Szkolenie: HPE
HP-UX Security I (H3541S)

Hewlett Packard Enterprise

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	6800 PLN NETTO*	5 dni
Stacjonarne	Tablet CTAB	7400 PLN NETTO*	5 dni

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00
Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

Cel szkolenia:

Kurs pozwala zapoznać się praktycznie z wieloma popularnymi narzędziami i technikami pozwalającymi zabezpieczyć systemy HP-UX.

Połowa kursu to wykład i połowa to ćwiczenia.

Po zakończeniu kursu uczestnik będzie umiał:

- Określić jakie informacje o systemie próbuje gromadzić haker, w jaki sposób monitoruje w tym celu system i jak ukrywa swoje ślady
- Ściągnąć i zainstalować łaty związane z bezpieczeństwem
- Zidentyfikować luki bezpieczeństwa w oprogramowaniu i zapobiegać przepełnieniu bufora
- Zarządzać hasłami użytkowników, włączyć starzenie haseł, zweryfikować bezpieczeństwo hasła użytkownika
- Zarządzać atrybutami bezpieczeństwa użytkowników i ich kontami
- Instalować, konfigurować i zarządzać systemem RBAC
- Konfigurować i korzystać z list ACL systemu JFS w celu zabezpieczenia plików i katalogów
- Konfigurować system HIDS pozwalający monitorować naruszenia bezpieczeństwa w systemach klienckich
- Zidentyfikować pliki i katalogi podatne na nieautoryzowany dostęp
- Zidentyfikować, konfigurować i wyłączać usługi sieciowe w celu zwiększenia bezpieczeństwa
- Instalować i konfigurować firewall IPFilter w celu blokowania lub udostępniania usług
- Udostępnić i skonfigurować system Bastille zapewniający standardowe polityki bezpieczeństwa

Słuchacze:

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Doświadczonych administratorów systemu i sieci odpowiedzialnych za bezpieczeństwo i monitorowanie systemu HP-UX

Plan szkolenia:

- Wprowadzenie
  - Zagrożenia dla bezpieczeństwa systemu komputerowego przedsiębiorstwa
  - Składowe polityki bezpieczeństwa
  - Narzędzia podnoszące bezpieczeństwo systemu HP-UX
- Ochrona kont użytkowników: hasła użytkowników
  - Budowa pliku /etc/passwd
  - Budowa pliku /etc/shadow
  - Szyfrowanie haseł
  - Zarządzanie hasłami użytkownika
  - Konfigurowanie mechanizmu shadow
  - Konfigurowanie mechanizmu starzenia się haseł
  - Łamanie haseł za pomocą programu John the Ripper
  - Uwierzytelnianie użytkowników za pomocą PAM
  - Konfigurowanie PAM za pomocą /etc/pam.conf
- Ochrona kont użytkowników: specjalne przypadki
  - Ochrona konta użytkownika: wskazówki
  - Ochrona konta administratora: wskazówki
  - Ograniczanie dostępu administratora i operatora za pomocą pliku /etc/security
  - Ograniczanie dostępu administratora i operatora za pomocą sudo
  - Ograniczanie dostępu administratora i operatora za pomocą narzędzia ograniczony SAM
  - Ograniczanie dostępu administratora i operatora za pomocą SMH
  - Konfigurowanie kont użytkowników tymczasowych
  - Konfigurowanie kont dla użytkowników pojedynczych aplikacji
  - Konfigurowanie kont dla zespołów i grup użytkowników
  - Zapobieganie istnieniu kont uśpionych
- Ochrona kont użytkowników: SMSE (Standard Mode Security Extensions)
  - Konfigurowanie SMSE
  - Korzyści stosowania SMSE
  - Znaczenie atrybutów SMSE
  - Konfigurowanie /etc/security.dsc
  - Konfigurowanie /etc/default/security
  - Konfigurowanie /etc/passwd i/etc/shadow

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Konfigurowanie /var/adm/userdb za pomocą poleceń userdbset, userdbget i userdbck
- Moduły odpowiedzialne za politykę bezpieczeństwa opartą o SMSE

