Executive Summary

In regards to the recent IT-related events, such as the recent degradation in service for a Federal Aviation Administration's system for tracking flights has got the GIAC senior executives attention. This technical paper serves as a process and procedures checklist for handling such incidents in the GIAC corporation. In the event that the GIAC network or servers become compromised or negatively affected, this process and procedures would ensure that the incident is adequately managed. This paper starts by analyzing the FAA incident and their lack of service availability that was the cause of hundreds of flight delays throughout the East Coast of the United States. This event followed a group of incidents involving United Airlines, The New York Stock Exchange, and the Wall Street Journal. These events demonstrate how large-scale information systems are subject to a wide variety of threats, both intentional and unintentional. The paper proposes incident response process and checklists to help the incident response leader determine if the cause of the glitch is human error or malicious intent. For the checklist, examples are provided on what we would expect to find if it was user error or malicious intent.

Public Relations Plan using FAA Case Study

During security-related incidents, keeping stakeholders informed is vital. Often, bad news or perceived bad news about the security-related event can create an existential threat to the organization. People make crucial decisions such as with whom to trust their money, their personal information, or even their lives based on news and publicity. Public relations and expectations about an event must be managed properly. In the FAA case study, there was a significant lack of information from the agency on what was being done to remediate the problems and current challenges and a timeline for making the system (En Route Automation Modernization, or ERAM) 100% operational. There appeared to be too much emphasis on the benefits of the new program that was introduced after long delays. While the public might be interested in the long-term advantages of the ERAM system, airline passengers have more immediate concerns about being able to fly sooner than later. The release of event information must be tightly controlled. Start all communications through a single person to prevent confusion. Ideally, crisis communications or news about an incident should be only released by Public Affairs personnel or senior executives after senior executives have reviewed it. In a presentation done by Scott Roberts titled “Crisis Comms for Incident Response”, the following approach was recommended regarding the communication and statements made to executives and the public population:

- It should be clear. The information should be presented preferably on a 5th-grade reading level. Remember a lot of your audience may not have a technical background. If people do not understand, the victims will be confused, and the skeptics will not trust the organization. Executives or public affairs personnel should stay consistent across messages and media.
- Information should be timely. It is best to over-communicate and reasonable prepare people for
- Information about incidents should be actionable by stakeholders. Sample questions to be answered should be: What is the organization during to mitigate and remediate the problem? How can people know if they are being affected? What can they do if they are affected? - The organizational leadership should indicate responsibility. Admitting what went wrong and said that you are sorry indicates that responsible action is being taken.
- The organization’s people should be displayed as being human. Senior executives should show a sense that they care. They should avoid legal terms and overuse of technical jargon. In the FAA case study, there did not seem to be a public face for the FAA. As a result, most news articles simply quoted one or two FAA tweets then they quoted several tweets from frustrated passengers. This did not present the agency as being responsive to the public’s needs.

Incident Response Process

The incident response process is developed:

- Based on lessons learned from recent incidents
- To discern the event's nature (Caused by something unintentional like bad weather or a cut cable line or from something sinister such as hackers from a nation-state, hacktivists, or an organized crime gang
- Assist in choosing appropriate remediation/mitigation actions
- Keeping stakeholders informed such as customers, stockholders, or the general public

It is critical to discerning the nature of the event:

- It drives appropriate mitigation/remediation activities
- It helps determine response (Law enforcement, military, investigative, public relations)

The incident response processes and timelines for determining a response are detailed in the below table. These set of processes run through the spectrum from small and routine incidents to critical incidents requiring a large-scale effort. Once the origins of a security-related event have been determined, we need to decide the following:

- Mitigation/Remediation. We need processes to address rapidly mitigating the effects of an event and remediating the vulnerabilities that caused it.
- Investigative. The determined nature of an event will determine what processes and procedures must be implemented to support investigative activities such as the gathering of evidence and establishing a chain of custody. Often, these processes must be in place before an event takes place.
- Keeping stakeholders informed. Often, bad news or perceived bad news about security-related event can create an existential threat to the organization. Public relations and expectations about an event must be managed properly.

