Wojskowa Akademia Techniczna Semestr zimowy 2016/2017

Wstęp do kryptoanalizy klucza publicznego

Projekt strony phishingowej

Grupa K5X1N1:

Mateusz Wojdat

Krzysztof Bruliński

Michał Bogdanowicz

Opis zadania:

Celem zadania jest zaimplementowanie prostej strony phishingowej, która będzie zawierała logowanie do wybranego portalu społecznościowego/portali społecznościowych/maili.

**Wymagania techniczne:**

1. **Sieć:**

* **Strona ma być dostępna w Twojej wewnętrznej sieci na komputerze**
* Strona ma być dostępna po HTTPS. Ma zawierać certyfikat [self-signed].
* Certyfikat ma wyświetlać się w przeglądarce jako zaufany.
* Strona ma być dostępna pod konkretnym adresem: w pasku przeglądarki ma wyświetlać się adres typu www.mojastrona.pl, a nie 192.168.X.X.

1. **Strona:**

* Strona ma zawierać co najmniej 1 formularz logowania.
* Strona ma przypominać wyglądem oryginalną stronę logowania do portalu lub wykorzystywać inny pomysł na przeprowadzenie ataku wykradającego dane do logowania [np. sklep internetowy wykorzystujący SSO z Facebook’a]
* Proces logowania ma wyglądać podobnie do procesu logowania na oryginalnej stronie.
* Strona ma gromadzić dane logowania ze wszystkich prób logowania [np. w bazie danych, localStorage, pliku]
* Przy implementacji staraj się wykorzystywać dobre praktyki programistyczne i bezpieczeństwa dla używanych przez Ciebie technologii :)

**Wymagania socjotechniczne:**

* Zaprojektuj scenariusz przekazania linku do Twojej strony phishingowej.
* Scenariusz ma mieć interpretację słowno-graficzną, tzn. jeśli link będziesz przekazywać w mailu, zaprojektuj wygląd maila, jego treść, formę wyświetlania linku, formę wyświetlania adresu nadawcy.

Koncepcja rozwiązania:

Zadanie można było wykonać na wiele różnych sposobów, od napisania samemu backendu serwera w dowolnym języku, poprzez znalezienie takiego kodu open-source i dodanie warstwy prezentacji wybranej strony. W naszej grupie, w myśl zasady – nie wymyślaj koła na nowo - postanowiliśmy użyc dedykowanego narzędzia Social Engineering Toolkit. SET jest standardem używanym przez pentesterów na całym świecie. Jest to open-source, napisany w pythonie.

Aby strona mogła zaistnieć w sieci potrzebny jest również serwer http. Do tego celu wybraliśmy Apache2 HTTP Server. Rozwiązanie to jest szeroko stosowane – w połowie 2015 roku było to 37% rynku. Oczywiście oprogramowanie jest open-source. Zawiera mod\_ssl, czyli interfejs do OpenSSL, co ułatwi zainstalowanie certyfikatu. W OpenSSLu wygenerujemy certyfikat self-signed.

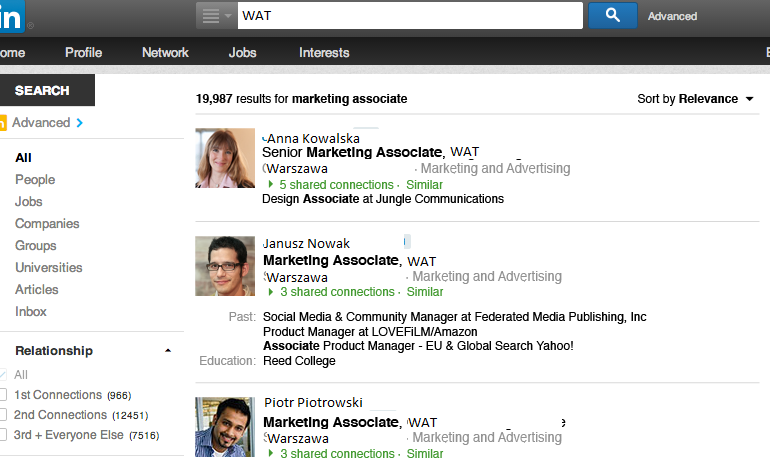
Todo – czy zaufany –

Oprócz tego użyjemy zmiany w pliku hosts, aby umożliwić przekierowanie z adresu DNS facebook.com na adres ip naszego serwera.

