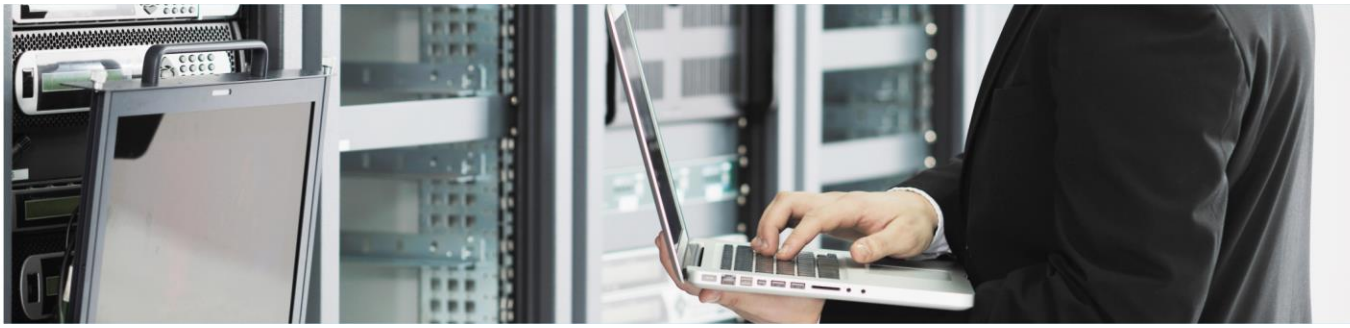

UpGreat
we know-how to do IT

AGENDA WARSZTATÓW

Testy penetracyjne
Przedsiębiorstwa komercyjne i organizacje publiczne

NR OF-12122023-1540-435.1
DATA OPRACOWANIA 12 grudnia 2023
AUTOR Piotr Flis
NADZÓR MERYTORYCZNY Jakub Staśkiewicz

UpGreat Systemy Komputerowe Sp. z o.o.
ul. Ostrobramska 22, 60-122 Poznań
NIP 779-20-28-330
REGON 631261350
KRS KRS0000179607
TEL.+48 616 641 620



Spis treści

1. Wstęp

Celem warsztatów jest przekazanie wiedzy i umiejętności w zakresie oceny bezpieczeństwa infrastruktury IT w firmach i organizacjach budżetowych. Warsztaty mogą zostać zorganizowane w siedzibie naszej firmy, w zewnętrznym ośrodku konferencyjnym lub w siedzibie Klienta. W tym ostatnim przypadku możliwa jest samodzielna ocena stanu bezpieczeństwa infrastruktury IT w przedsiębiorstwie lub w organizacji, z jednoczesnym udziałem i przeszkoleniem personelu Klienta.

1.1. Korzyści

Formuła testów penetracyjnych jako warsztatów prowadzonych z udziałem personelu Klienta gwarantuje poniższe korzyści:

- Ocena realnego stanu bezpieczeństwa infrastruktury z podsumowaniem dla kierownictwa,
- Podniesienie wiedzy i umiejętności personelu technicznego odpowiedzialnego za utrzymanie systemów,
- Możliwość ponawiania audytów bezpieczeństwa we własnym zakresie w przyszłości.

Pozostałe zalety rozwiązania:

- Warsztaty mogą odbywać się w siedzibie Klienta, przez co nie wymagają zatem delegowania pracowników i pozostawiania środowiska IT bez opieki. Formuła warsztatów umożliwia elastyczne zarządzanie czasem i w razie potrzeby obsłużenie nagłych awarii lub incydentów wymagających udziału personelu IT.
- Brak sztywnych i z góry narzuconych terminów, to my dostosujemy się do potrzeb Klienta.
- Wszystkie prezentowane na warsztatach narzędzia będą udostępnione uczestnikom wraz z materiałami szkoleniowymi. W warsztatach nie wykorzystujemy narzędzi wymagających ponoszenia jakichkolwiek dodatkowych kosztów lub zakupu licencji.
- Każdy z uczestników otrzyma na własność kartę WLAN służącą do testów penetracyjnych.
- Każdy z uczestników otrzyma na pendrive materiały szkoleniowe oraz bazy danych służące do testowania siły haseł.

