

Metody ataków na **zabezpieczenia** systemów informatycznych

Szkolenie prowadzone jest przez **Akademię Linux Magazine**, organizatora cyklu warsztatów i szkoleń poświęconych najnowszej wiedzy związanej z zagrożeniami i bezpieczeństwem systemów IT oraz tworzeniem i administrowaniem sieciami i serwerami komputerowymi.

Proponowane przez Akademię przedsięwzięcia kierowane są **głównie** do sektorów, w których poufność danych posiada najwyższy priorytet. W dzisiejszym świecie jest to kwestia bardzo istotna. Od świadomości zagrożeń i umiejętności ich niwelowania, zarówno w pracy prywatnych firm jak i instytucji użytku publicznego, zależy bezpieczeństwo każdego z nas.

Opiekę merytoryczną nad imprezami organizowanymi przez Akademię sprawuje Redakcja magazynu **Linux Magazine** – pisma będącego czołową publikacją dotyczącą Linuksa oraz szeroko rozumianego bezpieczeństwa systemów informatycznych.

Podstawowe informacje o warsztatach:

Uzyskanie nieuprawnionego dostępu do systemu czy sieci komputerowej wymaga niestandardowego i kreatywnego myślenia. Zapobieganie potencjalnym wtargnięciom we wcześniej zdefiniowany, ale mało oryginalny sposób nie zapewni przedsiębiorstwu wymaganego poziomu bezpieczeństwa, zarówno organizacyjnego jak i technicznego. **Nie jest możliwe utworzenie bezpiecznego środowiska informatycznego bez znajomości zagrożeń i schematów postępowania atakującego.**

Podczas szkolenia uczestnicy nauczą się identyfikować poszczególne zagrożenia poprzez świadome ich generowanie oraz obserwowanie efektów wykorzystania podatności wybranych zasobów. Dodatkowo uczestnicy uzyskają wiedzę pozwalającą na powzięcie odpowiedniego podejścia do zabezpieczania zasobów sieciowych oraz do planowania bezpieczeństwa wewnętrznego w przedsiębiorstwie.

Tematyka szkolenia:

- Klasyczne ataki – czyli metody wykorzystywania przepełnienia bufora, przepełnienia sterty, czy ciągów formatujących
- Automatyczne narzędzia – metody do automatycznego wyszukiwania exploitów
- Bezpieczeństwo haseł czyli jak zakodowane są hasła i jak je złamać
- Podśluchiwanie komunikacji w sieciach lokalnych
- Przejmowanie sesji oraz ataki typu Man-In-The-Middle;
- Ataki typu DOS;

Szkolenia skierowane jest do osób odpowiedzialnych za bezpieczeństwo infrastruktury informatycznej w przedsiębiorstwie: pasjonatów bezpieczeństwa, Administratorów Bezpieczeństwa Informacji, Architektów Bezpieczeństwa, administratorów IT, oficerów bezpieczeństwa, szefów działów IT; pracowników firm i instytucji posiadających rozbudowaną infrastrukturę IT – przedsiębiorstw z branży: telekomunikacyjnej, finansowej, energetycznej, przemysłu oraz instytucji administracji publicznej. Szkolenie może posłużyć Administratorom Bezpieczeństwa Informacji, jako dopełnienie wiedzy technicznej z zakresu bezpieczeństwa teleinformatycznego.

Dzięki warsztatom uczestnicy zdobędą następującą wiedzę i umiejętności:

- Dowiedzą się jak wygląda schemat postępowania atakującego, chcącego uzyskać dostęp do systemu, czy sieci komputerowej.
- Uzyskają wiedzę z zakresu wykrywania ataków – rozbudowanie świadomości bycia rozpoznawanym w sieci oraz możliwości gromadzenia informacji o sytuacji w sieci.
- Nauczą się rozpoznawać poszczególne sytuacje sieciowe na podstawie informacji przesyłanych w sieci.
- Pozyskają wiedzę z zakresu ataków komputerowych na poszczególne zasoby sieciowe i systemowe.