Scenariusz phishingowy:

W dzisiejszych czasach, przy takim natłoku infomacji, jaki można zaobserwować w mediach społecznościowych niekiedy bywa trudno odróżnić informacje prawdziwe od fałszywych. W wielu przypadkach wystarczy zapostować na jakąś facebookową grupę z jakimś „ciekawym” newsem – typu „Serialowa Kasia z „Na wspólnej” zdradza męża – ZOBACZ ZDJĘCIA”, następnie przekierowanie na naszą stronę. Dla normalnych osób może wydawać się to strasznie głupie, jednak wszystko zależy od celu ataku – lwia część ludzi jest nieświadoma takich zagrożeń.

W naszym przypadku potraktuje taki spear phishing jako element większego ataku. Powiedzmy, że dostaliśmy zlecenie aby dowiedzieć się wszystkiego na temat projektu „Bogdanov” firmy WAT. Pierwszym ruchem jaki wykonamy będzie OSINT czyli biały wywiad. Najlepiej w tym przypadku zacząć od przeszukania LinkedIn. Jest to świetna baza wiedzy.



Udało się. Mamy trafienia, a szczęście nam dopisuje, bo Anna Kowalska pracuje przy „Bogdanovie” i jest seniorem. Można teraz wpuścic nazwy użytkowników do OSRFramework, lub Maltego aby znaleźć matche w popularnych portalach. My sprawdzimy na facebooku. Znajdujemy konto należące do Anny Kowalskiej, a na nim zdjęcia – wiele zdjęć, w tym jedno z imprezy integracyjnej z kilkoma osobami, wśród nich jest Janusz Nowak, co pozwala założyć, że się znają. Miłą niespodzianką jest to, że nie posiada on tam konta. Zakładamy więc jego konto i pobieramy zdjęcie profilowe z LinkedIn. Aby konto wyglądało na bardziej legitne można dodać pare zdjęc z internetu, bazując na zainteresowaniach z LinkedIn i dodać paru znajomych z grup typu – „Dojrzałe kobiety szukają stałych związków”. Następnie wystarczy zaprosić ofiarę do znajomych. Przy odrobinie szczęscia – ofiary znają sie i lubią – dostaniemy wiadomość – „Ooo a kogo ja w końcu widze na facebooku :)))” dalej pójdzie już łatwo – ludzie raczej ufają tym których znają. Można wykorzystać zainteresowania z LinkedIn, aby podesłać linka jako – „Maltretowane psy w Rosji – podpisz petycje” (ze zdjęciem psów w klatkach) – jeśli ofiara lubi zwierzęta. Możliwości są nieograniczone. Jeśli natomiast nie dostaniemy wiadomości, zawsze możemy napisać sami – w końcu widać, że ci ludzie się znają. W takiej sytuacji po krótkiej rozmowie można podesłać „szaloną fotkę Kaśki z czwartego, tej od HR” (info z niezastąpionego LinkedIn). Ludzie nietechniczni złapią się na to. Po uzyskaniu hasła do facebooka można sprawdzić czy pasuje do innych serwisów, które znaleźliśmy na postawie username. Bardzo często zdarza się, że użytkownicy używają prywatnych kont do korespondencji służbowej. Nie inaczej było w tym przypadku – uzyskaliśmy adresy e-mail kilku współpracowników, co pozwoliło na eskalacje ataku. Na tym jednak zakończę opowieść ☺