Routine Incidental		High Impact Incidents			Critical Incidents	
After 15 minutes	**Within 30 Minutes**	**Within 1 hour**	**Within 1 hour**	**Within 2 hours**	**Within 2 hours**	**Every 2 hours**
Step 1: **If the incident doesn't have a predetermined workaround or resolution, notify the Service Manager.**	**Step 2:** The Service Manager (SM) will conduct an initial assessment. Designated Incident Manager (DIM) to take over if criteria are met. If not contained or resolved, move to Step 3.	**Step 3:** The SM/DIM notifies IT Service Management, Client Services and NOC of the initial assessment of a high impact incident and estimated resolution. Assessment team may be convened during this time. If resolved, notify IT Service Management, Client Services and NOC of Incident, Resolution and Root Cause. If contained or service is restored, Post Mortem Reporting will be begin If not contained or resolved, move to Step 4.	**Step 4:** SM/ DIM sends communications to IT Executive Management Team, Leadership team, Assessment team and Communications Team. GIAC Wide Communications is sent. If contained or service is restored, Post Mortem Reporting will be begin. If not contained or resolved, move to Step 5.	**Step 5:** SM/DIM consults EMT Commander to determine whether a communication to GIAC staff is needed and escalation to Critical status. SM/DIM works with the Communications Team to draft a communication to end-users – either targeted group or all GIAC staff If Emergency Management Team (EMT) Commander takes over, steps 6 and 7 are to be followed. If EMT Commander determines Incident should not be escalated, proceed to Step 7.	**Step 6:** EMT is activated when an Incident is escalated to EMT Commander. *This activity coincides with Step 5.*	**Step 7:** Periodic communications will be sent every 2 hours until containment or resolution. *Post Mortem Reported will be begin following containment or restoration of service.*
Elapsed Time	30 Minutes	1 Hour 30 Minutes	2 Hours 30 Minutes	3 Hours	5± Hours	
Process Area	Incident Management	Problem Management			Service Continuity Management	

Incident Response Checklists

The report includes a checklist to help the incident response leader determine if the cause of the glitch is human error or malicious intent. For the checklist, examples are provided on what we would expect to find if it was user error or malicious intent.

Web Outage Incident Response Checklist

The below checklist describes the checklist for web outages:

Step	Activity
	Preparation
1	SOC has Splunk dashboards configured to identify DDoS and web intrusion attempts
2	SOC has a contact list on-call and an escalation chart for NOC, Network team and the web team.
3	GIAC is engaged with DDoS mitigation vendor Akamai for DDOS mitigation, which provide the following benefits: - It uses on-demand protection where the traffic is only routed following a request from the customer - Akamai monitors GIAC traffic using Netflow from routers. Profile GIAC traffic and generate alert when anomalies are detected
	Identification
4	SOC receives alert regarding possible GIAC web service outage or DOS/DDOS attack through secure email or phone call from: - Akamai - Splunk DDOS Detector Alert - Network team - NOC
5	The phone call is followed by a secure email with details, such as the source and destination IP addresses, along with a graph that depicts the anomaly
	Containment and Eradication
6	SOC analyst analyses the alert by verifying the traffic that is generated by: - Verifying Splunk dashboard and logs - Verifying PCAP
	<u>Website outage - Criteria to identify if it is web application related outage</u> Is the CPU utilization of the application server and database server normal when compared to the baseline? Is the memory utilization of application server and database server normal compared to the baseline? Is the database connection active? Is the number of connections to the server high compared to the baseline? Is the network performance normal compared to the baseline?

	Website outage - Criteria to identify if it is DDoS related outage Is there high UDP denied traffic compared to the baseline? Is there high ICMP traffic compared to the baseline? Is there high traffic volume compared to the baseline? Is there high CPU and memory usage in the perimeter firewall/router compared to a baseline? Is there higher volume of website request errors compared to a baseline? Is there lower packet volume from the web server compared to a baseline? Website outage - Criteria to identify if it is intrusion-related outage Were there any IPS signatures triggered before the website outage? Is there any port scan activity related to IDS signatures triggered before the website outage? Is there any SQL injection-related IDS signatures triggered before the website outage? Is there any privilege escalation related IDS signatures triggered before the website outage? Is there any high volume firewall or IPS drops before the website outage? Is there any login failure/brute force attempts before the website outage?
7	Based on the analysis, SOC analyst: - Creates incident case - Escalates the alert to the Incident Response team on call, the web server team, the network team and the NOC with relevant information for further action
Follow-up	
9	Follow up for updates regarding the alert
10	Update and close incident case

Based on prior experience and best practices the GIAC SOC has configured DDoS dashboards. For example, normally UDP traffic is used by DDoS tools if there is very high UDP dropped traffic it is an indication of DDoS. The contact lists are well established to prevent any last minute confusion during the incident. GIAC has DDoS mitigation service readily available when there is a DDoS attempt.

