Internet – studia podyplomowe

Cyberterroryzm

mgr Tomasz Jach

Instytut Informatyki,

Uniwersytet Śląski

Ćwiczenie 1

- Skomponuj i stwórz prawdziwy mail phishingowy.
- Za temat niech posłuży coś spersonalizowane związanego z Twoją placówką edukacyjną.
- Zadbaj o „wiarygodny” powód i skieruj użytkownika na tą stronę: http://lamp.ii.us.edu.pl/~tjach/form/
- **Po otrzymaniu zgody** od władz Twojej szkoły spróbuj przeprowadzić atak na kolegów z pracy. **Skrypt niczego nie zapisuje w bazie danych**.
- Pomyśl w jaki sposób dotrzeć do uczniów z takim przekazem.

Ćwiczenie 2

1. Przejrzyj stronę internetową szkoły pod kątem:
   1. Treści, które ładują się zbyt wolno, zbyt dużych zdjęć, itp.
   2. Treści obraźliwych lub niestosownych.
   3. Martwych odnośników.
   4. Formularzy, do których można „wstrzyknąć” złośliwy kod. Sprawdzamy to najłatwiej wpisując do pola coś takiego:
      "><h1>Test XSS</h1>
      Jeśli strona jest podatna (jak np. http://www.spskgryzliny.pl/ksiega-gosci) to wyświetli „Test XSS” bardzo dużą czcionką.
   5. Jak strona wyświetla się w różnych przeglądarkach? Możesz skorzystać ze strony http://browsershots.org/
   6. Innych nieprawidłowości (spisz je i przedyskutuj w grupie)

Ćwiczenie 3

- Czasami w celu analizy witryny internetowej należy zapisać jej stan. Proste Plik -> Zapisz jako czasami nie wystarcza.
- Skorzystaj z darmowych rozszerzeń (np. **Screenshot stron www dla Chrome)** aby zapisać stronę w całości jako jeden obrazek.
- Tenże obrazek udostępnij w internecie. Np. w serwisie http://pl.tinypic.com/
- Po wszystkim, wyczyść wszystkie prywatne dane przeglądarki (ctrl+shift+delete).

Ćwiczenie 4

- Niestety, takie czyszczenie danych **nie usuwa** śladów historii użytkownika.
- Otwórz menu start, konsolę windowsa (win+r, wpisz „cmd”) a następnie wydaj polecenie: ipconfig /displaydns > c:/dns.txt

- W pliku dns.txt na dysku C znajdą się wszystkie dotychczasowo odwiedzone witryny, **nawet te usunięte z historii przeglądarki**

Ćwiczenie 5

- Proszę zredagować tekst będący podwalinami do tzw. Polityki bezpieczeństwa i wymiany informacji drogą elektroniczną w szkole.
- Należy zadbać o:
  - Prosty język przekazu (dla laików)
  - Zadbanie o jasny i klarowny przekaz
  - Zwrócenie uwagi na najważniejsze sygnały i próby wyłudzenia informacji
  - Objęcie zakresem nie tylko maila, ale także innych form komunikacji elektronicznej (fax, telefon, itp.)
  - Jak przenosić informacje? Korzystanie z nośników niewiadomego pochodzenia.
  - Jak tworzyć dobre hasła?
  - Jak zabezpieczona jest sieć WiFi? Czy hasło jest publicznie znane? Czy sieć jest odseparowana od sieci wewnętrznej?
  - Może się przydać zrobienie testu (ang): http://www.sonicwall.com/furl/phishing/