- Ochrona kont użytkowników: RBAC (Role Based Access Control)
  - Cechy i zalety RBAC
  - Instalowanie systemu RBAC
  - Konfigurowanie i przydzielanie ról RBAC
  - Konfigurowanie i przydzielanie autoryzacji RBAC
  - Konfigurowanie poleceń i przywilejów RBAC
  - Weryfikowanie bazy RBAC
  - Konfigurowanie audytu RBAC
  - Wykonywanie poleceń za pomocą privrun
  - Edycja plików za pomocą privedit
- Ochrona danych za pomocą praw dostępu i list ACL (Access Control Lists) systemu JFS
  - Jak hakerzy wykorzystują nieprawidłowe prawa dostępu do plików i katalogów
  - Sprawdzenie i zmiana praw dostępu
  - Wyszukiwanie plików z nieprawidłowymi prawami dostępu
  - Definiowanie i korzystanie z bitu SUID
  - Definiowanie i korzystanie z bitu SGID
  - Definiowanie i korzystanie z bitu sticky
  - Konfigurowanie i korzystanie z list ACL systemu JFS
- Ochrona danych za pomocą swverify, md5sum i Tripwire
  - Przegląd metod sprawdzania integralności pliku
  - Sprawdzanie integralności plików wykonywalnych za pomocą swverify
  - Sprawdzanie integralności plików za pomocą md5sum
  - Sprawdzanie integralności plików za pomocą Tripwire
  - Instalowanie Tripwire
  - Tworzenie kluczy Tripwire
  - Tworzenie plików konfiguracyjnych Tripwire
  - Tworzenie plików z polityką Tripwire
  - Tworzenie bazy danych Tripwire
  - Wykonanie sprawdzenia integralności plików za pomocą Tripwire
  - Aktualizacja bazy Tripwire
  - Aktualizacja pliku z polityką Tripwire
- Ochrona danych za pomocą EVFS (Encypted Volumes and File Systems)
  - Cechy EVFS
  - Architektura EVFS

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Wolumeny EVFS
- Klucze szyfrowania, klucze użytkownika i klucze odzyskiwania
- Krok 1: Instalacja i konfigurowanie systemu EVFS
- Krok 2: Generowanie kluczy użytkownika
- Krok 3: Generowanie kluczy odzyskiwania
- Krok 4: Tworzenie wolumenów LVM lub VxVM
- Krok 5: Tworzenie plików specjalnych EVFS
- Krok 6: Tworzenie i wypełnienie obszaru EMD wolumenu
- Krok 7: Udostępnienie wolumenu EVFS
- Krok 8: Tworzenie i montowanie systemu plików
- Krok 9: Udostępnienie autostartu
- Krok 10: Przeniesienie danych do wolumenu EVFS
- Krok 11: Wykonanie kopii zapasowej konfiguracji EVFS
- Zarządzanie użytkownikami wolumenu EVFS
- Zarządzanie bazą danych kluczy EVFS
- Rozszerzanie wolumenu EVFS
- Zmniejszanie wolumenu EVFS
- Usuwanie wolumenów EVFS
- Wykonywanie kopii zapasowej wolumenów EVFS
- Ograniczenia EVFS
- Integracja EVFS i TPM/TCS

- Zabezpieczanie usług sieciowych: inetd i tcpwrapper
  - Przegląd usług uruchamianych za pomocą inetd
  - Plik konfiguracyjny inetd
  - Zabezpieczanie inetd
  - Zabezpieczanie usług wewnętrznych inetd
  - Zabezpieczanie usług RPC
  - Zabezpieczanie usług Berkeley
  - Zabezpieczanie FTP
  - Zabezpieczanie FTP w oparciu o klasy użytkowników
  - Zabezpieczanie anonimowego FTP
  - Zabezpieczanie konta gościnnego FTP
  - Inne zabezpieczenia w pliku ftpaccess
  - Zabezpieczanie pozostałych usług uruchamianych za pomocą inetd
  - Zabezpieczanie usług uruchamianych bez pośrednictwa inetd
  - Zabezpieczanie inetd za pomocą programu TCPwrapper

