IMPORTANT: For ANY question you are not able to determine the answer to, you must do the following: (1) in your answer to that question, explicitly state that there is insufficient information available to determine the answer, & **(2)** include an appropriate RECOMMENDATION requesting access to whatever additional evidence sources would allow you to actually answer that question.

SITUATION

The SITUATION section provides a fairly brief overview of the situation or incident that triggered the investigation you are about to undertake.

SITUATION should contain NONE of your conclusions or findings determined *after* actually beginning your investigation. All investigation findings belong in the ASSESSMENT section.

S1 Write a 1-2 sentence summary of the instigating incident or "situation" that kicked off this investigation in the first place.

Another security analyst recorded a PCAP of a possible remote intrusion attempt on the private network belonging to client AT-USA.

S2 If this investigation concerns a particular client, name it here. (Upon whose behalf are you conducting this investigation?)

The private network belongs to a client named AT-USA - which we are conducting this investigation on behalf of.

S3 Reiterate any relevant hypotheses or observations included in whatever information you were provided at the onset about the instigating incident.

~~A multitude of failed authentication attempts within the short span of ~1.5min point towards this being a malicious Brute Force attack using a tool named ‘Hydra’, and not the result of failed user sign-in attempts.~~

I was informed that there was a series of failed authentication attempts on our client AT-USA’s private network.

What I’ve hypothesized is that an attacker has attempted to gain unauthorized access to the AT-USA network.

S4 Is this investigation related to any other previous OR ongoing investigations? If so: identify and cite the previous OR ongoing investigations.

No - there is no previous evidence that has been given/revealed that this incident is related to a previous or ongoing investigation.

BACKGROUND

The BACKGROUND section describes in greater detail the information you were given prior to beginning your investigation. Enrich the information about the instigating incident by determining the information can be gathered from logs or people about what might have led up to the incident.

BACKGROUND should contain NONE of your conclusions or findings determined *after* actually beginning your investigation. All investigation findings belong in the ASSESSMENT section.

B1 What is the date and time[range] of the *reported* incident? Be sure to include the timezone.

Date: Dec. 6 2017, Time Range: 18:34:19.962565 - 18:35:47.958228 GMT

Time: 18:34:45.670837 GMT [Client response]
Time: 18:34:45.692311 GMT [Server response]

B2 What exactly is the task that has been assigned to you? (What must you determine before your investigation can be considered completed?)

My task is to analyze the PCAP and the failed authentication attempts, cross reference this with log data in the SIEM, and confirm or disconfirm malicious activity.

B3 Who assigned the investigation of this incident to you?

Virgil reached out to me regarding the incident and asked to investigate the issue further.

B4 What sources of evidence were you given access to in order to conduct your investigation? (An older SBAR? SIEM logs? PCAP? Memory image? Forensic disk image? The ability to interview specific employees? **If you have been given access to it during your investigation, make it clear here!**)*

** If any of your provided evidence sources feature only evidence from a particular timestamp or date||time range, **this is the place to make note of it.***

I was given access to a PCAP file containing a log of the suspicious activity; as well as access to the database of log-based metadata collected within the Splunk SIEM.

ASSESSMENT

The ASSESSMENT section contains "answers" to all the outstanding questions your investigation was tasked with addressing.

This is usually the meatiest part of the report: you are presenting the bulk of your investigation findings in this section, providing the final analysis & implications of the information that was gathered during the course of the investigation. Remember: as an analyst, it is your job to connect all the dots based on the evidence you are able to dig up; if you describe a specific detail or event, ensure you are making it clear why you are including that information. What is its meaning||significance||implications? Your answers should clearly include this context about the information you are providing.

Details about the specific evidence you discovered that supports the findings you describe here should be included in the TECHNICAL APPENDIX; the answers here should **only** include findings you were able to determine from the examination of that evidence during the course of your investigation.

A1 ANY CORRECTIONS TO MAKE TO INFO REPORTED IN S OR B? • Did you discover that any founding hypotheses reported in the SITUATION or BACKGROUND section were incorrect? If so: you should state explicitly what you determined to be incorrect, along with the relevant corrected information.

