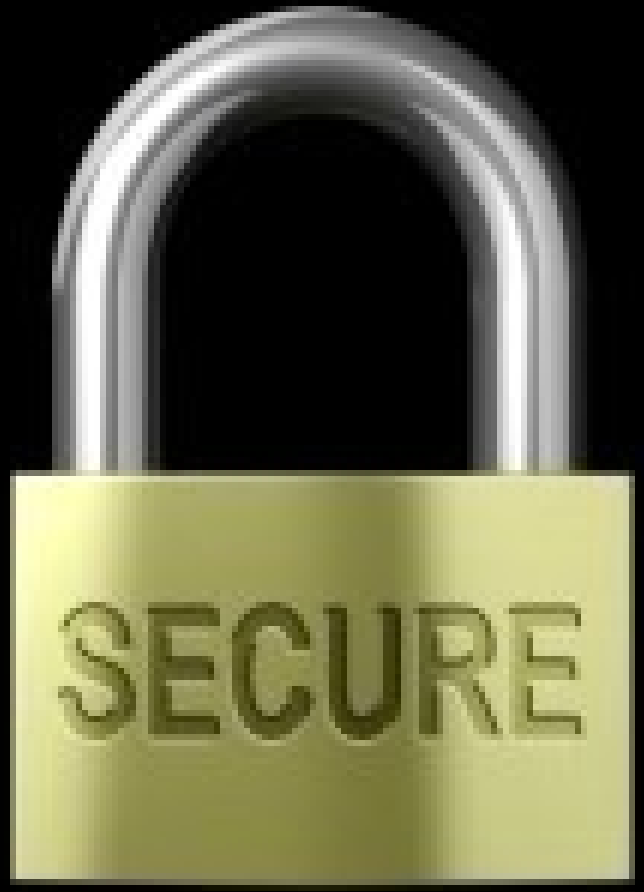
Ethical Hacking
Conceitos básicos de Testes de penetração



Cleórbete Santos - www.cleorbete.com

Quem sou eu?

- Analista de Sistemas formado no Instituto Federal do Tocantins;
- Pós-graduado em Segurança da Informação pela União Latino-americana de Tecnologia;
- Acadêmico de Direito na Universidade Federal do Tocantins;
- Capacitado por instituições nacionais e internacionais como a Universidade de São Paulo, Fundação Getúlio Vargas e DoD – US Department of Defense;
- Instrutor na modalidade presencial e à distância de cursos de Direito, Java, Grails e Ethical Hacking;
- Instrutor do curso de Segurança da Informação da ESMAT - Escola Superior da Magistratura Tocantinense;
- Ex-membro da equipe de desenvolvimento do PJe – Processo Judicial Eletrônico do Tribunal Superior Eleitoral;
- Autor do livro “Muito além do antivírus”;
- Servidor do quadro de Tecnologia da Informação da Justiça Eleitoral;
- Palestrante;
- Instrutor internacional (em andamento...);

PARTE I

TEORIA

O que é Segurança da Informação?

Normas de SI

- PCI DSS - Payment Card Industry Data Security Standard
- HIPAA - Health Insurance Portability and Accountability Act
- SOX - Sarbanes Oxley
- NIST - National Institute of Standards and Technology
- ISO 27000 Series
- Lei Carolina Dieckmann
- Marco Civil da Internet

Princípios básicos de SI

- Confidencialidade
- Integridade
- Disponibilidade

Conceitos básicos de SI

- Ativo
- Ameaça
- Vulnerabilidade
- Risco
- Contramedida

Hackers (espécies)

- White hats (Ethical hackers)
- Black hats (Crackers)
- Grey hats

Pentest

Pentest ou Penetration Testing é a simulação de ataques reais para a identificação de riscos associados a potenciais brechas de segurança (vulnerabilidades). Obs.: Os pentesters não somente descobrem vulnerabilidades, mas as exploram, para identificar quais ganhos seriam atingidos por potenciais atacantes em caso de sucesso na invasão.

O que faz um pentester?

Descobre vulnerabilidades relativas a:

- Zero-day
- Injection
- Engenharia Social
- Senhas vazadas/quebradas
- Defacing
- MitM
- Etc

Alguns tipos de Pentests:

- Interno (Ex.: Insider)
- Externo (Ex.: Via Web)
- Controle de segurança física
- Segurança de redes sem fio
- Engenharia Social
- Etc

Fases de um Pentest:

- Pré-compromisso (Pre-engagement);
- Levantamento de informações (Information/Intelligence gathering);
- Modelagem de ameaças (Threat modeling);
- Análise de vulnerabilidades (Vulnerability analysis);
- Exploração (Exploitation);
- Pós-exploração (Post exploitation);
- Geração do(s) relatório(s) (Reporting);

Site: http://www.pentest-standard.org/index.php/Main_Page

Fase de Pré-compromisso (Pre-engagement):

- Acontece antes do teste;
- Serve para alinhar o pensamento do pentester com o cliente;
- É o momento onde todas as perguntas pertinentes devem ser feitas;

Itens da fase de Pré-compromisso:

- Definição do escopo;
- Quando será a janela para o teste;
- Quem deverá ser o contato do pentester na empresa;
- Emissão do contrato (permissão para o teste);
- Definição do preço a ser pago;

Obs.: Incluir no contrato uma cláusula de confidencialidade;

Fase de Levantamento de informações:

É a obtenção de informações dos alvos definidos no escopo por meio de técnicas e ferramentas (port scan, por exemplo);

Fase de Modelagem de ameaças:

É o momento onde o pentester pensará como um atacante e definirá estratégias de invasão aos alvos definidos no escopo utilizando as informações obtidas na fase de Levantamento de informações;

Fase de Análise de vulnerabilidades:

É o momento no qual o pentester utilizará técnicas e ferramentas para descobrir as brechas de segurança nos alvos definidos no escopo do teste;

Fase de Exploração:

É o ataque propriamente dito, onde o pentester invadirá os alvos usando técnicas e ferramentas específicas para tal (metasploit, por exemplo);

Fase de Pós-exploração:

É onde o pentester definirá, a partir dos alvos invadidos com sucesso, o que é impactante para o cliente;

Fase de Geração do(s) relatório(s):

É a última fase de um teste de penetração, muito embora tão importante quanto as demais, pois é onde o pentester traduzirá o que aconteceu nas fases anteriores em texto inteligível para seu cliente (seja do setor técnico ou não). Por ser (ou dever ser) dividido em dois tipos: Executivo e Técnico.

PARTE II

PRÁTICA

Criando o laboratório

VMWare Player: http://www.vmware.com/products/player/ (ou Virtualbox, etc)

Kali Linux 1.0.6: http://www.kali.org/downloads/

Máquinas virtuais de S.O.'s diversos

[FASE DE] Levantamento de informações

OSINT - Opensource Intelligence
- Netcraft (www.netcraft.com)
- BuildWith (www.builtwith.com)
- Comando whois
- Comando nslookup
- Comando host
  - host -t ns zoneedit.com
- theHarvester
  - theharvester -d <site> -l 500 -b all
- Google Dorks (www.exploit-db.com/google-dorks/)

Maltego (www.paterva.com)

[FASE DE] Levantamento de informações

Port Scannning manual (nc)

nc -vv <ip> <porta>

Port Scanning com nmap

nmap -sS <ip_inicial>-<ip_final> -oA <arquivo> //Syn, Syn-Ack sem Ack [TCP]

nmap -sV <ip_inicial>-<ip_final> -oA <arquivo> //Versão (com Ack) [TCP]

nmap -sU <ip_inicial>-<ip_final> -oA <arquivo> // [UDP]

nmap -sS -p <porta> <ip> //Porta específica

[FASE DE] Modelagem de ameaças

1. Levantar informações sobre as ameaças;
2. Identificar e categorizar os ativos;
3. Identificar e categorizar as ameaças;
4. Mapear ameaças x ativos;

[FASE DE] Análise de vulnerabilidades

- Nessus (www.tenable.com)
  /etc/init.d/nessusd
  https://localhost:8834/
  Policies / Basic Network Scan
- NSE - Nmap Script Engine
  cd /usr/share/nmap/scripts
  nmap -sC <ip_inicial>-<ip_final> //Default script
  nmap --script-help nfs-ls
  nmap --script=nfs-ls <ip> //Monta compartilhamentos e exibe permissões
- Sites de exploits
  www.securityfocus.com
  www.packetstormsecurity.org
  www.exploit-db.org
  www.cve.mitre.org

Metasploit Framework

É um framework de análise e exploração de vulnerabilidades atualmente pertencente à Rapid7 (www.rapid7.com). O metasploit possui um repositório de exploits que é atualizado por hackers do mundo inteiro, facilitando a vida de pentesters (e de black hats...).

Encontrando um módulo do metasploit para uma vulnerabilidade encontrada

http://www.rapid7.com/db/modules/

msf > search <aplicação>

Metasploit Framework (Uso)

/etc/init.d/postgresql start
/etc/init.d/metasploit start
msfconsole
use <caminho/do/exploit>
show options
set <opções>
check/exploit/run

[FASE DE] Análise de vulnerabilidades [CONTINUAÇÃO]

Metasploit Check Function

```
msf > use windows/smb/ms08_067_netapi
set RHOST <ip>
check
```

Obs.: Para atualizar a base de dados do Metasploit, use o comando "msfupdate".

[FASE DE] Análise de vulnerabilidades [CONTINUAÇÃO]

- DVWA - Damn Vulnerable Web Application
- Nikto

  nikto -h <ip/url>

[FASE DE] Exploração

http://www.rapid7.com/db/modules/

http://www.rapid7.com/db/modules/exploit/windows/smb/ms0

http://www.rapid7.com/db/modules/exploit/windows/ftp/warftp

Meterpreter

Meterpreter é um payload disponível no Metasploit que utiliza a técnica de Reflective DLL Injection, que permite sua instanciação apenas na memória do servidor, evitando a criação de um novo processo que poderia ser detectado por IPS's e IDS's presentes;

Obs.: Payload é o código que executará ações após a exploração de uma vulnerabilidade.

Invadindo um alvo

```
msfconsole
use <caminho/do/exploit>
show options
set <opções>
exploit
```

Engenharia social

Redes sociais
Phishing, Spear phishing
Spam, hoax
Romance scan
Telefone
Dumpster diving
Shoulder surfing
Conversação

Engenharia social

SET - setoolkit

Injection

sqlmap --url <site><pagina>.php?id=1 -b

sqlmap --url <site><pagina>.php?id=1 –current-db

sqlmap --url <site><pagina>.php?id=1 -dbs

sqlmap --url <site><pagina>.php?id=1 -D <banco> --tables

[FASE DE] Pós-exploração

Quebrando senhas

- Comando hashdump do meterpreter
- John The Ripper
- Rainbow tables
- Cloud Cracker (www.cloudcracker.com)

[FASE DE] Geração do(s) relatório(s)

- Executivo
- Técnico

OBRIGADO...

Cleórbete Santos
www.cleorbete.com
facebook.com/cleorbete