Network/Server Outage Checklist

The below checklist describes the checklist for network and server related outages:

Step	Activity
Preparation	
1	NOC/SOC has Splunk dashboards configured to identify network outage
2	NOC/SOC has a contact list on-call and an escalation chart for the NOC, the network team, and the web team
3	GIAC is engaged with Cisco for premium 24/7 support
Identification	
4	SOC receives an alert regarding a possible GIAC network service outage through secure email and phone call from: - Splunk Dashboards/alert - Network team - NOC
5	The phone call is followed by an email from with details such as the source and destination IP addresses, along with a graph that depicts the anomaly
Containment and Eradication	
6	SOC analyst analyzes the alert by verifying the traffic that is generated by verifying: - Splunk Dashboard and logs - PCAP & Netflow
	Network Outage - Troubleshooting Criteria Is there high UDP denied traffic compared to the baseline? Is there high ICMP traffic compared to the baseline? Is there high traffic volume compared to the baseline? Was there a power outage? Is the network outage contained to one data center? Are there alerts related to physical cables? Is the CPU and memory usage of the network device normal? Is the issue related to any recent configuration change? Is the issue related to any recent software or operating system upgrade? Is the issue related to automatic failover or recovery configuration? Is there any traffic to external networks prior to the outage? Is there any IDS/IPS alerts related to the network device IP address?
	Linux Server Outage Checklist Is the CPU, hard disk space and memory usage of the server normal? Are there any recent logs that are suspicious? Are there any suspicious cronjobs(scheduled jobs)? Are there any kernel messages which are suspicious? (dmesg) Is there a high number of Apache threads running? Are there suspicious arguments passed to the program? (cat /proc/<PID>/cmdline)

7	Based on the analysis, the SOC analyst: - Creates incident case - Escalates the alert to the Incident Response team on call, the network team and the NOC with relevant information for further action
Follow-up	
9	Follow up for updates regarding the alert
10	Update and close incident case

Application Outage DevOps Checklist

The below checklist describes the checklist for application related outages:

Step	Activity
Preparation	
1	NOC/SOC has Splunk dashboards configured to identify application outage
2	NOC/SOC has a contact list, on-call and escalation chart for NOC, Network team, application teams and the web team.
3	GIAC is engaged with application support vendors to have established support contract
Identification	
4	SOC receives alert regarding possible GIAC network service outage through secure email and phone call from: - Splunk dashboards/alert - Network team, application team - NOC
5	The phone call is followed by an email with details such as the source and destination IP addresses, application information, and the problem description
Containment and Eradication	
6	SOC analyst analyses the alert by verifying the traffic that is generated by: - Verifying Splunk dashboard and logs - Verifying PCAP & Netflow
	Application Outage Related to DevOps - Troubleshooting Criteria Is the issue related to any recent software/operating system upgrade ? Did the errors in the application increase after recent code deployment ? Is there any recent suspicious logins before the outage ? Is there any recent unauthorized code deployment before the outage ?
7	Based on the analysis, SOC analyst: - Creates incident case - Escalates the alert to the Incident Response team on call, the network team and the NOC with relevant information for further action
Follow-up	

9	Follow up for updates regarding the alert
10	Update and close incident case

Incident Response Examples - System Malfunction or Malicious Intent?

There are several indicators to check for when investigating whether the malicious intent was part of a system/network shutdown or glitch. Included below are a few of the common attack vectors associated with each of the relevant categories. It is important to note this is not an exhaustive or complete list and intends only to cover the more common attack vectors.

Website Glitch - Denial of Service (DoS) attacks (Incident)

Denial of Service attacks involves an attacker making a resource unavailable to legitimate users and disrupting regular service to the application, network, system, or service. An attacker may perform such an attack in a variety of different ways. Luckily for incident responders, DoS attacks are easy to detect; however, they can be time-consuming to halt and restore services when in progress. DoS attacks may be application-based or network based, both of which may negatively affect the performance of a production web server and network.

Network/Router - Denial of Service (DoS) attacks (Incident)

While there are many network based DoS of service attacks, one attack might involve an abnormally large amount of half-open connections that intentionally do not complete the TCP three-way handshake. To crash modern networks (or at a minimum, cause any real degradation of performance), an attacker must have access to a large number of "bot" machines that he controls.

Website outage - Criteria to identify if it is DDoS related outage

Is there high traffic volume to the website compared to the baseline?

Splunk Query
source=palo_alto giac.org|timechart span=1h count(packets) AS total_packets, values(date_hour) AS hour |lookup ddos_baseline_Packet hour |fields _time, total_packets, Baseline_Packet_Count