~~There are no corrections or amendments needing to be made to the information reported in S or B at this time.~~

An amendment to the hypotheses reported would be that the malicious host (IP 10.5.10.105) seems to be internal, as the IP address is private. This changes the dynamic of the attack, and could potentially point towards the attacker being someone on the inside (insider threat). With the amount of failed authentication attempts in such a short timespan, as well as the detection of ‘Hydra’ in the useragent, we cannot dismiss this situation as being potentially non-malicious.

A2a WHAT HAPPENED • **How did this take place?** (What tool(s) or technique(s) caused the incident to occur?)

This was a Brute Force attack carried out by a password guessing tool named ‘Hydra’.

A2b WHAT HAPPENED • **What is the full date||time range of the entire incident? Are there distinct timeranges that define specific "clusters" of activity? At what particular timestamps did important events occur at?**

~~Full time range of the entire incident is: Dec. 6 2017, Time Range: 4PM - 8PM GMT (16:00-20:00 PM GMT)~~

~~The time range of 4-5PM GMT contained 22,224 events; and the time range of 6-7PM contained 15,086 events – very large clusters of activity.~~

~~Important activity regarding the *reported* incident began occurring at: 6:34:24 - 6:35:33 GMT, where an influx of authentication attempts occurred~~

[2019-11-23 18:14 UTC] ARP poisoning (begins): ATTACKER begins using network pentesting tool (bettercap) to MITM internal traffic using ARP cache poisoning. *LAN traffic within the 10.5.10.0/20 subnet begins to be captured and monitored by ATTACKER.* [10.5.10.118, 10.5.10.0/20]

[2017-12-06 6:15:07 GMT] First successful unauthorized authentication of the WP instance occurs; Credentials used are currently unknown.

[2017-12-06 6:34:45 GMT] Second successful unauthorized authentication of the WP instance occurs; Credentials are - login: admin, password: Winter2017wp@dmin

[2017-12-06 6:47:02 GMT] Third successful unauthorized authentication of the WP instance occurs; Credentials used are currently unknown.

[2017-12-06 6:51:01 GMT] Fourth successful unauthorized authentication of the WP instance occurs; Credentials used are currently unknown.

3,981 events occur [2017-12-06 6:15 PM GMT] - this correlates with the first successful unauthorized authentication of the WordPress instance on 10.5.20.16

1,302 events occur [2017-12-06 6:18 PM GMT] - the majority of these events seem to be consisting of ‘Built TCP’ and ‘Teardown TCP’ connections*

2,487 events occur [2017-12-06 6:34 PM GMT] - this correlates with the second successful unauthorized authentication of the WordPress instance on 10.5.20.16

2,322 events occur [2017-12-06 6:35 PM GMT] - the majority of these events seem to be consisting of ‘Built TCP’ and ‘Teardown TCP’ connections*

1,280 events occur [2017-12-06 6:46 PM GMT] - the majority of these events seem to be consisting of ‘Built TCP’ and ‘Teardown TCP’ connections*

1,381 events occur [2017-12-06 6:49 PM GMT] - the majority of these events seem to be consisting of ‘Built TCP’ and ‘Teardown TCP’ connections*

*Seeing a large number of "Built TCP connection" and "Teardown TCP connection" events in the logs is not necessarily an indicator of malicious activity on its own - these log messages are common in network communication, and legitimate activities like users accessing web services, applications connecting to databases, or machines communicating with each other can generate numerous TCP connections. While all this is true, the large spikes surrounding the unauthorized authentications indicate they are most likely related to those attempts.

A2c WHAT HAPPENED • **What actually happened during this incident?** This should be a description of the sequence of events that occurred during this incident, listed in chronological order. This should be one of the lengthier answers in your SBAR!

A Brute Force attack was carried out by a password guessing tool named ‘Hydra’ coming from an internal host with the IP 10.5.10.105.

A web application instance of a WordPress site was the target, specifically an admin level account - vulnerabilities that allowed this attack were: no multi-factor authentication safeguard, no account user lockout policy, and credentials that were not strong/unique enough.

The IP of attacked device is 10.5.20.16. In terms of gaining unauthorized access to the web app instance, this attack was successful. The brute force attack carried out via Hydra was able to guess the credentials to the WordPress instance on the device with the IP 10.5.20.16 (login=admin, password=Winter2017wp@dmin).

