Incident Report: Ping Flood ICMP Attack 2024-05-13 #3   
Globe Sistemas - Av Libertador Jardin America

Report Overview

| **Part 1: Summary of the issue found in DNS and ICMP traffic logging.** | |
| --- | --- |
| The UDP protocol reveals that:  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  The port indicated in the error message is used for:  The most likely problem is: | |
|

| **Part 2: Explain your analysis of the data and provide at least one cause of the incident.** |
| --- |
| Time the incident occurred:  Explain how the IT team learned about the incident:  Explain the actions taken by the IT department to investigate the incident:  Note the key findings from the IT department's investigation (i.e. details related to the affected port, DNS server, etc.):  Consider a probable cause of the incident: |

| **Part 1** | | |
| --- | --- | --- |
| **Provide a summary of the issue found in the DNS and ICMP traffic log.** | | **Explanation** |
| **TO** | As part of the DNS protocol, the UDP protocol was used to contact the DNS server and retrieve the IP address of the domain name globesistemas.com.  The ICMP protocol was used to respond with an error message, indicating problems contacting the DNS server. | **Include a brief summary of the tcpdump log analysis and identify what protocols were used for the network traffic.**  The scenario summarizes the problem and identifies the protocols used.  The scenario: “ To load the web page, your browser first sends a query to a DNS server over the UDP protocol to retrieve the IP address of the website's domain name; this is part of the DNS protocol...  The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: "udp port 53 unreachable". |
| **B** | The UDP message going from your browser to the DNS server is displayed in the first two lines of each log event.  The ICMP error response from the DNS server to your browser is displayed on the third and fourth lines of each log event with the error message "udp port 53 unreachable".  Since port 53 is associated with DNS protocol traffic, we know that this is a problem with the DNS server.  Problems with the execution of the DNS protocol are even more evident because the plus sign after the query ID number 35084 indicates flags with the UDP message and the letter "A?".  The symbol indicates flags with active DNS protocol operations. | **Provide some details about what was indicated in the record.**  The first and second steps of the scenario section indicate that you performed a network analysis using tcpdump, which recorded UDP packets from your source computer to the DNS server IP address and port (203.0.113.2.domain).  It also recorded ICMP error responses from the DNS server to your computer with the error message "udp port 53 unreachable".  We mentioned in the sixth step that “ Port 53 is a port for the DNS service”, which means that this is a problem with the DNS server.  We included more signals of DNS performance issues in the fifth step of the scenario,”  The plus sign after the query ID number indicates that there are flags associated with the UDP message.  The “A?” indicates an indicator associated with the DNS request for an A record, where an A record maps a domain name to an IP address.” |
| **C** | Due to the ICMP error response message on port 53, it is very likely that the DNS server is not responding.  This assumption is further supported by the indicators associated with the outgoing UDP message and the domain name retrieval. | **Interpret the problems found in the log.**  The Scenario section (or a quick Internet search for “port 53”) will show that this port number is commonly used for DNS communications protocol.  Since port 53 is unreachable and that port is commonly used for DNS server communications, you can conclude that the DNS server is unreachable or "not responding".  This could be due, for example, to a DoS attack against the DNS server. |

| **Part 2** | | |
| --- | --- | --- |
| **Explain your analysis of the data and provide at least one cause of the incident.** | | **Explanation** |
| **TO** | The incident occurred today at 1:24 p.m. | **Please indicate when the issue was first reported.**  This information was obtained from the date and time stamps in the log file. In the log, this is the first sequence of numbers shown: 13:24:32.192571.  This shows the time 1:24 pm, 32.192571 seconds, with the time in 24-hour format.  The scenario indicates that this event occurred today. |
| **B** | Customers notified the organization that they received the message "destination port unreachable" when they tried to visit the globesistemas.com website. | **Provide the scenario, events, and symptoms identified when the event was first reported.**  The scenario states that a handful of customers contacted your company to report that they were unable to access the company's website and saw the "destination port unreachable" error after waiting for the page to load. |
| **C** | The cybersecurity team providing IT services to your client's organization is currently investigating the issue so that customers can access the website again. | **Explain the current status of the problem.**  The scenario states that “this incident, meanwhile, is being handled by security engineers after the analyst reported the issue to his supervisor.” |
| **D** | In our investigation of the issue, we performed packet sniffing tests using tcpdump.  In the resulting log file, we found that DNS port 53 was not accessible. | **Describe the information discovered while investigating the problem up to this point.**  Provide a concise summary of what you did to investigate the problem.  The scenario says: The website is visited and also the error "destination port unreachable" is received.  Next, the network analysis tool, tcpdump, is loaded and the web page is loaded again. This time, many packets are received on your network analyzer.  On the sniffer, it sends UDP packets and receives an ICMP response to return to the host.  The results contain an error message: "UDP port 53 unreachable." |
| **AND** | The next step is to identify if the DNS server is down or if the firewall is blocking traffic to port 53. | **List the next steps to troubleshoot and resolve the problem.**  The next step in troubleshooting is to determine if the DNS server is not working properly.  If the DNS server is OK, the team should check the firewall settings to see if someone changed the settings to block network traffic on port 53.  Firewalls offer the ability to block network traffic on specific ports. Port blocking can be used to stop or prevent an attack. |
| **F** | The DNS server may be down due to a successful denial of service attack or misconfiguration. | **Provide the suspected root cause of the problem.**  Previously, you have learned about several types of denial of service (DoS) attacks.  The goal of a DoS attack is to send a flood of information to a network device, such as a DNS server, to crash it or prevent it from responding to legitimate network traffic.  An attacker may have disabled the DNS server with a DoS attack.  Alternatively, someone on your team could have made a configuration change to the firewall that blocked port 53. |