyber-attacked. - If the SSH connection is successful, the attacker gains unauthorized access to the targeted system, potentially compromising sensitive data and resources.
Recommendations	- Configure firewall rules and ACLs to restrict SSH access to known, trusted IP addresses or authorized remote networks. - Setup robust firewall rules to block traffic from known blacklist IP addresses. Utilize threat intelligence feeds and regularly update firewall rules to stay current with emerging threats. - Implement IDS/IPS solutions to monitor and analyze incoming traffic for suspicious patterns or behavior, automatically blocking or alerting on traffic from blacklisted IPs. - Use a strong password. (Minimum 8 characters long, including uppercase/lowercase letters, numbers, and special characters)

SSH Access from Blacklist IP (Traffic Log)

At least 1 traffic event which following condition:
- Destination IP is private IP or IP of organization
- Source IP is the suspicious or malicious
- Destination port is 3389
- Occurs in 1 seconds

Can be detected from IDS/IPS, UTM

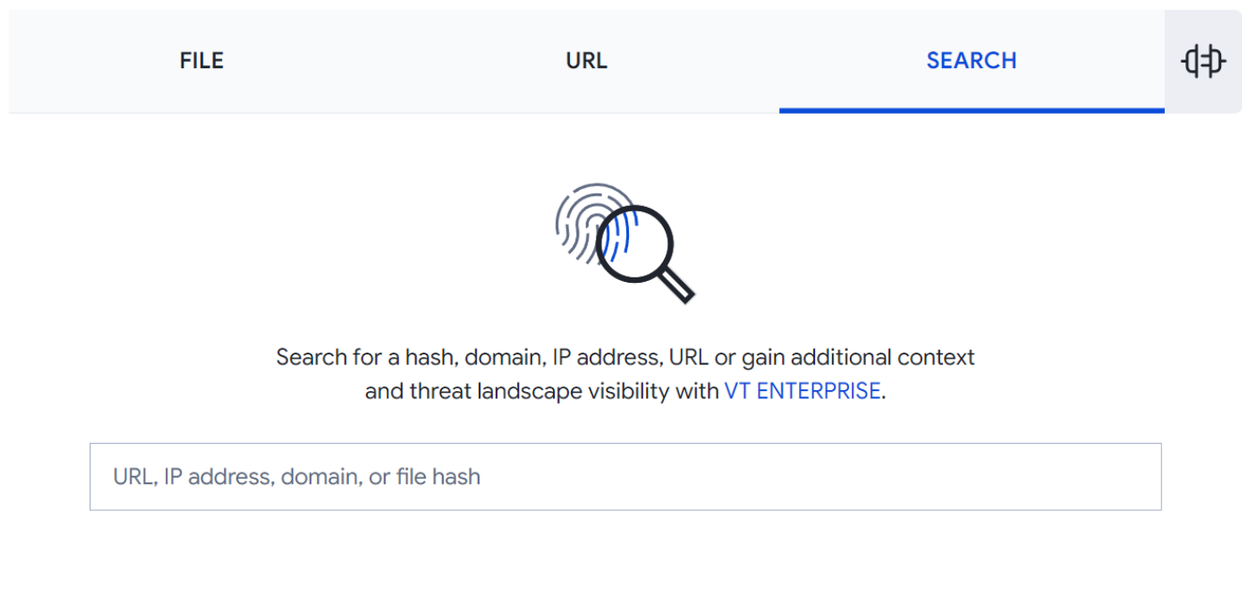
Severity: Medium

Time	Message	Source IP	Destination IP	Source Port	Destination Port	Action
5/5/2023 23:48:00	Traffic	64.62.197.92	210.33.44.51	26296	22	Allow
5/5/2023 23:50:01	Traffic	64.62.197.92	210.33.44.51	26300	22	Allow
5/5/2023 23:54:02	Traffic	64.62.197.92	210.33.44.51	26311	22	Allow
5/5/2023 23:59:04	Traffic	64.62.197.92	210.33.44.51	26315	22	Block
6/5/2023 00:15:06	Traffic	64.62.197.92	210.33.44.51	26321	22	Allow
6/5/2023 01:00:07	Traffic	64.62.197.92	210.33.44.51	26327	22	Allow