There were multiple successful authentications (4 total), and it looks like each successful authentication came from the same IP (10.5.10.105), via the work of the Hydra password guessing tool.

A3 ROOT CAUSE ANALYSIS • **What vulnerable services or threat vectors were taken advantage of during this incident?** Note version number whenever possible.

~~The threat vector used to gain initial access was a Brute Force attack, via a password cracking tool named 'Hydra'~~

The web application whose authentication form was brute-forced was: WordPress/4.9.1; http://10.5.20.16. The authentication form for the web app instance was vulnerable due to several reasons: It did not contain any method of multi-factor authentication, the credentials were too lenient and easily obtainable/guessable, and there were no account lockout policies in place - these security measures (had they been in place) could have assisted in the prevention of the attack.

A4a SCOPE • **How large is the scope of the incident?** *How* many devices were affected in *what* way?

~~At the moment, we only have information that (1) domain level account belonging to a WordPress site has been compromised. Depending on the contents of this site and the users permissions, there could be data or other related information at risk.~~

Upon further inspection, it seems the host with the IP of 10.5.10.105, has a private IP address and is an internal host. This deepens the scope of this incident, and points towards a potential insider threat.

A4b SCOPE • **Which internal hosts were involved?** Be sure to list the role that each internal device played in this incident. *Include both hostname and IP address whenever possible.*

Host: LAB-5505-asa, IP: 10.5.20.16: this is the host that was attacked. An admin account was accessed; there is insufficient information as to what this account has access to to determine an outcome at this time. Recommendation would be to contact the account admin/owner to obtain further information.

IP: 10.5.10.105: This is the host that is acting maliciously; with a private IP address, this host is within the private network and potentially belongs to one of our own employees.

<HOSTNAME> (<IP ADDRESS>): <ROLE this device played in the incident>. [Level of COMPROMISE; <ultimate OUTCOME>.]

A4c SCOPE • **Were any users OR services OR devices compromised?** If so: describe what, exactly, was compromised...& what caused the compromise?

A Brute Force attack solved the login and password (log: admin, pwd: Winter2017wp@dmin) of a WordPress site - no other services/users were found to be compromised at this time. Currently, we do not know the credentials that were used for the (3) other successful authentication attempts at this moment.

what credentials were used during any of the three other successful authentication events).

A4d SCOPE • **Which external hosts were involved?** Be sure to list the role that each external host played in this incident. *Include both resolved domain name and IP address whenever possible.*

<HOSTNAME> (<IP ADDRESS>): <ROLE this device played in the incident>. [Level of COMPROMISE; <ultimate OUTCOME>.]

Currently we have no evidence of external host activity. The malicious host has a private IP address range, indicating that they are within the network (internal).

~~Host: Cisco_1c:1f:eb, IP: 10.5.10.105: This is the host that is acting maliciously; it has gained access to a Domain-level account. The full details on how severe this action is are unclear as we do not have sufficient information regarding what is on the hacked account.~~

A5a SEVERITY • **How serious is this incident?** Assess the severity of the incident by taking into consideration factors like whether anything of potential value was compromised, and how much this incident disrupted normal business functioning.

The severity of this incident is high as an unknown, possibly malicious outsider has gained unauthorized access to a host on a client's private network. There could be sensitive information that is at risk, though we do not have sufficient information to confirm this. Obtaining further information on the contents of the accessed account is recommended. Despite the insufficient information, we do know that the attacker used a popular pentesting tool, but did not change the user agent string, which suggests they could be extremely novice or do not care about getting caught. Additionally, the web application does not appear to be frequently used; the only traffic recorded in the SIEM is associated with the attacking device, with no legitimate visitors during the observed time period.

A5b SEVERITY • **Of the compromised users OR services OR devices, were any of particular value to an attacker?** This answer should address whatever you described in the answer to Were any users OR services OR devices compromised?.

At this moment, there is insufficient evidence whether the contents of the accessed account contain sensitive information. Further investigation into this account is recommended. The administrator level account that was compromised could prove to be valuable to the attacker as it most likely has elevated privileges. Access to this account could also be valuable if it contains sensitive information to other devices on the network.