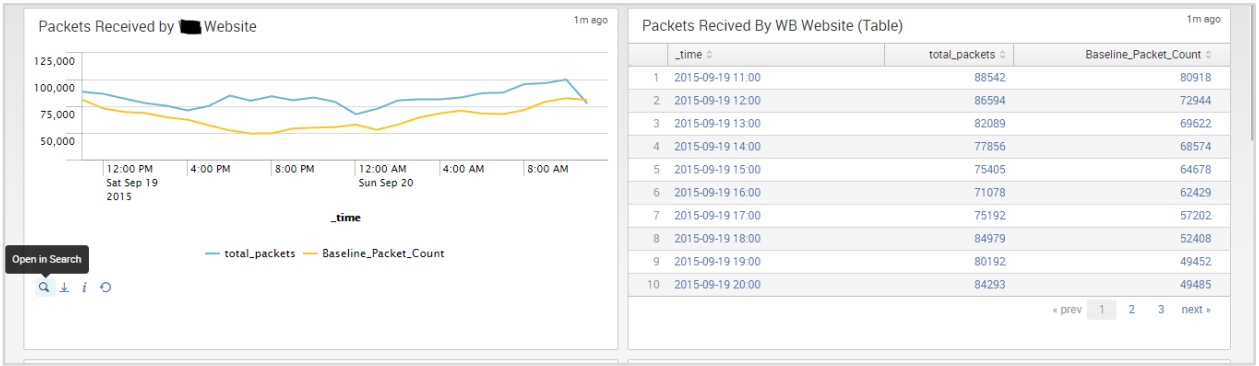

Figure 1: Splunk Output Outlining Current Usage Versus Baseline Usage

Is there high traffic volume to the firewall compared to the baseline?

Splunk Query
index=pan_logs_traffic source=palo_alto vendor_action=deny|timechart span=1h count(packets) AS total_packets, values(date_hour) AS hour |lookup ddos_baseline_Packet_FW hour |fields _time, total_packets, Baseline_Packet_Count

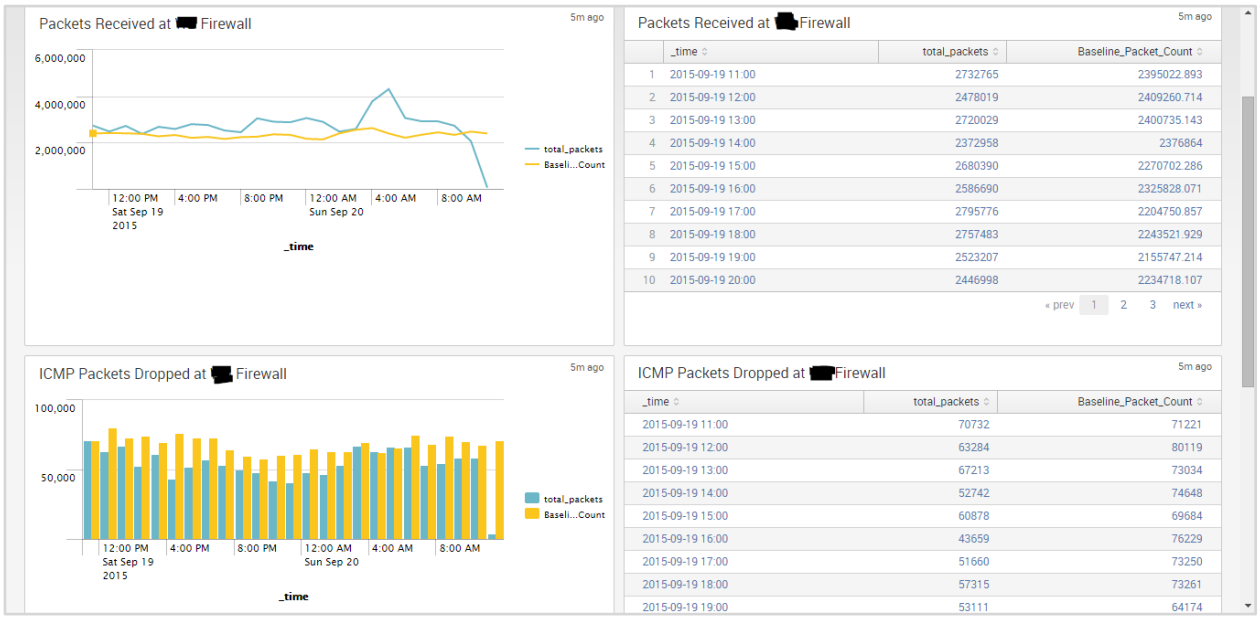

Figure 2: Splunk Output Detailing Amount of Dropped Packets

Are there high amounts of dropped ICMP traffic when compared to the baseline?

Splunk Query
source=palo_alto proto=icmp vendor_action=deny |timechart span=1h count(packets) AS total_packets, values(date_hour) AS hour |lookup ddos_baseline_Packet_ICMP hour |fields _time, total_packets, Baseline_Packet_Count