2. Program warsztatów

Standardowo realizacja poniższej agendy warsztatów zajmuje 3 dni, jednak na życzenie Klienta możemy dostosować zakres tematów do aktualnych potrzeb osób szkolonych.

2.1. Moduł 0 – Wprowadzenie do testów penetracyjnych (45 min.)

W tym module zajmiemy się wyjaśnieniem podstawowych pojęć związanych z tematyką testów penetracyjnych i bezpieczeństwa. Poznamy zagadnienia takie jak Red teaming, blue teaming, white box, black box i dowiemy się co o testach penetracyjnych mówią polskie przepisy Kodeksu Karnego.

Zagadnienia:

- Terminologia,
- Przepisy prawa obowiązujące w Polsce,
- Metodyki przeprowadzania testów.

2.2. Moduł 1 – Przygotowanie środowiska testowego (45 min.)

W tym module zajmiemy się przygotowaniem i skonfigurowaniem środowiska potrzebnego w pracy pentestera. Każdy uczestnik szkolenia będzie dysponował własnym systemem oraz zestawem narzędzi. Każdy otrzyma również na własność i przygotuje do pracy kartę WIFI służącą do analizy bezpieczeństwa sieci bezprzewodowych.

Zagadnienia:

- Przygotowanie środowiska Kali Linux,
- Instalacja skanera podatności OpenVas,
- Konfiguracja i aktualizacja baz,
- Zabezpieczenie środowiska.

2.3. Moduł 2 – Rekonesans informacyjny (90 min.)

W tym module dowiemy się jakie informacje na temat naszej firmy, jej infrastruktury oraz pracowników potencjalni intruzi mogą znaleźć w Internecie. Dowiemy się też jak te informacje mogą być wykorzystane przez cyberprzestępców lub penetesterów w dalszych fazach ataku lub audytu.

Zagadnienia:

Zbieranie danych na temat firmy i jej infrastruktury

- Serwery DNS,
- Bazy RIPE,
- Nagłówki SMTP,
- Google hacking,
- Serwisy internetowe,
- Wycieki haseł.

2.4. Moduł 3 – Skanowanie i enumeracja systemów (90 min.)

Moduł, w którym przechodzimy do interakcji z testowaną infrastrukturą w celu rozpoznania stosowanych w niej systemów, urządzeń i oprogramowania. W tym module dowiemy się m.in. jak już na etapie skanowania sieci można znaleźć poważne podatności, a nawet uzyskać nieautoryzowany dostęp do urządzeń sieciowych.

Zagadnienia:

- Rozpoznawanie dostępnych usług i ich wersji,
- Wykorzystanie narzędzia nmap,
- Metody skanowania (TCP/UDP/ICMP),
- Wykorzystanie skryptów nmap,
- Wykrywanie podatności systemów na etapie skanowania.

2.5. Moduł 4 – Wyszukiwanie i analiza podatności (120 min.)

W tym module poznamy narzędzia służące do zautomatyzowanego poszukiwania podatności w systemach. Dowiemy się też w jaki sposób interpretować wyniki skanowania oraz oceniać krytyczność znalezionych podatności. Efektem naszej pracy będzie wygenerowanie raportów podsumowujących poziom bezpieczeństwa testowanego środowiska.

Zagadnienia:

- Wykorzystanie systemu OpenVas w poszukiwaniu podatności,

- Wykorzystanie systemu Sparta w poszukiwaniu błędów konfiguracyjnych,
- Ocena zagrożeń z wykorzystaniem baz CVE,
- Punktacja CVSS.

2.6. Moduł 5 – Wykorzystywanie podatności do przełamywania zabezpieczeń (120 min.)

W tym module dowiemy się co to są exploity, w jaki sposób je wyszukiwać oraz wykorzystywać do przełamywania zabezpieczeń w systemach. Poznamy też bogate środowisko Metasploit.

Zagadnienia:

- Środowisko Metasploit – warsztat pentestera,
- Konfiguracja i uruchamianie exploita,
- Przejmowanie podatnego systemu na przykładzie Windows,
- Przechwytywanie haseł, obrazu z kamery, plików oraz wejścia klawiatury,
- Eskalacja uprawnień,
- Omówienie znanych exploitów i ich wykorzystanie w praktyce.