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Zabezpieczanie usług sieciowych: SSH
  - Luki w tradycyjnych usługach sieciowych: DNS
  - Luki w tradycyjnych usługach sieciowych: programy podsłuchujące
  - Luki w tradycyjnych usługach sieciowych: podszywanie się pod adres IP
  - Rozwiązanie: zabezpieczenie infrastruktury sieciowej
  - Rozwiązanie: korzystanie z szyfrowania z kluczem symetrycznym
  - Rozwiązanie: korzystanie z szyfrowania z kluczem publicznym
  - Rozwiązanie: korzystanie z uwierzytelniania opartego o klucz publiczny
  - Przegląd produktów HP-UX do szyfrowania i uwierzytelniania
  - Konfigurowanie szyfrowania i uwierzytelniania serwera za pomocą SSH
  - Konfigurowanie uwierzytelniania klienta/użytkownika za pomocą SSH
  - Konfigurowanie usługi Single Sign-On w SSH
  - Korzystanie z klientów uniksowych SSH
  - Korzystanie z klientów SSH w oparciu o PuTTY
- Zabezpieczanie usług sieciowych: IPFilter
  - Wprowadzanie do firewalli
  - Firewalle oparte o filtrowanie pakietów
  - Firewalle wykorzystujące translację adresów (NAT)
  - Firewall hosta a firewall brzegowy
  - Instalacja IPFilter
  - Zarządzanie regułami IPFilter
  - Definiowanie odrzucania jako domyślnej polityki
  - Zapobieganie podszywaniu się pod adresy IP i pętli zwrotnej
  - Kontrolowanie dostępu do usług UDP
  - Kontrolowanie dostępu do usług TCP
  - Kontrolowanie dostępu poprzez aktywne i pasywne FTP
  - Testowanie reguł firewalla IPFilter
  - Monitorowanie firewalla IPFilter
- Zabezpieczanie usług sieciowych: nmap
  - Wprowadzanie do skanerów sieci
  - Przegląd skanerów sieci
  - Instalacja i uruchomienie skanera Nmap
  - Instalacja i uruchomienia skanera Nessus
  - Łączenie się z serwerem Nessus
  - Wybieranie wtyczek
  - Wybieranie hostów do badania

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Rozpoczynanie badania za pomocą Nessusa
- Przeglądanie wyników badania
- Zapisywanie raportów Nessusa

- Monitorowanie działań w systemie za pomocą logów systemowych
  - Monitorowanie plików z logami
  - Monitorowanie logowań użytkowników za pomocą last, lastb i who
  - Monitorowanie procesów za pomocą ps, top i whodo
  - Monitorowanie dostępu do plików za pomocą ll, fuser i lsof
  - Monitorowanie połączeń sieciowych za pomocą netstat, idlookup i lsof
  - Monitorowanie połączeń do usług inetd
  - Monitorowanie systemu za pomocą syslogd
  - Konfigurowanie /etc/syslog.conf
  - Ukrywanie połączeń, procesów i argumentów
  - Fałszowanie wpisów w logach i znaczników czasowych
- Monitorowanie działań w systemie za pomocą audytu SMSE
  - Wprowadzenie do podsystemu audytu
  - Audyt w systemie zaufanym (Trustem System) a audyt SMSE
  - Włączanie i wyłączanie audytu
  - Sprawdzanie aktualnego stanu audytu
  - Wybieranie zdarzeń i funkcji systemowych do audytu
  - Wybieranie użytkowników do audytu
  - Przeglądanie rejestrów zdarzeń
  - Przełączanie pomiędzy rejestrami zdarzeń
  - Znaczenie przełączników AFS i FSS programu audomon
  - Nazwy rejestrów zdarzeń nadawane przez audomon
  - Konfigurowanie parametrów programu audomon
  - Dostosowywanie programu audomon do potrzeb użytkownika za pomocą skryptów
- Monitorowanie podejrzanych działań w systemie za pomocą systemu HIDS (Host Intrusion Detection System)
  - Wprowadzenie do systemu HIDS
  - Architektura HIDS
  - Instalowanie HIDS
  - Szablony HIDS i ich właściwości
  - Tworzenie grup nadzorujących HIDS
  - Tworzenie harmonogramów śledzenia HIDS
  - Tworzenie skryptów obsługujących alerty HIDS

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Przypisywanie harmonogramów śledzenia do klientów
- Monitorowanie alertów HIDS i błędów

