Kod szkolenia: **H3541S**

Tytuł szkolenia: **HP-UX Security I**

Dni: 5

Authorized HP Training Reseller

Opis:

Adresaci szkolenia

Doświadczeni administratorzy systemu i sieci odpowiedzialni za bezpieczeństwo i monitorowanie systemu HP-UX

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.

Główne korzyści
Po szkoleniu uczestnicy zdobędą wiedzę i umiejętności:

- 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

Wymagania

- HP-UX System and Network Administration I H3064S
- HP-UX System and Network Administration II H3065S

lub

- HP-UX Administration for Experienced UNIX Administrators H5875S

lub

- Znajomość zagadnień omawianych na tych kursach

Parametry szkolenia

5*8 godzin (5*7 godzin netto) wykładów i warsztatów.

Wielkość grupy: maks. 8-10 osób.

Program szkolenia:

- Wprowadzenie: Zagrożenia dla bezpieczeństwa systemu komputerowego przedsiębiorstwa, Składowe polityki bezpieczeństwa, Narzędzia podnoszące bezpieczeństwo systemu HP-UX
- Ochrona kont użytkowników: specjalne przypadki
- Ochrona danych za pomocą praw dostępu i list ACL (Access Control Lists) systemu JFS
- Ochrona danych za pomocą EVFS (Encypted Volumes and File Systems)
- Zabezpieczanie usług sieciowych: SSH
- Zabezpieczanie usług sieciowych: nmap
- Monitorowanie podejrzanych działań w systemie za pomocą systemu HIDS (Host Intrusion Detection System)
- Zabezpieczania systemu HP-UX z pomocą Bastille
- Dodatek: Zwiększenie bezpieczeństwa użytkownika i hasła za pomocą systemu zaufanego (trusted system)
- Ochrona kont użytkowników: hasła użytkowników
- Ochrona kont użytkowników: RBAC (Role Based Access Control)
- Ochrona danych za pomocą swverify, md5sum i Tripwire
- Zabezpieczanie usług sieciowych: inetd i tcpwrapper
- Zabezpieczanie usług sieciowych: IPFilter
- Monitorowanie działań w systemie za pomocą audytu SMSE

- Monitorowanie łat bezpieczeństwa za pomocą SWA (Software Assistant)
- Ochrona danych za pomocą chroot(), FGP (Fine Grain Privileges) i przedziałów bezpieczeństwa (security compartments)