Bezpieczeństwo komputerowe - laboratorium

Analiza ruchu sieciowego

Konrad Grochowski, Piotr Kołodziejczyk

Październik 2019

1 Wstęp

Celem zadania było zbadanie ruchu sieciowego. W tym celu należało odpowiednio skonfigurować laptopa oraz udać się w miejsce publiczne i udostępnić niezabezpieczoną sieć Wi-fi. Następnie, z użyciem odpowiednich narzędzi nasłuchiwać sieć i wyciągnąć informacje m.in. o odwiedzanych przez użytkowników stronach www czy używanych protokołach.

2 Realizacja

Jako odpowiednie miejsce do realizacji zadania wybraliśmy strefę gastronomiczną w Pasażu Grunwaldzkim, uznając, że to tam znajdziemy potencjalnie najwięcej ludzi, którzy chcieliby połączyć się z siecią wi-fi. Właściwe badania przeprowadzaliśmy na sieci o nazwie "Pasaz Free Wi-Fi", aby zachęcić jak najwięcej użytkowników. Dla SSID typu losowy ciąg znaków czy nazwa urządzenia nie odnotowaliśmy ruchu - może to świadczyć, że jeśli ktoś szuka otwartej sieci, to uznaje za bezpieczniejszą taką udostępnianą przez obiekt czy restaurację.

2.1 Poszukiwane sieci

Po przełączeniu karty sieciowej w tryb monitorowania, jest ona w stanie nasłuchiwać ruchu sieciowego w otoczeniu. Na tej podstawie sporządziliśmy listę sieci, do których podjęto najwięcej prób automatycznego połączenia się przez urządzenia.

Nazwa sieci:	Liczba prób:
KFC Hotspot	1073
eduroam	925
PizzaHut Hotspot	414
McD-Hotspot	403
101	251
Pasaz Grunwaldzki free WiFi	156
FIDOM1	90
Gaestehaus-Mueller	78
julia	63
Social WiFi	46
71211213	45
HHOT	44
Darmowe_Orange_WiFi	44
wi-fi	31

2.2 Liczba połączonych klientów

Spośród testowanych nazw udostępnianych sieci, sukces w postaci liczby połączeń odniosły następujące:

Nazwa sieci:	Liczba urządzeń:
North Fish Wi-Fi	3
Pasaz Free Wi-Fi	6

Ip lokalne urządzeń w pliku `ip_lokalne`

2.3 Przeglądane strony

Przechwycone pakiety DNS (które są nieszyfrowane) pozwalają poznać domeny, z którymi łączyli się użytkownicy. Nie mniej, tylko część z nich stanowi faktycznie odwiedzane strony, pozostałe to usługi przy korzystaniu z urządzania czy działające w tle (sprawdzanie aktualizacji etc.)
Lista stron w pliku `strony_z_dns`

2.4 Protokół HTTP

W przypadku gdy dana witryna nie wykorzystuje szyfrowania (protokół http, nie https), mamy wgląd zarówno w adresy stron, które użytkownik odwiedza, jak i np. dane przesyłane w formularzach, więc i loginy i hasła. Wtedy więc nie stanowi żadnego problemu kradzież danych. Niestety dla przestępców, ale na szczęście dla użytkowników, liczba nieszyfrowanych stron wymagających podawania danych jest dziś już znikoma.
Przechwycone nieszyfrowane strony, z których potencjalnie można wykraść dane np. formularzy w pliku `podatne`$_h ttp$

2.5 Lista protokołów

`Zestawienie liczby pakietow dla każdego protokołu. (tez nie wiem czy potrzebne)`

Protokół:	Liczba pakietów:
DNS	13063
Raw	10258
TCP	6705
ESP	5976
ARP	452
TCP in ICMP	163
ICMPv6	149
http w Raw	102
MLDv2	86
DHCP options	85
ISAKMP payload	10

2.6 Mapa

`Programem geoip-lookup wyznaczyliśmy lokalizacje serwerów, z którymi łączyły się urządzenia.`

Kraj:	Liczba IP:
US, United States	90
IE, Ireland	16
PL, Poland	16
FR, France	4
EU, Europe	4
DE, Germany	4
NL, Netherlands	4
GB, United Kingdom	3
CH, Switzerland	2
AP, Asia/Pacific Region	1
JP, Japan	1
DK, Denmark	1