
UNAERP
Universidade de Ribeirão Preto
Campus Ribeirão Preto · Campus Guarujá

Segurança da Informação

Tópicos Especiais em Engenharia

Maior Dúvida

- ✘ Se o antivírus não tem uma assinatura, ele deixa o vírus passar?
- ✘ Sobre violação, as empresas devem deixar público sobre o fato ocorrido e isso acaba manchando a reputação da mesma, e nesse caso não deixar público seria melhor para elas. O que é feito para fiscalizar e garantir que essas empresas sejam transparentes perante à esse tipo de ocorrência?
- ✘ É possível um malware permanecer mesmo depois de feito a total formatação do sistema?
- ✘ Antivírus para dispositivos móveis é realmente eficiente e necessário igual ocorre com os computadores pessoais?
- ✘ Eu baixei um arquivo do site do próprio fabricante meu antivirus barrou ele, como eu sei se realmente é um virus ou um falso positivo

Maior Dúvida

- ✘ Qual o nível se segurança dos Apps das lojas de aplicativos?(Apple Store, Google Play .. etc).
- ✘ Qual seria a melhor forma ou a mais utilizada pra garantir/monitorar usuários "comuns" de uma empresa se estão cumprindo os requisitos mínimos de segurança de informação?
- ✘ Em relação aos anti-malwares/anti-virus existe algum melhor que os outros? Como saber qual o melhor para eu utilizar?
- ✘ Como os rootkits conseguem interceptar os dados requisitados, deixando apenas "passar" os dados não infectados, para que os antivirus não consigam detectar alguma ameaça ou arquivo malicioso?

Ethical Hacking

Hacker ético

Ethical Hacker

- ✘ Profissional de SegInfo qualificado que trabalha dentro das leis
- ✘ Encontrar e explorar vulnerabilidades em vários softwares da mesma forma que um Hacker mal intencionado
- ✘ Ethical Hacker usa suas *skills* de maneira correta e legal para tentar encontrar vulnerabilidades e corrigi-las antes que pessoas mal intencionadas possam aproveitar dessas falhas para realizar um ataque
- ✘ Kali Linux – Distribuição Linux

Regras Ethical Hacker

- ✘ Respeitar a privacidade das pessoas
- ✘ Permissão para investigar o sistema ou a rede
- ✘ Informar o desenvolvedor quaisquer vulnerabilidades de segurança


PenTest
Teste de Intrusão / Penetração

Fases de um Pentest

- ✘ Etapa 0 : Negociação
- ✘ Etapa 1 : Levantamento de dados (FootPrinting)
- ✘ Etapa 2 : Varredura
- ✘ Etapa 3 : Ganhando Acesso
- ✘ Etapa 4 : Mantendo Acesso
- ✘ Etapa 5 : Limpando Rastros
- ✘ Etapa 6 : Escrita de Relatórios

Etapa 0: Negociação / Projeção

- ✘ Projeção ou um contrato inicial do Teste de Invasão
  - Mapa Mental
  - Softwares de diagramação
    - Visio
    - Enterprise Architect
    - Diagrams.net

Etapa 1: Identificação ou Coleta de Dados

- ✘ Fontes que possam trazer informações sobre a empresa
  - softwares
  - sites
  - pessoas
  - livros
  - jornais

Ferramentas para Coleta de Dados

- ✘ Maltego: Software da Paterva instalado no Kali Linux que coleta os dados de um alvo e monta um diagrama de relações e informações importantes sobre o alvo.
- ✘ Spokeo.com: faz pesquisa na web e procura informações sobre pessoas.
- ✘ AnyWho.com: pesquisa sobre pessoas.
- ✘ Google Maps: utilizado para ver estruturas e endereços.
- ✘ Yasni.com: pesquisa sobre pessoas.
- ✘ Lista Telefônica: Obtenção sobre telefones não listados na web
- ✘ Jornais: Notícias, Escândalos, Nomes de Pessoas e Anúncios do Alvo
- ✘ Livros: Biografias de Líderes e informações que possam ajudar ataques

Etapa 2: Varredura

- Softwares/sites que fazem varreduras buscando por vulnerabilidades:
  - nmap
  - nslookup
  - Nessus
  - ping
  - nbtsat
  - macof
  - netdiscover
  - smbclient
  - SuperScan
  - Pstools
  - nikto
  - owasp-zap
  - Sqlmap
  - Google Hacking

Etapa 3: Ganho de Acesso

- ✘ Softwares/sites que explorem as vulnerabilidades encontradas
  - sqlmap
  - SET – Social Engineering Toolkit
  - OphCrack
  - netcat (nc)
  - Armitage
  - AirCrack
  - Metasploit
  - Beef XSS

Etapa 4: Mantendo acesso

- ✘ Softwares que encontrem falhas para manter acesso no alvo
  - Trojans
  - Backdoors
  - Shell Reverso
  - KeyLogger

Etapa 5: Limpando Rastros

- ✘ Softwares que eliminem rastros de um ataque
  - Tor Browser
  - Proxychains
  - Wipe
  - Scrub
  - Steghide
  - Limpeza de Logs de Firewall e IDS/IPS
  - Criptografia de Dados

Etapa 6: Relatórios

- ✘ Softwares para elaborar relatório final sobre o pentest
  - Vi, Vim, Nano, Gedit, Word.
  - Nessus
  - Owasp-zap
  - Hacker Ético coloca as soluções das vulnerabilidades encontradas e exploradas no relatório e como prevenir futuras invasões

DÚVIDAS?

- ✘ Não esqueça de enviar sua maior dúvida pelo link que está no ClassRoom.
- ✘ Críticas/Sugestões: ezarpelao@unaerp.br
- ✘ Próxima aula: Ataques

Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Photographs by Unsplash