- Monitorowanie łat bezpieczeństwa za pomocą SWA (Software Assistant)
  - Znaczenie łat bezpieczeństwa
  - Ogólne omówienie pakietu SWA
  - Biuletyny doradcze US-CERT
  - Biuletyny bezpieczeństwa HP-UX
  - Instalacja swa
  - Generowanie raportów swa
  - Przeglądanie raportów SWA
  - Wyszukiwanie łat rekomendowanych przez swa
  - Instalowanie łat rekomendowanych przez swa
  - Instalowanie innych produktów rekomendowanych przez swa
  - Wykonanie pozostałych zmian rekomendowanych przez swa
  - Generowanie raportów swa po wprowadzeniu zmian
  - Czyszczenie danych tymczasowych swa
  - Przeglądanie logów swa
  - Dostosowywanie parametrów swa
  - Zapobieganie nieautoryzowanemu dostępowi do swa i swlist
  - Zapobieganie atakom przepełnienia bufora
  - Ustawianie parametru jądra executable_stack
  - Ustawianie opcji stosu za pomocą chatr +es
- Zabezpieczania systemu HP-UX z pomocą Bastille
  - Ogólne omówienie pakietu Bastille
  - Instalacja Bastille
  - Generowanie raportu z aktualnym stanem systemu
  - Tworzenie pliku konfiguracyjnego Bastille
  - Wykonanie zmian w oparciu o własny plik konfiguracyjny Bastille
  - Wykonanie zmian w oparciu o plik konfiguracyjny dostarczany z pakietem Bastille
  - Wykonanie zmian w oparciu o plik konfiguracyjny dostarczany z pakietem Bastille podczas instalowania systemu za pomocą Ignite-UX
  - Przeglądanie logów pakietu Bastille
  - Monitorowanie zmian za pomocą bastille_drift
  - Przywrócenie konfiguracji sprzed zastosowania Bastille
- Ochrona danych za pomocą chroot(), FGP (Fine Grain Privileges) i przedziałów bezpieczeństwa (security compartments)
  - Część 1: Koncepcje

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Przegląd metod izolacji aplikacji
- Cześć 2: Implementacja chroot()
- Ograniczanie dostępu za pomocą chroot()
- Konfigurowanie aplikacji w środowisku chroot
- Część 3: Implementacja FGP
- Ograniczanie przywilejów za pomocą FGP
- Instalacja modułu FGP
- Rozpoznawane przywileje
- Zbiory przywilejów: dopuszczalne, efektywne, odziedziczone
- Definiowanie przywilejów za pomocą setfilexsec
- Definiowanie przywilejów za pomocą systemu RBAC
- Definiowanie i używanie trybu FGP TRIALMODE
- Część 4: Koncepcja przedziałów
- Ograniczanie dostępu do obiektów IPC, sieci i plików bez przedziałów
- Ograniczanie dostępu do obiektów IPC, sieci i plików z przedziałami
- Reguły dla przedziałów
- Przedział INIT
- Przypadki użycia przedziałów
- Część 5: Definiowanie przedziałów
- Planowanie struktury przedziałów
- Instalacja oprogramowania do obsługi przedziałów
- Włączanie obsługi przedziałów
- Definiowanie i modyfikowanie przedziałów
- Przeglądanie przedziałów
- Wykonywanie poleceń w przedziale bez RBAC
- Wykonywanie poleceń w przedziale z RBAC
- Wykonywanie poleceń w trybie discovery
- Usuwanie przedziałów
- Wyłączanie obsługi przedziałów
- Cześć 6: Definiowanie reguł dla przedziałów
- Reguły interfejsu sieciowego
- Reguły systemu plików
- Reguły obiektów IPC
- Reguły dla sygnałów
- Reguły ograniczania przywilejów
- Dyrektywy preprocesora

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

Dodatek:

- Zwiększenie bezpieczeństwa użytkownika i hasła za pomocą systemu zaufanego (trusted system):
  - Wprowadzanie do systemu zaufanego
  - Definiowanie polityk dla formatu hasła
  - Definiowanie polityk starzenia hasła
  - Definiowanie polityk konta użytkownika
  - Definiowanie polityk bezpieczeństwa terminala
  - Definiowanie polityk kontroli dostępu
  - Struktura katalogu /tcb

Wymagania:

- HP-UX System and Network Administration I
- HP-UX System and Network Administration II

lub

- HP-UX Administration for Experienced UNIX Administrators

lub

- Znajomość zagadnień omawianych na tych kursach

Poziom trudności

Certyfikaty:

Uczestnicy otrzymują po zakończeniu szkolenia zaświadczenie o ukończeniu autoryzowanego kursu HPE.

Prowadzący:

Autoryzowany wykładowca firmy HPE.

Informacje dodatkowe:

W przypadku wybrania opcji szkolenia wraz z tabletem CTAB Compendium CE informuje, że firma HPE

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

Polska nie udostępnia materiałów w formie elektronicznej, **a tablet przekazywany jest kurierem po zakończeniu szkoleń** prowadzonych przez HPE Polska.

Program "CTAB - materiały szkoleniowe na tablecie" jest prowadzony tylko i wyłącznie przez firmę Compendium CE, HPE Polska nie jest w żaden sposób powiązane z oferowanymi tabletami CTAB.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313