VIRUSTOTAL

VIRUSTOTAL

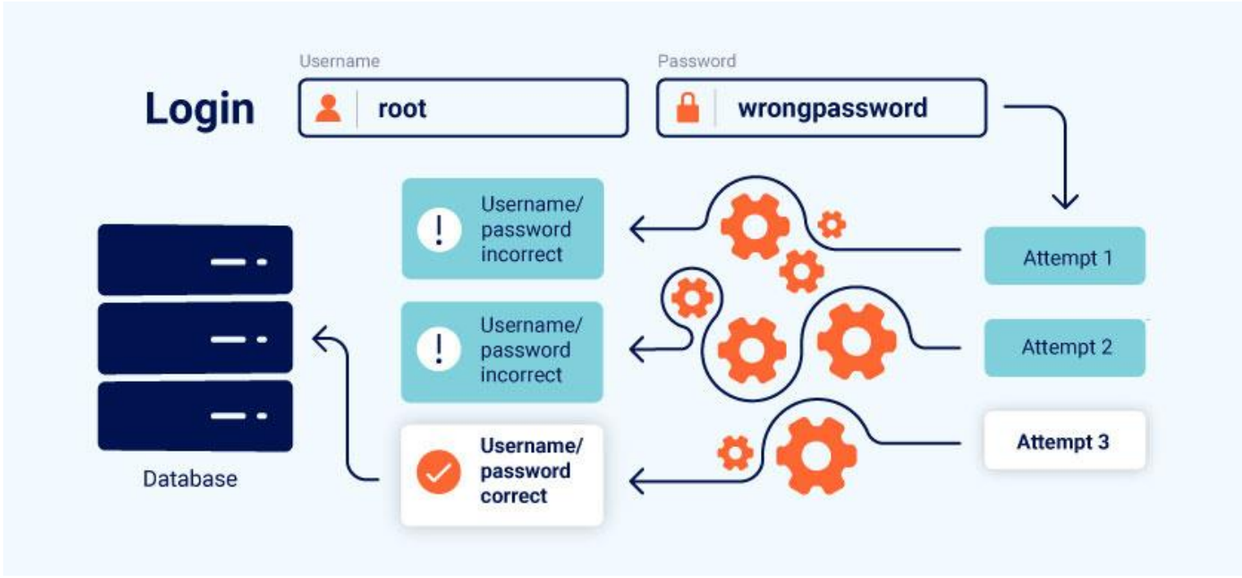
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.



https://www.virustotal.com/

System Attacks

Brute force Login Attack Success



Description	A brute force login attack success refers to a cybersecurity threat scenario where an attacker successfully gains unauthorized access to a system, application, or user account by systematically trying multiple username and password combinations until the correct one is discovered. Brute force attacks are typically automated and can exploit weak or easily guessable credentials.
Impact	If attackers gain unauthorized access to systems, applications, or user accounts, potentially compromising sensitive data and resources.
Recommendations	- Implement account lockout policies that temporarily lock or suspend user accounts after a specified number of failed login attempts. - Use a strong password. (Minimum 8 characters long, including uppercase/lowercase letters, numbers, and special characters). - Enforce strong authentication methods, such as multi-factor authentication (MFA), to add an extra layer of security and make it more difficult for attackers to guess login credentials.

Brute force Login Attack Success Detection (System Log)

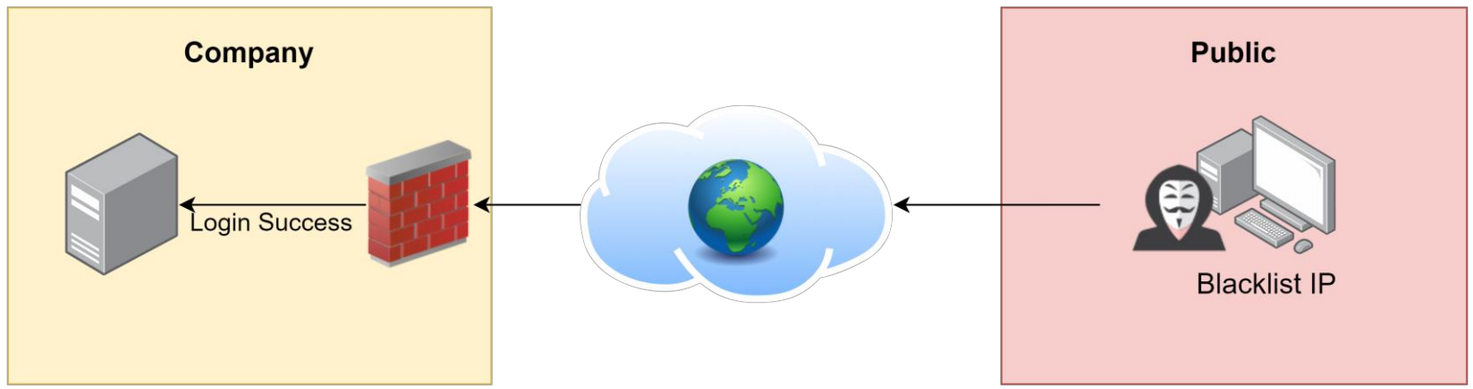
At least 10 login event which following condition:

- Destination IP are the same
- Source IP are the same
- Source user are the same
- Start with 9 login failed event follow by login success event
- Occurs in 10 seconds

