KURSY PROGRAMOWANIA DLA DZIECI

NAZWA KURSU: Hacking i tworzenie Stron Internetowych
GRUPA DOCELOWA: Gimnazjum i Liceum (14 - 19 lat)

OPIS KURSU: Kurs obejmuje 2 semestry. Uczeń poznaje na nim tajniki hackingu, pentestingu oraz bezpiecznego korzystania z dobrodziejstw współczesnej cyfrowej cywilizacji. Zajęcia poświęcone są badaniu, używaniu oraz tworzeniu skryptów i programów hackerskich (keyloggery, trojany, wirusy, exploity). Kursant uczy się przeprowadzania oraz obrony przed atakami typu Social Enginering, DDOS, Phishing, Injections i innych. Uczeń poznaje system operacyjny Kali Linux i narzędzia przez niego udostępniane. Uczy się również korzystania z serwerów Proxy, VPN-ów, sieci Tor, w celu zachowania anonimowości w sieci Internet. Część zajęć poświęcona jest na tworzenie profesjonalnych, nowoczesnych stron internetowych, wykorzystujących języki takie jak HTML, CSS, JavaScript oraz systemy zarządzania treścią CMS. Uczeń tworzy i publikuje w sieci własny serwis internetowy.

E-MAIL: SEKRETARIAT@GIGANCIPROGRAMOWANIA.EDU.PL
WWW.GIGANCIPROGRAMOWANIA.EDU.PL
TEL: 22 112 10 63

PROGRAM KURSU:

Semestr I (15 spotkań = 30 godzin lekcyjnych):

1. Wstęp i podstawowe pojęcia związane z hackingiem. Cmd - podstawowe komendy. Pliki wsadowe bat. Wirus overload memory (aplication floader).
2. Atak typu Social Enginering. Wirus Zip Bomb. Wiping.
3. Uruchamianie wirusa w trybie invisible. Wirusy Folder Floading i File Floading.
4. Ataki typu DOS i DDOS (przeprowadzony przy pomocy cmd).
5. Atak Phishing - Aplikacja desktopowa udająca inną aplikację (na przykładzie gry Tibia). Quiz.
6. Tworzenie stron internetowych: HTML, CSS.
7. Tworzenie stron internetowych: JavaScript.
8. Język PHP. WAMP Serwer. Atak Phishing - Aplikacja Webowa udająca stronę logowania do Facebooka.
9. Anonimowość w sieci Internet. Deep Web. Proxy. VPN. Tor.
10. Kryptografia i Kryptoanaliza. Szyfry i hasze. Bezpieczeństwo haseł i sposoby ich łamania. Quiz.
11. Virtual Box. Instalacja systemu Kali Linux. Komendy Linuxa.
12. Kali Linux - Information Gathering - narzędzia służące do przeprowadzania rekonesansu.
13. Kali Linux – Password Cracking – narzędzia służące do łamania haseł.
14. Kali Linux - ataki typu DDOS przeprowadzane przy pomocy narzędzi udostępnianych przez system Kali Linux (Ettercap, Slowloris).
15. Tworzenie Keyloggera. Quiz.

Semestr II (15 spotkań = 30 godzin lekcyjnych):

1. Przypomnienie materiału z I semestru. CMS (1) - tworzenie profesjonalnej strony internetowej. Joomla!
2. CMS (2) - tworzenie profesjonalnej strony internetowej. Joomla!
3. CMS (3) - tworzenie profesjonalnej strony internetowej. Joomla! Zabezpieczanie przed atakami
4. Hosting. Domena. DNS. Publikacja strony w sieci Internet.
5. Cookies. Wykradanie ciasteczek. Quiz.
6. Kali Linux - Bezpieczeństwo haseł. Ataki słownikowe oraz z wykorzystaniem tablic tęczowych.
7. Kali Linux - Ataki typu Spoofing i Sniffing - przy pomocy narzędzi publikowanych przez system Kali Linux.
8. HTTP vs HTTPS. SSL Strip.
9. DNS Spoofing.
10. Ataki na sieci Wifi. WEP, WPA. Atak typu Twin Evil Wifi. Quiz.
11. Kali Linux - Social Enginering – narzędzia służące do ataków socjotechnicznych.
12. Web Hacking – XSS
13. Web Hacking – SQL Injection
14. Web Hacking – CSRF i File Uploader
15. Bezpieczeństwo urządzeń mobilnych. Rotowanie Androida. Przegląd narzędzi służących do hackowania w systemie Android. Quiz.

Każde zagadnienie omawiane jest poprzez wykonywanie ćwiczeń i laboratoriów lub poprzez tworzenie skryptów i aplikacji (w różnych językach programistycznych).

