LEI: Segurança Informática e nas Organizações 2019-2020

Projeto 1: Exploração de Vulnerabilidades

Entrega: 18 de Outubro, 23:59

Objetivos

- Determinação de vulnerabilidades existentes
- Determinação do risco e impacto
- Exploração de vulnerabilidades

1 Descrição

Este trabalho visa explorar os conceitos relacionados com o risco de sistemas informáticos, em particular quando vulneráveis a ataques por adversários remotos, e considerando tecnologias Web.

Pretende-se que os alunos explorem os CVE existentes num sistema informático que disponibiliza uma página de uma pequena loja. Tanto a página, como os restantes sistemas possuem várias e variadas vulnerabilidades, com dificuldades e impactos também eles variados.

A página em sí é vulnerável a diversas vulnerabilidades, a que se acrescentam várias outras vulnerabilidades diretas sobre o software instalado.

2 Preparação

Obtenha a imagem de máquina virtual que se encontra na página da disciplina, para a realização deste trabalho. Crie uma máquina virtual usando a aplicação virtualbox e adicione a imagem como um disco.

Crie um interface para a máquina, podendo este ser do tipo `Bridge` ou `HostOnly`. O sistema deverá adquirir um endereço IP automaticamente. **NÃO** utilize uma rede `NAT`.

Inicie a imagem, espere alguns instantes e deverá obter a informação do endereço IP utilizado. Caso tenha escolhido a opção `HostOnly`, o endereço tipicamente será do estilo `192.168.56.1xx`.

Aceda à página web da máquina virtual, devendo obter uma página simples de uma loja.

3 Trabalho a realizar

O objetivo do trabalho é construir um relatório que descreva uma análise à segurança da máquina virtual. Pretende-se que a análise consista numa discussão de cada ponto. Caso se demonstrem exploração de vulnerabilidades, a exploração deve ser ela demonstrada de forma detalhada.

Os alunos deverão interagir com a máquina apenas através do interface de rede, não devendo considerar o acesso físíco à VM. Poderão utilizar ferramentas para determinar a existência de ataques, mas também deverão desenvolver pequenos scripts que explorem as mesmas.

Tarefas propostas:

1. Enumere os portos abertos, descrevendo a sua funcionalidade.
2. Enumere o sistema operativo e aplicações disponíveis na máquina, incluindo versões de aplicações. Descreva a função de cada aplicação e valide que se encontram em operação.
3. Enumere e descreva potenciais vulnerabilidades encontradas nos serviços, com nível superior a 7 (`http://cvedetails.com`). Consegue validar a existência de alguma vulnerabilidade?
4. Analise a página web e descreva potenciais vulnerabilidades encontradas. Existe um leque variado, relacionadas com validações de entrada, autorizações, más configurações, más práticas.
5. Explore as vulnerabilidades encontradas, descrevendo cada passo tomado, a razão dela existir e qual o potencial impacto.
6. Crie uma ferramenta (script python) para automatizar os passos que levam à exploração da vulnerabilidade mais grave que encontrar.

4 Ferramentas úteis

As seguintes ferramentas poderão facilitar a realização das tarefas em causa. De notar que a máquina virtual poderá ter algumas proteções, que se ativam se estas ferramentas forem detetadas.

- `nmap`: permite enumerar portos abertos e determinar os serviços em execução. Através de scripts, incluídos no próprio programa, é possível enumerar CVEs existentes (ex, nmap-vulners,vulscan).
- `john the ripper` e `hashcat`: permitem realizar ataques por força bruta a credenciais armazenadas.
- `nikto2`: permite analisar páginas web, determinando a existência de potenciais problemas.
- `sqlmap`: permite pesquisar páginas web por ataques do tipo injeção de SQL.
- `hydra`: permite realizar ataques por força bruta a servidores SSH.
- `metasploit`: permite realizar uma panóplia de ataques.

5 Notas

Considera-se que os trabalhos são realizados por 2 alunos e que o documento final submetido é de sua autoria. A utilização de recursos existentes na Internet ou partilhado com outros colegas leva à anulação imediata do trabalho.