Severity: Critical

Time	Message	Source IP	Destination IP	Source User	Source Port	Application	Action
5/5/2023 11:15:00	Login	123.213.55.47	20.57.63.77	root	53156	SSH	Failed
5/5/2023 11:15:01	Login	123.213.55.47	20.57.63.77	root	53153	SSH	Failed
5/5/2023 11:15:02	Login	123.213.55.47	20.57.63.77	root	53150	SSH	Failed
5/5/2023 11:15:04	Login	123.213.55.47	20.57.63.77	root	53154	SSH	Failed
5/5/2023 11:15:06	Login	123.213.55.47	20.57.63.77	root	53151	SSH	Failed
5/5/2023 11:15:07	Login	123.213.55.47	20.57.63.77	root	53156	SSH	Success

Successful Login from Blacklist IP



Description	A successful login from a suspicious host refers to a cybersecurity threat scenario where an unauthorized user or entity gains access to a system, application, or user account from an IP address or network location that is considered suspicious or untrusted. This type of threat may indicate a security breach, credential compromise, or malicious activity.
Impact	Attackers or malicious entities gain unauthorized access to systems, applications, or user accounts, potentially compromising sensitive data and resources.
Recommendations	- Add the source IP address to your firewall or intrusion detection system (IDS) to block all traffic from that source. - Segment your network to isolate critical systems from less critical ones, reducing the risk of lateral movement in the event of a successful login to a suspicious host. - Maintain whitelists of trusted IP addresses and blacklists of known malicious or suspicious IP addresses. Configure systems to allow access only from whitelisted sources. - Deploy and regularly update endpoint security solutions (antivirus, anti-malware, etc.) to detect and prevent infections on devices within your network. - Use a strong password. (Minimum 8 characters long, including uppercase/lowercase letters, numbers, and special characters) - Ensure that all systems and software are up to date with the latest security patches to minimize vulnerabilities.

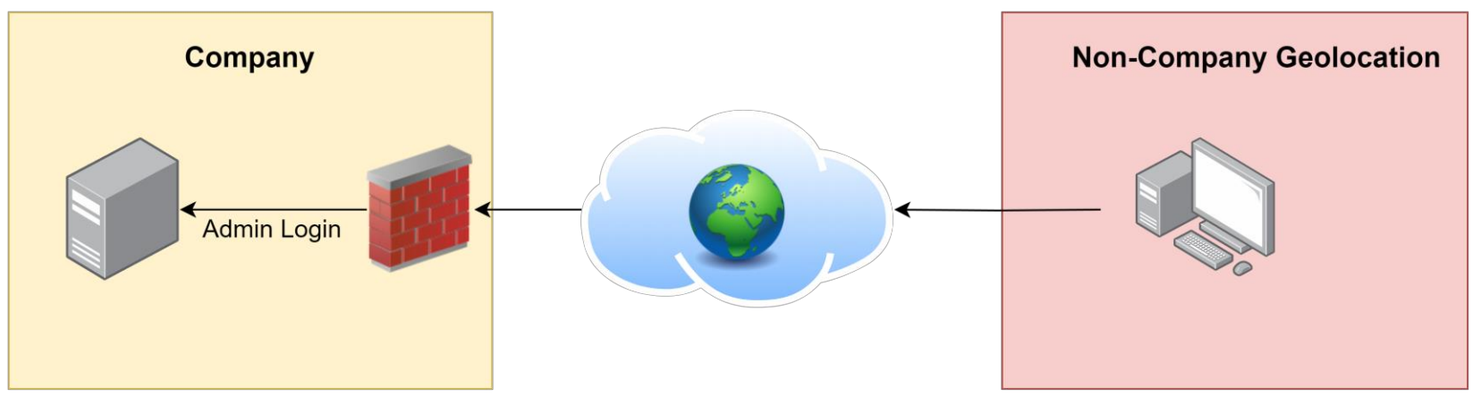
Successful Login from Blacklist IP Detection (System Log)

1 successful login event which following condition:
- Destination IP is private IP or IP of organization
- Source IP is the suspicious or malicious
- Occurs in 1 second

Severity: Critical

Time	Message	Source IP	Destination IP	Source User	Source Port	Application	Action
5/5/2023 11:15:00	Login	64.62.197.92	20.57.63.77	root	53156	SSH	Success
5/5/2023 11:15:01	Login	64.62.197.92	25.33.85.28	Administrator	53153	RDP	Success

Unauthorized Admin Logon from Non-Company Geolocation



Description	Unauthorized admin logon from a non-company geolocation refers to an incident where an individual or entity gains access to administrative accounts within your organization's network or systems from a physical location that is not authorized or recognized as part of your company's infrastructure. This threat typically involves unauthorized access to privileged accounts, such as administrator or root accounts, from a remote or foreign location.
Impact	- Unauthorized access to administrative accounts can lead to data breaches, resulting in the exposure of sensitive information, intellectual property, and customer data. - Attackers with admin privileges can compromise systems, install malware, or steal data, potentially causing widespread damage and disruption.
Recommendations	Implement geolocation-based access controls to restrict admin logons to recognized company locations or authorized geographic regions. This can be enforced through the use of VPNs or geolocation-based authentication mechanisms.