ZAKRES UZYSKANEJ WIEDZY:

Zakres wiedzy zdobytej przez ucznia po ukończeniu I semestru:

1. Zna podstawowe pojęcia związane z hackingiem. Potrafi posługiwać się konsolą systemu Windows i zna podstawowe komendy. Wie jak tworzyć proste skrypty i zapisywać je w postaci plików .bat. Potrafi stworzyć pierwszego wirusa.
2. Wie na czym polega atak Social Enginering i jak się przed nim ustrzec. Potrafi tworzyć pierwsze skryptowe wirusy.
3. Potrafi uruchomić dowolny program w trybie invisible. Potrafi tworzyć pierwsze wirusy w języku C#.
4. Wie na czym polegają ataki DOS i DDOS oraz potrafi przeprowadzić go przy pomocy cmd.
5. Zna sposoby Phishingu i potrafi bronić się przed tym atakiem. Potrafi stworzyć aplikację łudząco podobną do innej aplikacji i przesłać dane wprowadzone przez użytkownika na swojego maila.
6. Potrafi tworzyć statyczne strony internetowe przy pomocy języków HTML i CSS.
7. Potrafi tworzyć proste skrypty w języki Java Script i dodawać bardziej rozbudowane skrypty do swojej strony internetowej.
8. Zna podstawy języka PHP. Potrafi stworzyć stronę łudząco podobną do innej strony i zapisać np. dane logowania użytkownika.
9. Potrafi korzystać anonimowo z sieci Internet. Umie korzystać z serwerów Proxy i VPN-ów. Wie jak przeglądać i poruszać się po Deep Web.
10. Wie czym są maszyny wirtualne i potrafi zainstalować system operacyjny Kali Linux na Virtual Boxie.
11. Potrafi korzystać z systemu Kali Linux. Zna podstawowe komendy Linuxa.
12. Wie jak powinno wyglądać bezpieczne hasło, potrafi złamać proste hasła za pomocą narzędzi systemu Kali Linux.
13. Potrafi przeprowadzić podstawowy rekonesans strony internetowej za pomocą narzędzi systemu Kali Linux.
14. Umie stworzyć własnego Keyloggera w języku C#.
15. Potrafi przeprowadzić atak typu DDOS za pomocą narzędzi systemu Kali Linux.

Zakres wiedzy zdobytej przez ucznia po ukończeniu II semestru:

1. Potrafi stworzyć profesjonalną, nowoczesną, responsywną stronę internetową za pomocą CMSa (Joomla!) i wybranego szablonu.
2. Potrafi opublikować własną stronę w Internecie.
3. Wie czym są pliki Cookies i potrafi wykorzystać je do nieautoryzowanego dostępu do aplikacji Internetowych.
4. Potrafi wykorzystać narzędzia systemu Kali Linux do łamania rozbudowanych haseł.
5. Wie czym są ataki typu Spoofing i Sniffing oraz jak je przeprowadzać za pomocą narzędzi systemu Kali Linux.
6. Zna różnice pomiędzy transmisją danych za pomocą protokołów HTTP i HTTPS. Potrafi podejrzeć pakiety w transmisji HTTPS za pomocą techniki SSL Strip.
7. Wie czym jest DNS i jak przeprowadzić atak DNS Spoofing w sieci lokalnej.
8. Zna narzędzia do przeprowadzania ataków socjotechnicznych.
9. Umie przeprowadzić ataki na sieci Wifi i wie jak się przed nimi bronić.
10. Zna podstawowe podatności stron i serwisów internetowych – XSS, SQL Injection, CSRF itd.
11. Zna podstawy bezpieczeństwa urządzeń mobilnych. Potrafi zrootować telefon z systemem Android.

CENA: 35 zł za 45 minut zajęć.
Semestr składa się zwyczajowo z 15 spotkań, raz w tygodniu 2 x 45 minut. Długość semestru może się różnić w zależności od długości semestru szkolnego (przykładowo jeden semestr może trwać 14 spotkań, wtedy drugi będzie trwać 16).
Cena za semestr przy 15 spotkaniach to 1050 zł (opłata jednorazowa) lub 5 x 210 zł (opłata rozłożona na raty).

CZAS TRWANIA: Dwa semestry (30 spotkań), spotkanie raz w tygodniu, trwająca 2 x 45 minut plus 5 minut przerwy.

TERMINY KURSU:
Poniedziałek - piątek w godzinach 16.40-20.00
Soboty w godzinach 10.00-16.50

LICZBA UCZESTNIKÓW: 5- 12 Osób

E-MAIL: SEKRETARIAT@GIGANCIPROGRAMOWANIA.EDU.PL
WWW.GIGANCIPROGRAMOWANIA.EDU.PL
TEL: 22 112 10 63

giganci programowania