Wymagania względem uczestników: podstawowa znajomość usług sieciowych, podstawowa znajomość stosów protokołów rodziny TCP/IP, podstawowa znajomość aspektów bezpieczeństwa np. definicji ataków, podstawowa znajomość zagadnień bezpieczeństwa systemów operacyjnych, podstawowa znajomość programowania (język C), umiejętność pracy w środowisku tekstowym Windows i Linux.

Zajęcia będą odbywać się przy stanowiskach komputerowych w środowisku Windows XP (większość ćwiczeń) oraz Linux. Każdy z uczestników otrzyma komplet materiałów szkoleniowych zawierający m.in. płytę z zestawem narzędzi i oprogramowania.

Metody ataków na zabezpieczenia systemów informatycznych

Agenda - dzień pierwszy (23 lutego)

09:10-09:50	<i>Rejestracja</i>
09:50-10:00	<i>Powitanie</i>
10:00-10:30	Wykład wprowadzający. Omówienie podstawowych zagadnień (wykład) Uczestnicy zostaną wprowadzeni w podstawowe pojęcia z zakresu bezpieczeństwa jakie będą poruszone podczas zajęć. Dodatkowo poruszony zostanie temat socjotechniki.
10:30-11:50	Footprinting pasywny i aktywny: wyszukiwanie informacji (wykład i ćwiczenia) Uczestnicy zostaną wprowadzeni w tematykę wyszukiwania informacji na temat celu ataku bez ingerencji w strukturę i zasoby sieci atakowanego obiektu.
11:50-12:10	<i>Przerwa</i>
12:10-14:00	Skanowanie sieci i hosta (wykład i ćwiczenia) Uczestnikom zostaną przedstawione metody służące do odkrywania struktury badanej sieci oraz do pozyskiwania informacji na temat hosta – sprawdzanie otwartych portów, identyfikacja systemu operacyjnego, enumeracja użytkowników itp. Uczestnik zostanie zapoznany z budową stosu TCP/IP oraz sposobami służącymi do identyfikacji systemów operacyjnych.
14:00-14:40	<i>Obiad</i>
14:40-17:00	Ataki na systemy: klasyczne ataki przepełnienia (wykład i ćwiczenia) Tutaj przedstawione zostaną klasyczne metody związane z przepełnieniami bufora, sterty oraz wykorzystujące łańcuchy formatujące. Uczestnik w części ćwiczeniowej będzie miał możliwość samodzielnego przeprowadzenia takich ataków.
17:00-17:10	<i>Podsumowanie I dnia</i>

Agenda - dzień drugi (24 lutego)

08:55-09:00	<i>Rozpoczęcie drugiego dnia</i>
09:00-10:20	Ataki na systemy - Ataki na hasła (wykład) Przedstawione zostaną różne metody ataków na hasła. Uczestnik zostanie zapoznany z różnymi metodami kodowania haseł takich jak MD3, SHA oraz metodami ich łamania.
10:20-10:30	<i>Przerwa</i>
10:30-11:20	Ataki na systemy - Ataki na hasła (ćwiczenia) Podczas ćwiczeń uczestnik będzie mógł sam skorzystać z narzędzi w celu złamania haseł zakodowanych różnymi metodami.
11:20-12:00	Ataki na systemy: automatyczne wyszukiwanie podatności i exploitów (wykład i ćwiczenia) – Przedstawione zostaną narzędzia do automatycznego wyszukiwania podatności oraz gotowych exploitów wykorzystujących owe podatności.
12:00-12:10	<i>Przerwa</i>
12:10-13:20	Podsłuchiwanie (wykłady i ćwiczenia) – Tutaj uczestnik będzie miał okazję poznania technik służących nie tylko do samego podsłuchiwania ale także pozna ataki związane z podsłuchiowaniem – arpspoofing czy arpflooding.
13:20-13:30	<i>Przerwa</i>
13:30-14:30	Przejmowanie sesji (wykłady i ćwiczenia) – Uczestnik zostanie zapoznany z metodami stosowanymi do przejmowania sesji. Zaprezentowane zostanie wykorzystanie ataku mitm.
14:30-14:50	Ataki typu DOS (wykład) Krótki wykład prezentujący podstawowe metody służące do przeprowadzenia ataku typu (D)DOS
14:50-15:00	<i>Podsumowanie i zakończenie</i>
15:00-15:40	<i>Obiad</i>

