Wykrywanie ataków sieciowych - lab 9

Created	@May 9, 2022 2:29 PM
Class	WAS

Zadanie 1

Jednym ze sposobów na zapobieganie temu zjawisku jest wdrożenie do systemu firewalli, które limitują ilość pakietów SYN przesyłanych do danego serwera. Innym sposobem jest implementacja SYN cookies. Mechanizm ten polega na odpowiednim doborze początkowych numerów sekwencyjnych ISN wysyłanych przez serwer w pakietach SYN+ACK podczas nawiązywania połączenia TCP/IP. Mechanizm uaktywnia się w momencie przepełnienia tabeli stanów pakietami SYN. Serwer zamiast ignorować kolejne próby nawiązania połączenia TCP (pakiety SYN), odpowiada klientom wysyłając pakiet SYN+ACK z odpowiednio wyliczonym ISN, nie zapisując tego faktu w przepełnionej tabeli stanów. Jeżeli serwer otrzyma pakiet ACK, szuka odpowiadającego mu połączenia w tabeli stanów. Jeżeli połączenie nie zostanie dopasowane, serwer sprawdza wiarygodność pakietu ACK na podstawie zawartego w nim numeru sekwencyjnego.

Zadanie 2

ICMP Echo (ping) wywołane na interfejsie z wyłączonym trybem nasłuchu:

```
PING 172.16.149.128 (172.16.149.128): 56 data bytes
64 bytes from 172.16.149.128: icmp_seq=0 ttl=64 time=0.540 ms
64 bytes from 172.16.149.128: icmp_seq=1 ttl=64 time=0.511 ms
64 bytes from 172.16.149.128: icmp_seq=2 ttl=64 time=0.682 ms
64 bytes from 172.16.149.128: icmp_seq=3 ttl=64 time=0.884 ms
64 bytes from 172.16.149.128: icmp_seq=4 ttl=64 time=0.692 ms
^C
--- 172.16.149.128 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.511/0.662/0.884/0.133 ms
```

Średni czas odpowiedzi wyniósł 0.662 ms.

ICMP Echo (ping) wywołane na interfejsie z włączonym trybem nasłuchu:

```
PING 172.16.149.128 (172.16.149.128): 56 data bytes
64 bytes from 172.16.149.128: icmp_seq=0 ttl=64 time=0.993 ms
64 bytes from 172.16.149.128: icmp_seq=1 ttl=64 time=0.553 ms
64 bytes from 172.16.149.128: icmp_seq=2 ttl=64 time=0.756 ms
64 bytes from 172.16.149.128: icmp_seq=3 ttl=64 time=0.521 ms
64 bytes from 172.16.149.128: icmp_seq=4 ttl=64 time=0.566 ms
^C
--- 172.16.149.128 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.521/0.678/0.993/0.178 ms
```

Średni czas odpowiedzi wyniósł 0.678 ms.

Różnica jest niewielka z przewagą dla wyłączonego trybu nasłuchu.

Zadanie 3

Tak. Wireshark wysyła zapytania dot. pakietów, jeżeli pojawi się pakiet wysłany na nieistniejący adres.

Zadanie 4

Najpopularniejszym sposobem używanym do generowania kluczy dla RansomWare obecnie jest kombinacja algorytmów AES i RSA.

W tym schemacie zarówno oprogramowanie ransomware, jak i serwer wygenerują swoją parę kluczy RSA. Klucze klienta będziemy nazywać: **Cpub.key** dla klucza publicznego klienta i **Cpriv.key** dla klucza publicznego klienta, **Spub.key** dla klucza publicznego serwera i **Spriv.key** dla klucza prywatnego serwera. Oto jak to będzie działać:
W przypadku każdej infekcji ransomware wygeneruje w locie **Cpub.key** i **Cpriv.key**, a także oprogramowanie ransomware będzie miało zakodowany na sztywno **Spub.key**. Zaszyfruje **Cpriv.key** za pomocą **Spub.key**. Rozpocznie się procedura szyfrowania plików, pliki zostaną zaszyfrowane za pomocą AES, po zakończeniu wszystkie klucze AES zostaną zaszyfrowane za pomocą **Cpub.key**.

Aby ofiara odzyskała swoje pliki, niezbędne są klucze AES. Niestety są one zaszyfrowane za pomocą **Cpub.key**, aby odszyfrować klucze AES, potrzebny jest **Cpriv.key**, niestety ponownie, **Cpriv.key** jest zaszyfrowany za pomocą **Spub.key**. Aby odszyfrować **Cpriv.key**, deszyfrator potrzebuje **Spriv.key**, a ten znajduje się tylko na serwerze