Techniki Hackingu i Cyberprzestępczości

Atak i Obrona systemów IT

Agenda:

- Nmap NSE Hardening
- Systemy do analizy słabości serwisów sieciowych
- Enumeracja i audytowanie ustawień systemu Linux
- Enumeracja i audytowanie ustawień systemu Windows
- Systemy automatyzujące testy bezpieczeństwa
- Haki na przeglądarkę użytkownika
- Hakowanie Wordpressa
- Hakowanie Joomli
- Hakowanie baz danych MySQL
- Ruby Code Execution
- Hakowanie serwera Tomcat
- Kradzież tokenów autoryzacyjnych
- Hacking Apache Struts - Remote Command Execution
- Hacking Apache Axis2
- Hacking Remote Services - SSH, FTP, SNMP
- Metody „odgadywania” haseł zaszyfrowanych plików
- Hacking Elasticsearch
- Hacking and Discover User Account
- Atakowanie Windows Remote Management
- Hakowanie serwera Jenkins
- Hacking Oracle GlassFish - Code Execution
- Zaawansowany Port Knocking jako zabezpieczenie przed exploitami i 0day
- Budowa i konfiguracja podwójnej autoryzacji
- Scenariusz ataku na system informatyczny - 1
- Scenariusz ataku na system informatyczny - 2

- **Wyzwanie !!!**

FOR SEC
Forensics&Security