# Cybersecurity Incident Report:

# Network Traffic Analysis

Jesteś analitykiem cyberbezpieczeństwa pracującym w firmie specjalizującej się w świadczeniu usług konsultantów IT. Kilku klientów skontaktowało się z Twoją firmą, aby zgłosić, że nie mogli uzyskać dostępu do witryny internetowej firmy www.yummyrecipesforme.com i zobaczyli błąd „port docelowy nieosiągalny” po odczekaniu na załadowanie strony.

W dzienniku DNS i ICMP znajdują się następujące informacje:

1. W pierwszych dwóch wierszach pliku dziennika widać początkowe żądanie wychodzące z komputera do serwera DNS z prośbą o podanie adresu IP witryny yummyrecipesforme.com. To żądanie jest wysyłane w pakiecie UDP.
2. Następnie znajdziesz znaczniki czasu wskazujące, kiedy zdarzenie miało miejsce. W dzienniku jest to pierwsza wyświetlana sekwencja liczb. Na przykład: 13:24:32.192571. Spowoduje to wyświetlenie godziny 13:24, 32,192571 sekundy.
3. Następny jest źródłowy i docelowy adres IP. W dzienniku błędów ta informacja jest wyświetlana jako: 192.51.100.15.52444 > 203.0.113.2.domena. Adres IP po lewej stronie symbolu większego niż (>) to adres źródłowy. W tym przykładzie źródłem jest adres IP komputera. Adres IP po prawej stronie symbolu większego niż (>) to docelowy adres IP. W tym przypadku jest to adres IP serwera DNS: 203.0.113.2.domena
4. Drugi i trzeci wiersz dziennika pokazują odpowiedź na początkowy pakiet żądania ICMP. W tym przypadku wiersz ICMP 203.0.113.2 jest początkiem komunikatu o błędzie wskazującego, że pakiet ICMP nie mógł zostać dostarczony do portu serwera DNS.
5. Następnie znajduje się protokół i numer portu, który pokazuje, który protokół został użyty do obsługi komunikacji i do którego portu został dostarczony. W dzienniku błędów pojawia się to jako: port udp 53 nieosiągalny. Oznacza to, że protokół UDP został użyty do zażądania rozwiązania nazwy domeny przy użyciu adresu serwera DNS przez port 53. Port 53, który jest zgodny z rozszerzeniem .domain w domenie 203.0.113.2.domain, jest dobrze znanym portem DNS praca. Słowo „nieosiągalny” w wiadomości oznacza, że ​​wiadomość nie została przekazana do serwera DNS. Twoja przeglądarka nie była w stanie uzyskać adresu IP witryny yummyrecipesforme.com, którego potrzebuje, aby uzyskać dostęp do witryny, ponieważ żadna usługa nie nasłuchiwała na odbierającym porcie DNS, jak wskazuje komunikat o błędzie ICMP „port udp 53 nieosiągalny”.
6. Pozostałe wiersze w dzienniku wskazują, że pakiety ICMP zostały wysłane jeszcze dwa razy, ale za każdym razem otrzymano ten sam błąd dostarczenia.

# Teraz, po przechwyceniu pakietów danych za pomocą narzędzia do analizy sieci, Twoim zadaniem jest określenie, na który protokół sieciowy i usługę miało wpływ to zdarzenie. Następnie będziesz musiał napisać raport uzupełniający.

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| Logi analizatora sieci wskazują że port 53 jest niedostępny podczas próby załadowania strony yummyrecipesforme.com. Port 53 jest typowo używany przez serwer DNS co wskazuje że problem polega na tym że strona nie może przetłumaczyć nazwy domeny na odpowiedni adres IP przez brak dostępu do serwera DNS. Sugeruje to że serwer DNS został zaatakowany przez złośliwego aktora. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| Problem został zgłoszony przez klientów korzystających z yummyrecipesforme.com. Nie mogli oni uzyskać dostępu do strony, podczas ładowania otrzymywali powiadomienie „destination port unreachable”. Po analizie za pomocą Tcpdump zauważono że port 53 jest niedostępny. Wskazuje to na problem z serwerem DNS do którego klienci nie mają dostępu. Przypuszczamy że błąd występuje przez niepoprawnie działający serwer DNS, albo źle skalibrowany Firewall co może sugerować na akcje intruza.   1. Pierwszym krokiem jest sprawdzenie czy serwer DNS działa, jeśli nie skontaktowałbym się z administratorem systemu czy stwierdzono atak. 2. Jeśli działa poprawnie to sugerowane jest sprawdzenie ustawień Firewalla czy blokuje port 53 |