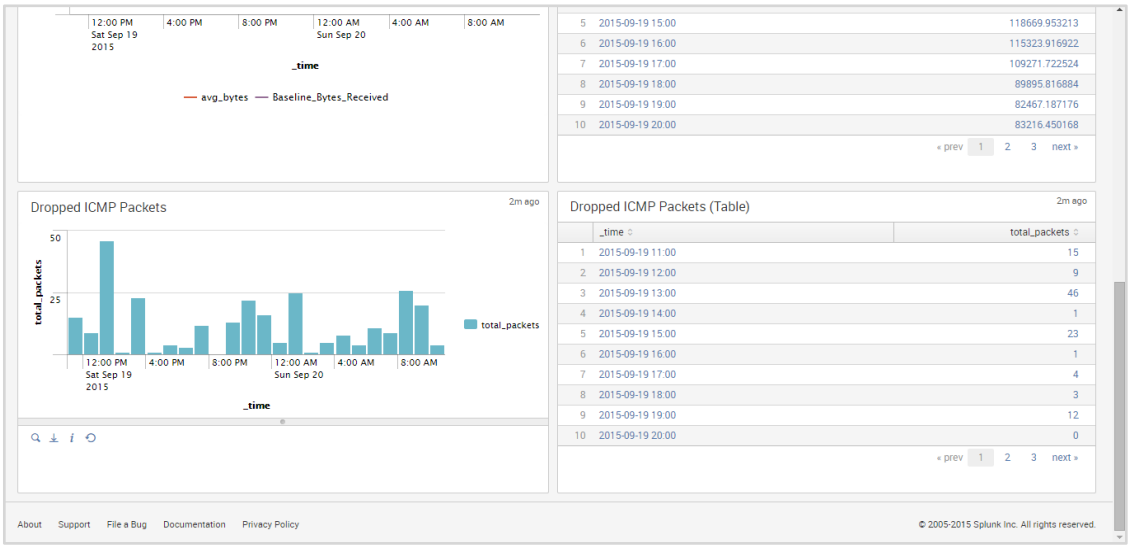

Figure 3: High Amount of Dropped ICMP Packets

Are there traffic size anomalies related to the web server compared to the baseline?

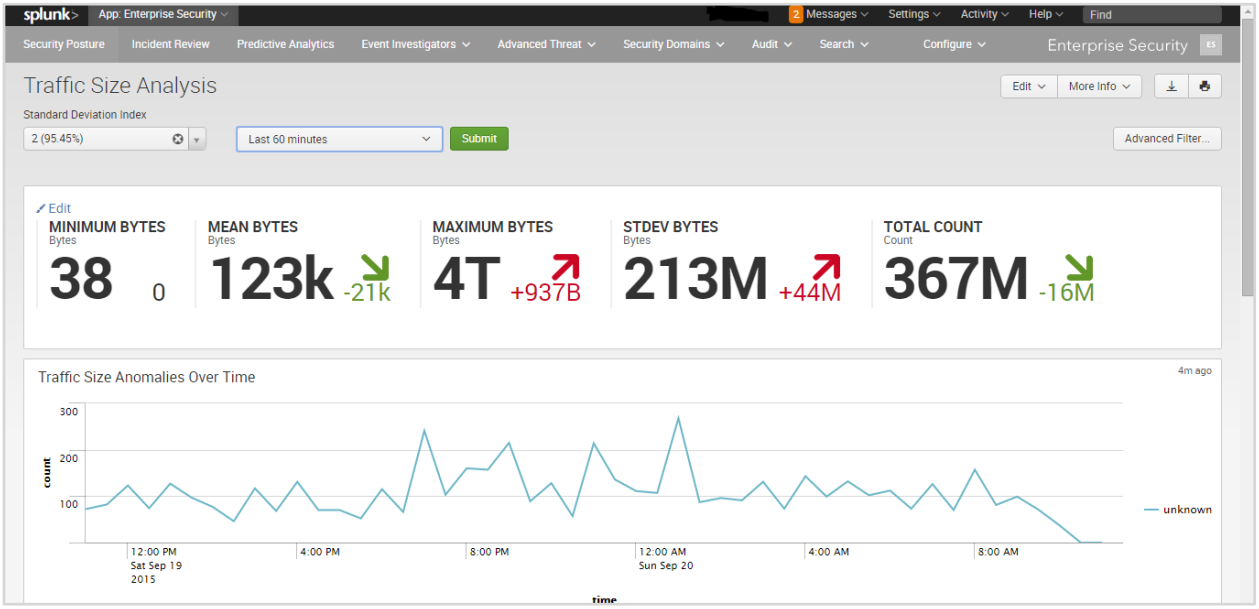

Figure 4: Splunk Output to Assist in Determining Traffic Anomalies

Are there high numbers of dropped UDP traffic compared to the baseline?

Splunk Query
source=palo_alto proto=udp vendor_action=deny |timechart span=1h count(packets) AS total_packets, values(date_hour) AS hour |lookup ddos_baseline_Packet_UDP hour |fields _time, total_packets, Baseline_Packet_Count

Structure Query Language (SQL) Injection (Incident):

SQL injection attacks occur when a malicious actor attempts to interrupt the execution of the backend web application by inputting specifically crafted characters. SQL injection attacks are an incredibly common attack vector among web application and can be difficult to defend adequately against. If a web application is having issues with glitches, crashing, or other bizarre behavior that is uncharacteristic and strays from the established baseline, check the web server's logs for a large number of error messages related to invalid input. Typically, an attacker is not successful with an SQL injection attack on the first try as they base their specifically crafted string off of the error responses received back from the server. While a web application may have input sanitization in place on user-supplied input, attackers still find ways to evade such filters.

