ANALIZA POWŁAMANIOWA

Metody ukrywania się intruzów w systemie oraz techniki analizy skompromitowanych systemów IT

Szkolenie organizowane 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.

Zasady uczestnictwa: Szkolenie to jest organizowane zarówno jako szkolenie otwarte jak i zamknięte. Koszt szkolenia podany w załączonym na ostatniej stronie formularzu dotyczy szkolenia otwartego. W przypadku szkoleń zamkniętych koszt ustalany jest indywidualnie z zamawiającym. Minimalna liczba uczestników to 5 osób, maksymalna 12.

Szkolenie zamknięte może odbyć się we współpracującym z nami ośrodku szkoleniowym lub w siedzibie firmy klienta. Dodatkowo zależnie od potrzeb, program warsztatów może zostać dostosowany do wymagań zamawiającego.

Podstawowe informacje o szkoleniu:

Każdego dnia na portalach związanych z bezpieczeństwem **pojawia się co najmniej 15 nowych** informacji dotyczących **podatności i potencjalnych dróg ataku**. Prędzej czy później maszyny, którymi administrujemy lub które mamy pod swoją opieką mogą zostać skompromitowane i posłużyć agresorom. W najlepszym wypadku jako stacje zombie rozbudowanych botnetów, w najgorszym - musimy liczyć się z utratą poufnych informacji, problemami w świadczeniu usług oraz często z innymi, długoterminowymi stratami materialnymi.

Głównym zadaniem, a zarazem najważniejszym, w przypadku zaistnienia takiej sytuacji jest prawidłowa reakcja personelu technicznego. Niestety bardzo często się zdarza, że sam fakt udanego ataku nie zostaje prawidłowo odnotowany, nie występuje prawidłowa reakcja, lub wręcz procedury reagowania na włamania nie istnieją.

Celem szkolenia jest zapoznanie z metodami analizy po-włamaniowej. Uczestnicy będą mieli możliwość prześledzenia postępowania intruza natychmiast po włamaniu, zapoznania się z wykorzystywanymi przez niego narzędziami oraz metodami, w celu zapewnienia sobie długoterminowego oraz pełnowymiarowego dostępu do sieci i urządzeń serwerowych.

Zagadnienia poruszone podczas szkolenia:

- Specyficzne zachowania skompromitowanych systemów.
- Techniki ukrywania obecności w systemach Unix i Windows, na przykładzie Slackware i Windows 2003.
- Podstawy budowy rootkitów oraz backdorów i ich funkcjonowanie w systemach serwerowych.
- Sposoby ukrywania danych oraz metody ich ujawniania.
- Techniki wykrywania włamań.
- Wykrywanie rootkitów, backdorów, keyloggerów, koni trojańskich i innych anomalii systemowych.
- Analiza logów systemowych. Ustalenie historii wykonywanych operacji.
- Narzędzia i metody śledzenia zmian w systemie.
- Najlepsze praktyki analizy po-włamaniowej.
- Sposoby zabezpieczania dowodów elektronicznych.

Szkolenie skierowane jest: do administratorów małej i średniej wielkości sieci, a także do osób odpowiedzialnych za prawidłowe i rzetelne funkcjonowanie struktury informatycznej. Informacje przekazywane podczas szkolenia powinny szczególnie zainteresować pracowników działów IT urzędów administracji publicznej, opiekunów technicznych serwerów i stron rządowych, pracowników biur bezpieczeństwa łączności i informatyki, centrów zarządzania systemami teleinformatycznymi oraz organizacji i instytucji pokrewnych.

Najważniejsze korzyści dla uczestników, biorących udział w szkoleniu:

- Poznanie specyficznych symptomów świadczących o kompromitacji urządzeń sieciowych.
- Poznanie technik i narzędzi służących do ukrywania, wykorzystywanych przez intruzów.
- Nabycie umiejętności samodzielnego odszukiwania śladów włamań.
- Poszerzenie wiedzy dotyczącej sposobów działania intruzów oraz znajomości zagrożeń informatycznych.
- Poznanie niezbędnych narzędzi i technik, umożliwiających skuteczne wykrywanie i analizę włamań.
- Zapoznanie z metodami analizy po-włamaniowej oraz najlepszymi praktykami reagowania na incydenty.
- Poznanie podstawowych metod zabezpieczania dowodów elektronicznych.

Wymagania względem uczestników: znajomość systemu Linux oraz Windows(w tym W2k3) na poziomie swobodnego użytkowania, podstawowa znajomość protokołów sieciowych połączeniowych i bezpołączeniowych, podstawowa wiedza o programowaniu, w tym programowaniu sieciowym, minimalna teoretyczna znajomość podstawowych typów ataków.