A5c SEVERITY • **Did $whatever_was_compromised have access to $anything_of_value?**

At the moment, there is not sufficient information to determine whether the compromised system had access to anything of value. Further recommendation would be to contact the system admin/account owner to determine this.

A5d SEVERITY • **Was $anything_of_value stolen||exfiltrated during this incident?**

There is insufficient information available to determine whether any sensitive information/anything of value was exfiltrated/extracted as a result of this incident.

A6a INCIDENT RESPONSE (SO FAR) • **Has the threat been contained?**

~~This information was not made available in the initial briefing to be able to answer this. My recommendation would be to request additional information from management to determine whether or not the threat has been contained.~~

To my existing knowledge, the threat has not been contained/remediated.

A6b INCIDENT RESPONSE (SO FAR) • **To your knowledge, were any immediate mitigations put into place?**

There is insufficient information available to determine this. My recommendation would be to follow up with management/any other analysts working alongside this investigation in order to establish whether or not mitigations are currently in place.

RECOMMENDATION

The RECOMMENDATION section is where you reflect on how the organization might prevent incidents like this from happening in the future—be proactive! Be forward-thinking!

Always explicitly state your reasoning for making a particular recommendation.

REMEMBER:

- **You must always make a cost||benefit analysis when considering recommendations—prioritize solutions that offer the *greatest coverage* for the *least***

amount of effort. The amount of effort required by the organization to implement a suggestion should absolutely be justified by the degree of protection undertaking such an implementation would afford. Your recommendations are only as valuable as they are realistic to actually implement.

- **Be sure to include sufficient information about each recommendation** so that if another employee were tasked with implementing your recommendations, they will not need to do any additional research in order to implement your suggestion. If you're recommending that additional research into determining a viable specific solution be made, that should be stated explicitly.
- **Do not make *generic* security recommendations that are NOT related to what occurred during this incident;** each recommendation you make should be obviously related to something that is involved in the incident you are writing this SBAR about.

INCIDENT RESPONSE||TRIAGE

Try to include some immediate incident response triage recommendations. What immediate recommendations would you make to help contain the incident and prevent it from potentially escalating in SEVERITY &&|| SCOPE?

R1a INCIDENT RESPONSE||TRIAGE • **Should any devices be considered compromised and quarantined and/or reimaged?** If so: list each, describing what exactly should be done.

~~http://10.5.20.16/wp-login.php should be considered compromised - this WordPress site was the victim of Brute Force attack and should be further analyzed for any sensitive information being exploited.~~

The WordPress instance on the server should be considered compromised - and the threat should be considered ongoing/not contained. A recommendation would be to isolate the server and have a forensic image taken in order to determine the extent of the attacker’s access. The device associated with IP 10.5.10.105 should be considered compromised and needs further forensic analysis in order to determine if this attack was carried out via remote intrusion/or another route.

R1b INCIDENT RESPONSE||TRIAGE • **Should any credentials be reset?** If so: belonging to which user(s) and/or services?

~~I would recommend resetting the login and password belonging to the user: 'admin' (password/pwd: Winter2017wp@dmin). These were cracked during the brute force attack and should be considered unsafe to leave in their current state.~~

Since the attacker was able to crack administrator-level credentials to the web application instance, other existing accounts should be considered potentially compromised as the attacker could change the password to any of them. As such, all credentials related to the web site should be reset, and all currently existing accounts should be vetted to verify they belong to legitimate users.

R1c INCIDENT RESPONSE||TRIAGE • **Should any devices be singled out for additional analysis? (Should any logs be gathered from a particular device?)** If so: be sure to specify which device(s), what evidence you would want to access on each device, and what unanswered||remaining||open questions examining this additional evidence would help you resolve.

The device associated with IP 10.5.20.16 should be singled out for additional analysis. Further information regarding anything sent out from that device should be singled out. Authentication logs from the web application instance hosted on this server would also allow us to definitively determine which other user credentials were successfully compromised by the attacker. The device associated with IP 10.5.10.105 should also be singled out for additional analysis if possible - investigation of this device would help in uncovering further details on the attack.

R1d INCIDENT RESPONSE||TRIAGE • **Do any employees need to be questioned?** If so: whom, and regarding what? What unanswered||remaining||open questions would interviewing this employee help you resolve?