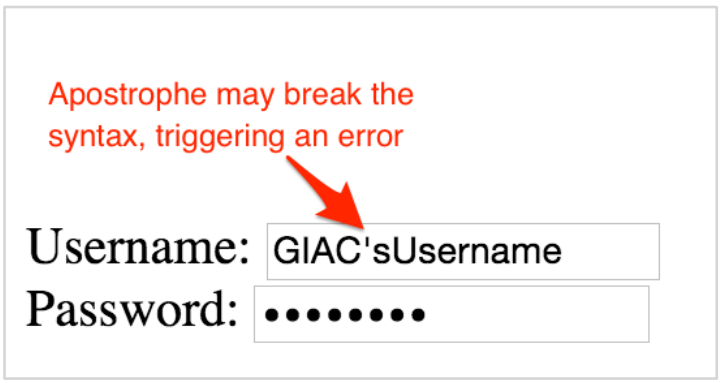

Figure 5: Apostrophe in Username Field May Cause Accidental Syntax Error in SQL Database

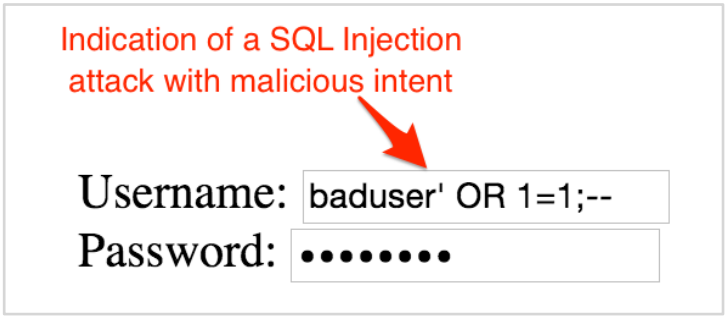

Figure 6: Indication of an SQL Injection attack with malicious intent. This simple attempt would likely be detected in IDS alert.

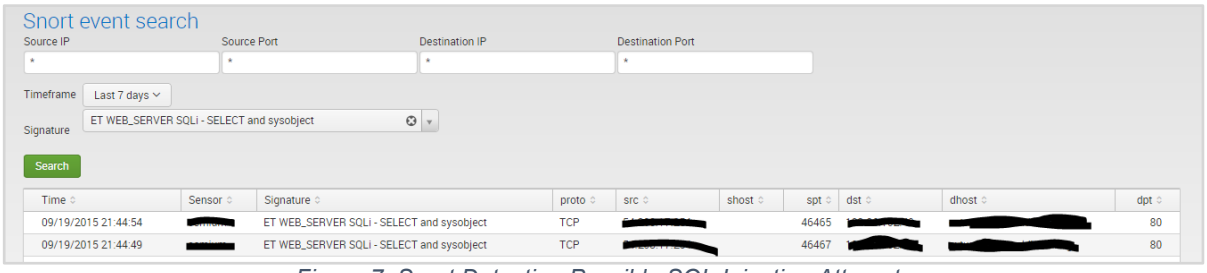

Figure 7: Snort Detecting Possible SQL Injection Attempts

Network/Router

- Login Brute Force (Incident):

Both administrative and standard user accounts are typically protected by some type of authentication mechanism. Attackers rely on weak authentication, such as a weak password, to quickly brute-force or guess the password of an account. If unauthorized changes or logins have occurred on the network router, check if there have been any brute force attempts against the router. Additionally, verify all accounts for unauthorized logins from foreign IP addresses.

The figure below outlines a password spraying attack, whereby an attacker uses a single common password across a large number of discovered user account profiles to prevent account lockout.