AKADEMIA LINUX MAGAZINE

Akademia Linux Magazine™ - ALM Centrum

NIP: 813-172-60-55, REGON: 141622092-00028, ul. Mangalia 4, 02-758 Warszawa, tel.: 22 742 14 57, faks: 22 742 14 56, e-mail: alm@alm.org.pl, www: alm.org.pl

Agenda - dzień pierwszy

09:20-09:50	*Rejestracja*
09:50-10:00	*Powitanie*
10:00-11:00	**Wykład wprowadzający: Specyficzne zachowania skompromitowanych systemów** W trakcie wykładu zostaną przedstawione główne powody ataków na systemy informatyczne. Uczestnicy będą mogli poznać i doświadczyć realnego zachowania skompromitowanego systemu komputerowego, w całym przekroju reakcji po-włamaniowych.
11:00-11:10	*Przerwa*
11:10-12:30	**Wykład + ćwiczenia: Techniki ukrywania obecności w systemach Unix i Windows.** Uczestnicy zapoznają się z podstawowymi sposobami ukrywania obecności w skompromitowanych systemach. W trakcie wykładów oraz ćwiczeń zostaną przedstawione podstawowe i niezbędne narzędzia, wykorzystywane do zapewnienia ukrycia w systemie komputerowym.
12:30-12:40	*Przerwa*
12:40-14:00	**Wykład + ćwiczenia: Techniki ukrywania obecności w systemach Unix i Windows.**
14:00-14:40	*Obiad*
14:40-17:00	**Wykład + ćwiczenia: Podstawy budowy rootkitów oraz backdorów i ich funkcjonowanie w systemach serwerowych.** Uczestnicy zapoznają się z oprogramowaniem malware typu rootkit oraz backdoor. Przedstawione zostaną zagadnienia związane z ich budową oraz funkcjonowaniem w środowiskach serwerowych opartych na systemie operacyjnym z kernelem Linuksa. Uczestnicy w trakcie ćwiczeń będą starali się wykorzystać możliwości istniejących rootkitów do zapewnienia sobie ukrytej, stałej i stabilnej powłoki systemowej na prawach administracyjnych.
17:00-17:10	*Podsumowanie I dnia*

Agenda - dzień drugi

09:25-09:30	*Rozpoczęcie drugiego dnia*
09:30-11:10	**Wykład + ćwiczenia: Sposoby ukrywania danych oraz metody ich ujawniania.** W trakcie tej części zajęć uczestnicy będą mogli zapoznać się z metodami ukrywania danych w systemach oraz poznać niezbędne podstawy Computer Forensics w procesie wykrywania włamań.
11:10-11:20	*Przerwa*
11:20-12:20	**Wykład + ćwiczenia: Reagowanie na incydenty – dokumenty i procedury.** Uczestnicy zapoznają się z dokumentami normatywnymi, opisującymi międzynarodowe sposoby i procedury podejścia do zagadnień związanych z wykrywaniem włamań i reagowaniem na incydenty.
12:20-12:30	*Przerwa*
12:30-13:50	**Wykład + ćwiczenia: Reagowanie – metody i sposoby pracy analitycznej.** W trakcie tej części zajęć uczestnicy będą mogli w praktyce zapoznać się z metodami i sposobami analitycznego podejścia do problemu wykrywania włamań. Zostaną omówione i pokazane podejścia różnych członków grupy analitycznej. Przedstawiony zostanie sposób formalizowania zadań.
13:50-14:30	*Obiad*
14:30-16:30	**Wykład: Techniki wykrywania włamań. Najlepsze praktyki analizy powłamaniowej oraz sposoby zabezpieczania dowodów elektronicznych –** Ostatnie spotkanie merytoryczne w dniu drugim da możliwość zapoznania się z najlepszymi technikami wykrywania włamań, prezentowanymi w sposób praktyczny, oraz z metodologiami prowadzenia analizy.
16:30-16:30	*Podsumowanie II dnia*

Agenda - dzień trzeci

09:25-09:30	*Rozpoczęcie trzeciego dnia*
09:30-10:35	**Wykład + ćwiczenia: Narzędzia i metody śledzenia zmian w systemie.** Uczestnicy zostaną zapoznani z podstawowymi metodami wykrywania zmian w systemach komputerowych. Zostaną przedstawione podstawowe narzędzia automatyzujące proces śledzenia modyfikacji plików i folderów.
10:35-10:40	*Przerwa*
10:40-13:00	**Ćwiczenia: Wykrywanie rootkitów, backdorów, keyloggerów, koni trojańskich i innych anomalii systemowych –** W trakcie trwania tego bloku ćwiczeń Uczestnicy zapoznają się w sposób praktyczny z metodami wykrywania i izolacji aplikacji malware.
13:00-13:10	*Przerwa*
13:10-14:50	**Ćwiczenia: Analiza logów systemowych. Ustalenie historii wykonywanych operacji** Uczestnicy przeprowadzą kompleksowy audyt powłamaniowy, mający na celu odtworzenie działań intruza w systemie komputerowym.
14:50-15:00	*Podsumowanie i zakończenie szkolenia*
15:00-15:40	*Obiad*