The owner of the account that was compromised should be questioned to determine whether there is sensitive data on the account, and what other things the account has access to in order to determine if any other systems or data is vulnerable. If possible, the owner of the device associated with 10.5.10.105 should also be investigated as they committed a serious crime - questioning them may help determine whether that device was remotely accessed to commit the malicious acts.

R1e INCIDENT RESPONSE||TRIAGE • **Does anybody—people or companies—need to be notified about this compromise or breach?** If so: whom, and what exactly do they need to be informed about?

The client, AT-USA, should be informed if they are not already aware of the compromise. The system administrator, the owner of the account, and all network analysts/related employees should be informed.

R1f INCIDENT RESPONSE||TRIAGE• **Do any new investigations need to be started?** If you discovered any potentially suspicious activity that turned out to not be related to your current investigation, be sure to specify here.

~~-I would recommend looking into other systems/accounts that could be access through the breached account.~~

I have yet to uncover any new details unrelated to my current task that warrant a new investigation.

R1g INCIDENT RESPONSE||TRIAGE • **Should any old or ongoing investigations be amended with corrected information discovered during this investigation?** If this investigation is related to a another investigation and you were able to determine any of the other investigation's findings were incorrect, specify what needs to be amended here.

There is no evidence /information that points toward old or other investigations needing to be amended

PREVENTION OF FUTURE INCIDENTS OF THIS TYPE

In your ASSESSMENT section, you should have identified in A3 (*What vulnerable services or threat vectors were taken advantage of during this incident?)*—whatever you identified in answering that question...you want to make remediation recommendations, whenever possible, on how to better protect that threat vector from being abused again in the future. What options does the client have when it comes to deciding how to prevent these in the future?

R2a PREVENTION • **Can you recommend any changes that could be implemented within the company's internal infrastructure that would actively prevent another attack like this from succeeding in the future?**

It seems this attack was detected fairly quickly, though making sure that the network is configured with an Intrusion Detection System (IDS), and that this system is properly monitored around the clock. Using 2-factor authentication has also been shown to help prevent brute force attacks.

R2b PREVENTION • **Can you think of any changes that could be made to the company's standard internal policies might better protect the company's infrastructure from being so vulnerable to this type of attack?**

I would recommend that 'admin' level accounts have their passwords meet certain criteria to avoid and prevent similar attacks in the future - this would be my top priority regarding this form of attack. Implementing an account lockout policy after a certain number of failed login attempts would also be extremely helpful in preventing passwords from being guessed in any future brute-force attacks. Including a multi-factor authentication method would also add another layer of needed security.

TECHNICAL APPENDIX

The TECHNICAL APPENDIX is where you "show your work" for the findings you have described in detail in the ASSESSMENT section.

REMEMBER:

- The potential reader of this SBAR is likely distracted and strapped for time—if they need to dig into the technical details of your analysis, they should be able to reproduce your results that led you to your conclusions using the details you include in your TECHNICAL APPENDIX. Keep the SBAR clear and concise by providing answers that are easily grasped *even if your reader is scanning your report quickly for relevant information.*
- All information required to reproduce your findings reported in the SBAR proper should be included here. If you were to need to replicate your investigation findings a year from now (after you've forgotten all the details yourself), what technical details would you want to have provided here to help save you time replicating your original findings? That's exactly what should be included here.
- Feel free to include Splunk search result URLs for valuable search queries, but if you do: clearly describe *why* the search was valuable so that nobody has to click it, load it, and then guess how it is relevant.

A2a - Technique IDs from MITRE ATT&CK: Domain account (T1078.002*), Brute Force Password Cracking (T1110.002*) https://attack.mitre.org/tactics/TA0001/ (T1078.002)

https://attack.mitre.org/tactics/TA0006/ (T1110.002)

WireShark filter to find successful authentication packet:

```
(((((!(tcp.flags == 0x002)) && !(tcp.flags == 0x012)) && !(tcp.flags == 0x010) && !(frame contains
"Lost your password?")) && !(tcp.flags == 0x011) ) && !(http.request.method == "GET")) &&
!(stp.protocol == 0x0000)
```