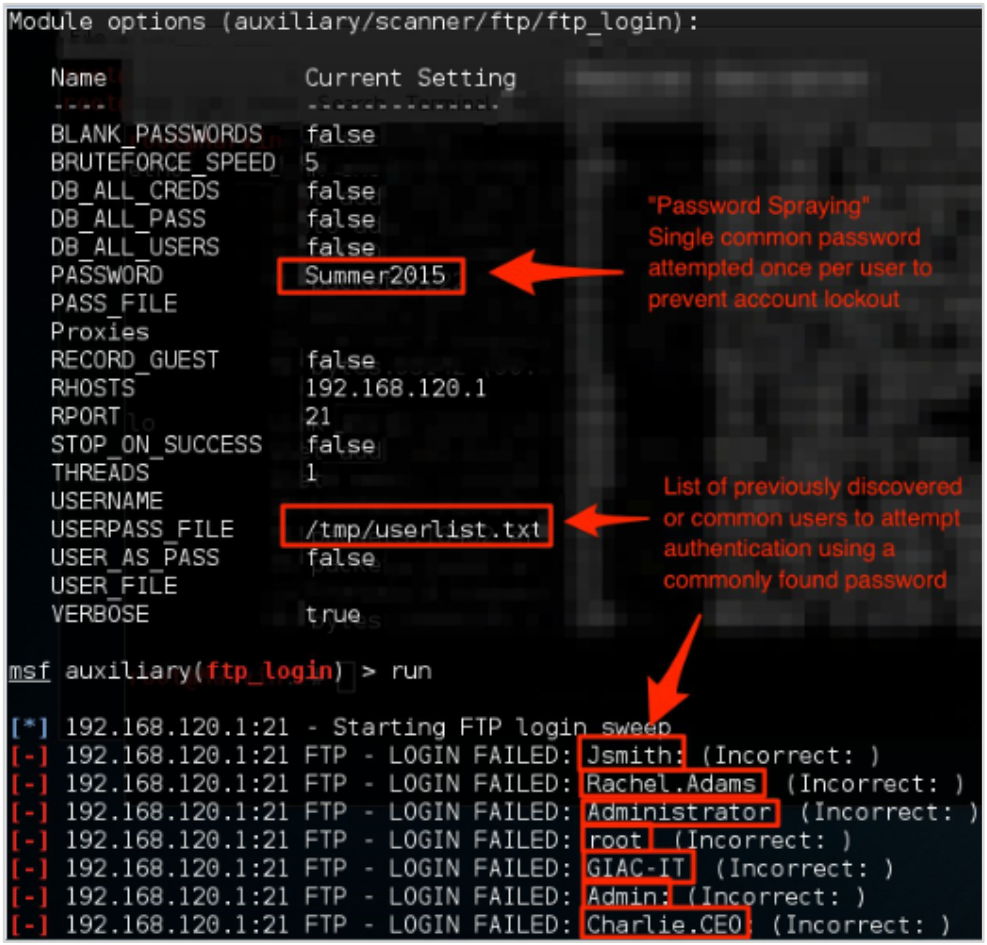

Figure 8: Example of a "Password Spraying" Attack - Easy to Detect and Compare to Legit Password Related Traffic

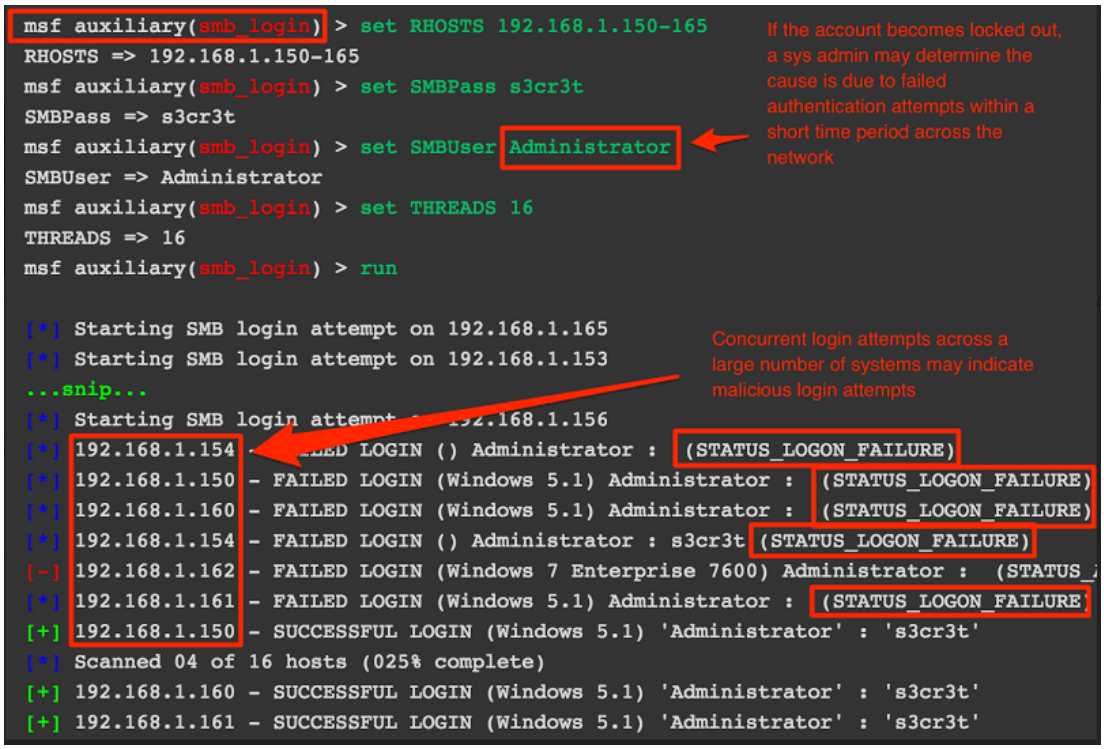

Figure 9: SMB Login Attack that Sends the Same Set of Credentials to a Large Number of Machines in a Short Period of Time, Indicating a Possible Attack Scenario