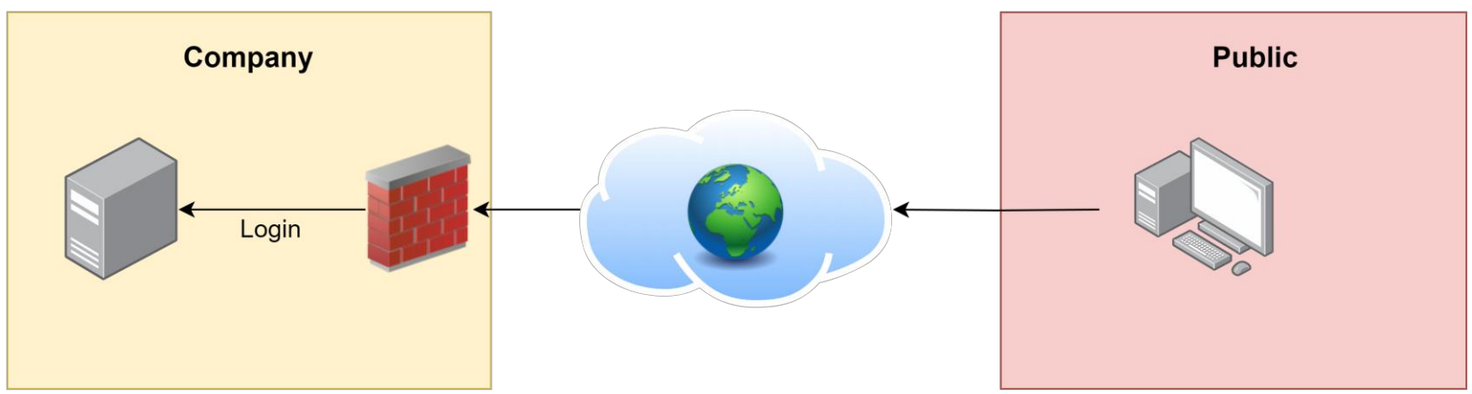
Unauthorized Admin Logon from Non-Company Geolocation Detection (System Log)

1 login event which following condition:
- Source IP is not come from company geolocation
- Source user is root or administrator
- Occurs in 1 second

Severity: Critical

Time	Message	Source IP	Destination IP	Source User	Source Port	Application	Action
5/5/2023 11:15:00	Login	64.62.197.92	20.57.63.77	root	53156	SSH	Fail
5/5/2023 11:15:01	Login	64.62.197.92	25.33.85.28	Administrator	53153	RDP	Success

Login Attempt from Locked or Disabled Account



Description	A login attempt from a locked or disabled account refers to an unauthorized effort to access a user account that has been intentionally locked or disabled by the organization's security policies. Such accounts are typically locked or disabled due to security concerns, such as multiple failed login attempts or a security incident. Attackers may attempt to gain access to these accounts to exploit vulnerabilities or steal sensitive information.
Impact	If attackers successfully log in to a locked or disabled account, they may gain unauthorized access to sensitive data, systems, or resources.
Recommendations	- Implement account lockout policies that automatically lock user accounts after a specified number of failed login attempts. Ensure that these policies are configured appropriately to balance security and usability. - Conduct regular audits of user accounts, reviewing access privileges and disabling or locking accounts that are no longer needed.

Malware Detected but Failed to Clean

Description	"Malware Detected but Failed to Clean" is a cybersecurity threat scenario where a security system or software has identified the presence of malicious software (malware) on a computer or network but is unable to successfully remove or quarantine the malware. Malware can include viruses, trojans, worms, ransomware, spyware, and other malicious code designed to compromise or damage systems.
Impact	- Malware can lead to data breaches or data loss by encrypting or stealing sensitive information. - Failure to remove malware means the system remains compromised, allowing attackers to maintain unauthorized access, launch further attacks, or use the system as part of a botnet.
Recommendations	- Implement network segmentation to limit the spread of malware within your network. - Ensure that you use reputable antivirus and anti-malware software with up-to-date definitions and regular scans. - Keep operating systems, software, and applications up to date with the latest security patches to reduce vulnerabilities that malware can exploit. - Deploy and regularly update endpoint security solutions (antivirus, anti-malware, etc.) to detect and prevent infections on devices within your network.

Question

&

Answer

INET Managed Services Co., Ltd.

Thank You

Innovation is our Business

INET Manged Services is a Leading Service Provider.