UML Flowchart: Peer Responses

Course: MSc Computer Science

Module: Secure Software Development (Computer Science)

Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Peer Response 1:

In response to:

Kikelomo Obayemi

Initial Post

75 days ago

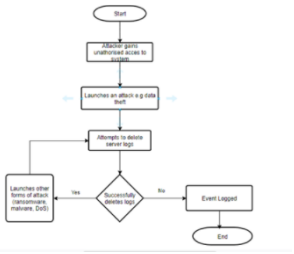
5 replies

Last 55 days ago

The OWASP top 10 is a document designed to create awareness to organisations and developers on the 10 most critical security risks of web applications (OWASP, 2021). The **A10: 2017 Insufficient Logging and Monitoring** risk addresses how attackers could exploit Insufficient logging and monitoring of critical events in a system and are able to achieve their goals without being detected (OWASP, 2017). Some common examples of critical events are login (successful and failed), password changes and high value transactions (Sahoo, 2021). According to OWASP (2021), recent breach studies revealed that it takes over 200 days (enough time for serious damage to be done) on the average to detect a security breach which is typically discovered by an external party rather than internal monitoring processes.

One key mitigation against this weakness is the implementation of logging facilities on critical operations of a system (Bach-Nutman, 2020). Sahoo (2021) suggests that logs should be backed up and synced to another server where they cannot be cleared. Alerting systems should also be created to send out alerts when certain events have been triggered or a particular threshold is reached (Sahoo, 2021). In consideration of these, my proposed software design would incorporate logging facilities (tools and databases) into a class diagram so that clients can visualize the relationship with other aspects of the system. I would also use an activity diagram to show the flow of activities from the start of a critical event to the end. Activity diagrams show sequential, branched and concurrent flows and as such can be very helpful in understanding the full operations of a system (tutorialspoint, 2021)

Flowchart



References

Bach-Nutman, M., 2020. Understanding The Top 10 OWASP Vulnerabilities. Available from: https://arxiv.org/ftp/arxiv/papers/2012/2012.09960.pdf [Accessed 15 August 2021]

OWASP (2021) OWASP Top 10, Available from: https://owasp.org/www-project-top-ten/ [Accessed 15 August 2021]

OWASP (2017) OWASP Top 10 – 2017: The ten most critical software web application security risks. Available from: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf [Accessed 16 August 2021]

Sahoo (2021) What is insufficient logging and monitoring and how can it be prevented? Available from: https://www.vistainfosec.com/blog/what-is-insufficient-logging-monitoring-and-how-can-it-be-prevented/ [Accessed 15 August 2021]

Tutorialspoint (2021) UML Activity Diagrams. Available from: https://www.tutorialspoint.com/uml/uml_activity_diagram.htm [Accessed 16 August 2021]

Post:

Hi Kike,

Very well put together post, focusing on the methods undertaken by ‘black hat hackers' to disguise their activities from an organisation. I find it interesting that the studies show that it takes over 200 days to detect a data breach in some instances, thus highlighting the need for regular system audits and associated log files.

Guidance from the UK National Cyber Security Centre suggests that organisations should aggregate logs as quickly as possible, ensuring that these are securely

transferred to a central repository to reduce the risk of information potentially being lost (National Cyber Security Centre, 2021). Not only can logs be used to identify cybersecurity incidents, but they can be used for identifying operational trends, as well as supporting general internal investigations (Berkeley Information Security Office, n.d.).

To which extent do you agree that businesses should be performing regular audits of their logs to identify cyber-attacks, as well as monitoring the behaviour of employees within the business (For example, applications executed and their sources)?

References:

Berkeley Information Security Office. (n.d.) Security Audit Logging Guideline. Available from: https://security.berkeley.edu/security-audit-logging-guideline [Accessed 21st August 2021].

National Cyber Security Centre. (2021) What exactly should we be logging?. Available from: https://www.ncsc.gov.uk/blog-post/what-exactly-should-we-be-logging [Accessed 21st August 2021].

Screenshot:

Post by **Kieron Holmes**
Peer Response

71 days ago

Hi Kike,

Very well put together post, focusing on the methods undertaken by 'black hat hackers' to disguise their activities from an organisation. I find it interesting that the studies show that it takes over 200 days to detect a data breach in some instances, thus highlighting the need for regular system audits and associated log files.

Guidance from the UK National Cyber Security Centre suggests that organisations should aggregate logs as quickly as possible, ensuring that these are securely transferred to a central repository to reduce the risk of information potentially being lost (National Cyber Security Centre, 2021). Not only can logs be used to identify cybersecurity incidents, but they can be used for identifying operational trends, as well as supporting general internal investigations (Berkeley Information Security Office, n.d.).

To which extent do you agree that businesses should be performing regular audits of their logs to identify cyber-attacks, as well as monitoring the behaviour of employees within the business (For example, applications executed and their sources)?

References:

National Cyber Security Centre. (2021) What exactly should we be logging?. Available from: **https://www.ncsc.gov.uk/blog-post/what-exactly-should-we-be-logging** [Accessed 21st August 2021].

Berkeley Information Security Office. (n.d.) Security Audit Logging Guideline. Available from: **https://security.berkeley.edu/security-audit-logging-guideline** [Accessed 21st August 2021].