Agenda może ulec zmianie

Dodatkowe informacje i zapisy:

W celu uzyskania dodatkowych informacji zapraszamy do odwiedzenia naszej strony internetowej. Z chęcią odpowiemy również na wszelkie pytania pod podanymi numerami kontaktowymi. Zapisów na szkolenie można dokonywać na stronie Akademii (akademia.linux-magazine.pl) lub wysyłając zgłoszenie faksem lub email'em.

Kontakt: Akademia Linux Magazine, alm@alm.org.pl, tel.: 022 742 14 57.

FORMULARZ ZGŁOSZENIOWY

Tytuł szkolenia: „Metody ataków na zabezpieczenia systemów informatycznych”
23-24 lutego 2012, Warszawa.

Imię i nazwisko:		Stanowisko:	
1			
2			
3			
Nazwa firmy:			
Adres:			
Tel.:		Faks:	
NIP:		email:	
Imię i nazwisko osoby dokonującej zgłoszenia:			
Uwagi:			
Koszt udziału w szkoleniu wynosi:		przy zgłoszeniu:	
<input type="checkbox"/>	1800 PLN + 23%VAT (2214 PLN)	do 16 lutego 2012 roku	
<input type="checkbox"/>	2100 PLN + 23%VAT (2583 PLN)	po 16 lutego 2012 roku	
Niniejszym upoważniam firmę ALM Centrum do wystawienia faktury VAT bez podpisu odbiorcy:			
		Pieczeń firmy i podpis osoby upoważnionej	

Warunkiem uczestnictwa w szkoleniu jest dokonanie wpłaty na rachunek:

37 2130 0004 2001 0491 1335 0001 (VW Bank)

Kopię dowodu wpłaty proszę przesłać faksem (na nr: 022 742 14 56) lub e-mailem (na adres: akademia@linuxmagazine.pl), w przeciągu 7 dni po jej otrzymaniu wystawimy fakturę VAT i wyślemy pocztą. Przy potwierdzeniu nadesłanym później niż 7 dni przed rozpoczęciem szkolenia, fakturę VAT otrzymają Państwo podczas spotkania.

Rezygnację z uczestnictwa należy złożyć w formie pisemnej (listem, bądź faksem):

Do 10 dni przed rozpoczęciem szkolenia uczestnicy mogą zrezygnować bez ponoszenia dodatkowych kosztów. Od 9 do 5 dni przed szkoleniem osoby rezygnujące są zobowiązane do zapłacenia 30% kosztów uczestnictwa. Od 4 dni przed rozpoczęciem szkolenia nie przyjmujemy rezygnacji. Osoby, które zarejestrują się na szkolenie i nie wezmą w nich udziału, a nie dokonają przedniej rezygnacji, zostaną obciążone pełnymi kosztami uczestnictwa.

Dane osobowe i teleadresowe:

Państwa dane zostaną umieszczone w bazie danych firmy ALM Centrum z siedzibą w Warszawie przy ulicy Mangalia 4. Zostaną one wykorzystane zgodnie z Ustawą z dnia 29.09.1997 o ochronie danych osobowych oraz odpowiednio Ustawą z dnia 18.07.2002 o świadczeniu usług drogą elektroniczną. Dane te będą służyć wyłącznie do przyjęcia i rejestracji Państwa zgłoszenia na szkolenie, a także do informowania Państwa o naszych szkoleniach i warsztatach w przyszłości. Prosimy o wyrażenie zgody na ich przetwarzanie.

Wyrażam zgodę na przetwarzanie moich danych osobowych oraz wyrażam zgodę na otrzymywanie poczty drogą elektroniczną przez ALM Centrum z siedzibą w Warszawie.

Pieczeń firmy i podpis osoby upoważnionej