Splunk Query & Dashboard

Splunk Query - Logon Failure per User Account
sourcetype="Snare:Security" (EventID=4771 AND Type="Failure Audit" AND Failure_Code=0x18) |stats count as Logon_Failure by Account_Name |sort - Logon_Failure

Splunk Query - Account Locked Out per User Account
sourcetype="Snare:Security" (EventID=4740) |stats count as Account_Locked_Out by Account_Name |sort - Account_Locked_Out | fields Account_Name,Account_Locked_Out

Splunk Query - Windows Audit Log Cleared
sourcetype="Snare:Security" (EventID=1102 OR EventID=517) | eval Date=strftime(_time, "%Y/%m/%d") | stats count by Account_Name, Date, host, index, CategoryString, Message | sort - count | rename Account_Name as "Account Name"

Splunk Query - Excessive Delete Files
sourcetype="Snare:Security" (EventID=4663 AND Accesses = "DELETE" AND Object_Type=File) NOT User=N/A Security_ID!="NT AUTHORITY\\SYSTEM" Security_ID!="S-1-5-18" | stats count by Account_Name | sort - count

Computer or "Automation" Glitch

Hardware and software may crash at any moment for nearly any reason. When a computer crashes, this does not immediately serve as definitive evidence that the computer has been compromised or is actively under attack. For example, there may be a fault application with a memory leak issue that, after being used for a certain period of time without being restarted, may slowly increase its memory requirements until the computer runs out of memory to handle the application and results in a crash.

- Incompatible Patches (Event):

As it is important to keep critical and productions up-to-date with the latest security patches from the vendor, many companies rush to patch affected systems to prevent compromise. Unfortunately, it is all too common for a company to apply quickly the latest patch to a production system or application before testing the patch in a staging environment first. This can cause a variety of incompatibility issues in the current system, such as crashing, rebooting, or rendering another application unusable under the new patch. If a system or application crashes, determine if patches have recently been applied to the system. If so, consider removing the system or application to a previous state by removing the patch to check if the issue resolves.

- Missing Critical Security Patches (Event):

While applying patches to a production environment prematurely may cause compatibility issues, failure to apply critical security patches may result in a compromise. On the suspected compromised system, are there critical security patches missing as identified in the updated vulnerability scanning utility? Ensure software version remain up to date and utilize a modern and vendor supported version.

- Administrative Only Changes (Incident):

Attacks may abuse certain administrative functions. Depending on the scenario, an attacker may find that the web server is running as an unnecessarily high privileged user, such as with system or root privileges. In this case, once an attacker is successful at compromising the website, they will then have unrestricted access to make dangerous changes to the web server. Additionally, if a web server is running under the privileges of a very limited user but recent unauthorized changes were made in the context of an administrator account, the attacker may have illegitimately obtain access to an administrator's account. Check account history for previous successful login sessions, ensure the source IPs match that of a valid administrator, and verify that the password has not been changed on the account. By verifying and tracking any changes made to the website, it can be easier to track the possible existence of an attacker by determining the privilege level utilized to accomplish the suspected task.

- Antivirus / IDS / IPS Logs (Event):

If the system encounters issues, review the antivirus, IDS, and IPS logs for malicious activity, such as the detection of malware, or other signature and anomaly-based traffic types. (Show Splunk logs for event vs malicious incident)

DevOps Example

After deploying code increase in warnings might indicate buggy code:

Figure 10: Warnings in a Code Deployment that May Not be an Indication of Malicious Intent

Conclusion

By following established processes, the GIAC IT team will be able to determine if the cause of a glitch is human error, automation error, or malicious intent. The GIAC IT team will be capable of providing a clear root cause analysis and communicate this appropriately with external media when necessary. This will ensure that the GIAC does not lose the investor's confidence, maintain the company's stellar reputation, and promote a quick recovery in the case of an incident.

References

https://www.reddit.com/r/sysadmin/comments/1646l8/linux_server_outage_checklist/

http://www.mainebankers.com/images/stories/MECB/2013/Bank_Expo_2013/DDoS_Preparation_and_Response--Greene.pdf

https://www.linkedin.com/pulse/checklist-build-devops-organization-thomas-theakanath

https://www.sans.org/reading-room/whitepapers/incident/incident-handling-annual-testing-training-34565

http://www.inquisitr.com/2341579/faa-fixes-glitch-that-cancelled-hundreds-of-flights/

http://www.csmonitor.com/USA/USA-Update/2015/0816/FAA-struggles-to-modernize-as-glitch-grounds-hundreds-of-flights

http://www.aviationtoday.com/av/commercial/ERAM-Not-the-Cause-of-Major-Flight-Delays-FAA-Says_85803.html#.Vf5frbnsned