SEGURANÇA NAS REDES E ADMINISTRAÇÃO DE SISTEMAS

Pós-Graduação em Cibersegurança e Informática Forense

Código: 124020

Área Cientifica Predominante: Arquitetura de Computadores, Sistemas Distribuidos e Cibersegurança

Docente: Nuno Alberto Ferreira Lopes

Idioma de Instrução: Português

Regime: S2

Carga Letiva: 30h Carga Trabalho: 50h

ECTS: 3,0

Objetivos

Esta unidade curricular tem como principal objectivo familiarizar os alunos das ferramentas que existem de modo a conseguir-se assegurar os sistemas e evitar ataques/mitigá-los o mais rapidamente possível.

A demonstração pratica dos conceitos utilizará o sistema operativo Linux.

Resultados da Aprendizagem

Os alunos que concluam com sucesso esta unidade curricular deverão ser capazes de:

Instalar e utilizar máquinas virtuais para executar vários sistemas
Saber como funcionam as permissões em linux
Cuidado a ter com passwords e o que se pode fazer para as melhorar, bem como verificar como se pode subir privilégios, em sistemas operativos windows, usando a ferramenta mimikatz
Utilizar aplicações para prevenir intrusões nos sistemas, e verificar a sua integridade
A importância da monitorização e dos backups, bem como instalar e configurar os mesmos

Conteúdos Programáticos

Assegurar um Sistema operativo

Instalação de um sistema operativo CentOS

Atualizar um Sistema Operativo e ferramentas

Permissões

Métodos de autenticação

Firewall (breve descrição do firewalld)

Logging

Monitorização

Configuração de snmp

Instalação de um servidor de monitorização

Plugins de monitorização

Backups

Instalação de um servidor de backups

Segurança em Serviços

Instalação de servidores web

Instalação de servidores de base de dados

Verificadores de Integridade do sistema

Bibliografia Recomendada

https://www.zabbix.com/documentation/1.8/manual/quickstart

https://icinga.com/docs/icinga-2/latest/

https://icinga.com/docs/icinga-director/latest/doc/02-Installation/

https://www.fail2ban.org/wiki/index.php/Main_Page

http://rkhunter.sourceforge.net/

https://github.com/gentilkiwi/mimikatz/wiki

Métodos de Ensino e de Aprendizagem

Os conteúdos programáticos desta UC abordam os principais conceitos na área de segurança de sistemas operativos linux.

Estes conceitos permitem a compreensão das principais característicasde funcionamento dos sistemas, de modo a poderem ser usados mais eficazmente, que são os objectivos da UC.

Métodos de Avaliação

Avaliação Contínua:

Participação na aula (15%)

Trabalho Prático (85%)

Avaliação Recurso e Especial:

Teste escrito (100%)