Peer Response 2:

In response to:

Victor Javier Martinez Hernandez

Initial Post

72 days ago

4 replies

Last 88 days ago

Almost 3 million Denial of Service (DoS) attacks were recorded in the first quarter of 2021 (Dark Reading, 2021) and even when this trend diminished in the second quarter of this year (Vigliarolo, 2021) it is expected that attacks could increase later this year. DoS attacks have been consistently increasing since they appeared in 1999 (Ostervail et al, 2019), when more than a hundred computers, infected with the script Trin00, denied the service from a computer in Minnesota University. Taking the first recorded event as an example, DoS attacks have the primary goal of disrupting normal traffic of a server, by channeling a tremendous amount of traffic to the targeted server and its adjacent infrastructure, like memory, disk space, network resources, among others.

Insufficient logging and monitoring considered one of the OWASP top 10 Web application vulnerabilities (OWASP, n.d.), could leave servers and cloud infrastructure exposed to DoS, since there is no reference for SysAdmins to acknowledge an irregular amount of traffic.

There are different kinds of DoS attacks that can be recognized depending on the vulnerability they are trying to exploit (Zlomislić et al, 2014), the one that has become the most common is the SYN flood, classified as a Flood kind, overruns the server with multiple SYN requests, the first part of the SYN-ACK handshake, as the targeted server allocates memory for the connection a considerable number of this connections can led server or router to denied valid requests or crash as it runs out of memory (Ganti, Yoachimik, 2021).

References

Dark Reading (2021) DDoS Attacks Up 31% in Q1 2021: Report. Available from: https://www.darkreading.com/attacks-breaches/ddos-attacks-up-31--in-q1-2021-report/d/d-id/1341036 [Accessed 18 August 2021]

Vigliarolo, B. (2021) DDoS attacks are down 38.8% in Q2 2021. Available from: https://www.techrepublic.com/article/ddos-attacks-are-down-38-8-in-q2-2021/ [Accessed 18 August 2021]

OWASP (n.d.) OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed 18 August 2021]

Zlomislić, V., Fertalj K. and Sruk V. (2014) Denial of service attacks: An overview. *2014 9th Iberian Conference on Information Systems and Technologies (CISTI), 2014, pp. 1-6*, doi: 10.1109/CISTI.2014.6876979.

Ganti, V. & Yoachimik, O. (2021) DDoS attack trends for 2021 Q2. Available from: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q2/ [Accessed 19 August 2021]

(1) The normal handshake from a regular user.

(2) The most common kind of attack, the SYN Flood.

Post:

Hi Victor,

You've produced a very detailed post, covering the early stages of DDoS attacks, as well as the risks these pose to the availability of a particular resource.

As mentioned by Hendrik above, it is worth noting that typical TCP-SYN flood attacks often use TCP packets with spoofed IP address headers, resulting in the non-response to the TCP-ACK message sent by the server. This causes the handshake to remain incomplete; however, the port will remain open for some time, impacting the genuine requests directed to the server (Imperva, n.d.). Therefore, a TCP-SYN attack would reside in the Transport layer (Layer 4) of the OSI model.

Over recent years, with the mass adoption of IoT technologies, DDoS attacks have become far more prevalent. Many devices are insecure and are shipped with default usernames/passwords, which, when encountered by a ‘scanner’ can be used as part of a DDoS botnet (Palmer, 2020). Access to such botnets are normally sold on a series of underground online forums, which make it easy for a novice user to conduct a vast DDoS attack on businesses.

Do you agree that the easy access and wide availability of DDoS tools are likely to contribute towards the overall number of attacks that are performed? If so, how could you see logging/monitoring tools being used to reduce the overall number/severity of attacks?

References:

Imperva. (n.d.) TCP SYN Flood. Available from: https://www.imperva.com/learn/ddos/syn-flood/ [Accessed 21st August 2021].

Palmer, D. (2020) DDoS attacks are cheaper and easier to carry out than ever before. Available from: https://www.zdnet.com/article/ddos-attacks-are-cheaper-and-easier-to-carry-out-than-ever-before/ [Accessed 21st August 2021].

Screenshot:

Post by **Kieron Holmes**
Peer Response

71 days ago

Hi Victor,

You've produced a very detailed post, covering the early stages of DDoS attacks, as well as the risks these pose to the availability of a particular resource.

As mentioned by Hendrik above, it is worth noting that typical TCP-SYN flood attacks often use TCP packets with spoofed IP address headers, resulting in the non-response to the TCP-ACK message sent by the server. This causes the handshake to remain incomplete; however, the port will remain open for some time, impacting the genuine requests directed to the server (Imperva, n.d.). Therefore, a TCP-SYN attack would reside in the Transport layer (Layer 4) of the OSI model.

Over recent years, with the mass adoption of IoT technologies, DDoS attacks have become far more prevalent. Many devices are insecure and are shipped with default usernames/passwords, which, when encountered by a 'scanner' can be used as part of a DDoS botnet (Palmer, 2020). Access to such botnets are normally sold on a series of underground online forums, which make it easy for a novice user to conduct a vast DDoS attack on businesses.

Do you agree that the easy access and wide availability of DDoS tools are likely to contribute towards the overall number of attacks that are performed? If so, how could you see logging/monitoring tools being used to reduce the overall number/severity of attacks?

References:

Imperva. (n.d.) TCP SYN Flood. Available from: **https://www.imperva.com/learn/ddos/syn-flood/** [Accessed 21st August 2021].

Palmer, D. (2020) DDoS attacks are cheaper and easier to carry out than ever before. Available from: **https://www.zdnet.com/article/ddos-attacks-are-cheaper-and-easier-to-carry-out-than-ever-before/** [Accessed 21st August 2021].