2.7. Moduł 6 – Bezpieczeństwo WIFI i łamanie haseł (120 min.)

W tym module nauczymy się analizować bezpieczeństwo sieci WIFI oraz przechwytywać ruch, który umożliwi łamanie haseł dostępowych. Poznamy też metody łamania haseł oraz służące do tego narzędzia i słowniki. Uczestnicy otrzymają bazy danych najpopularnijszych haseł, a także bazy słownikowe służące do łamania hashy.

Zagadnienia:

- Narzędzia do analizy sieci WLAN,
- Przechwytywanie ruchu,
- Łamanie haseł WEP i WPA2,
- Narzędzia do łamania haseł,
- Metody siłowe i słownikowe,
- Przydatne bazy i serwisy do łamania haseł.

2.8. Moduł 7 – Socjotechniki i backdoory (120 min.)

W tym module dowiemy się z jakich narzędzi korzystają cyberprzestępcy w atakach socjotechnicznych i jaki skutek mogą one odnieść w testowanym środowisku. W ramach warsztatów przygotujemy m.in. własnego backdoora oraz atak phishingowy.

Zagadnienia:

- Generowanie backdoora za pomocą środowiska Metasploit,
- Metody zaciemniania i dostarczania złośliwego oprogramowania,
- Social engineering toolkit,
- BeEF (Browser Exploitation Framework).

2.9. Moduł 8 – Testy penetracyjne aplikacji webowych (120 min.)

W tym module poznamy podstawowe zagrożenia związane z serwisami www. Nauczymy się wyszukiwać i wykorzystywać podatności takie jak SQL Injections, XSS, CSRF i inne z zestawienia OWASP Top 10.

Zagadnienia:

- Struktura aplikacji webowych (frontend, backend, serwery www),
- Przypomnienie/wprowadzenie do języka SQL,
- Skanowanie podatności z wykorzystaniem narzędzi proxy,
- Ataki SQL Injection, XSS, CSRF.

3. Wymagania techniczne

Udział w warsztatach wymaga:

- Laptop lub komputer spełniający następujące wymogi:
  - wolne 2GB pamięci RAM,
  - wolne 40GB przestrzeni na dysku,
  - gigabitowa karta sieciowa,
  - system operacyjny Windows, Linux lub OS X.
- Pobranie i zainstalowanie środowiska wirtualizacji VirtualBox
  - Link -> https://www.virtualbox.org/wiki/Downloads,
- Pobranie maszyny wirtualnej z systemem Kali Linux
  - Link -> https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/,
- Dostęp do sieci gigabit LAN dla każdego z komputerów w miejscu realizacji warsztatów.

4. Wycena

Cena zależna jest od miejsca organizacji warsztatów, wielkości firmowego środowiska IT, jeśli warsztat odbywa się w siedzibie Klienta oraz od liczby uczestników.

Niezależnie od powyższego, pamiętajcie, że:

- W cenie warsztatu otrzymujecie podstawowy audyt bezpieczeństwa,
- W cenie audytu przeszkolicie siebie lub swoich pracowników,
- W cenie warsztatu otrzymacie podsumowanie stanu bezpieczeństwa swojej firmy,
- W przyszłości zaoszczędzicie na testach penetracyjnych robiąc je samemu,
- O szczegółową ofertę zapytaj korzystając z danych kontaktowych:

  - Mariusz Żytko – mariusz.zytko@upgreat.com.pl, tel. +48 601 929 592,
  - Piotr Flis – piotr.flis@upgreat.com.pl, tel. +48 605 586 588,
  - Jakub Staśkiewicz – jakub.staskiewicz@upgreat.com.pl, kuba@opensecurity.pl, tel. +48 733 296 894.

UpGreat Systemy Komputerowe Sp. z o.o.
ul.Ostrobramska 22, 60-122 Poznań
TEL.+48 616 641 620

NIP 779-20-28-330
REGON 631261350
KRS KRS0000179607