Arquitetura e Organização de Sistemas Computadorizados - Teste de Invasão

Osmar de Oliveira Braz Junior

Márcia Cargnin Martins Giraldi

Objetivos

- Apresentar os testes de invasão e os atores e tecnologias envolvidas.

Cybercrime

- A cada minuto mais de 60 pessoas no Brasil e 1.000 no mundo foram vítimas de algum tipo de cybercrime;
- Por dia mais de 90.000 brasileiros são vítimas dos cybercriminosos.
- No mundo são 1.500.000 de vítimas.

Cybercrime

- Grupos são criados em todo o mundo para estudarem novas formas de ataque.
- O Brasil é um dos líderes ranking mundial de hackers e crimes virtuais.

Cybercrime

- **China e Brasil são as maiores vítimas do cybercrime no mundo !**

  - Pesquisas mostram que a maioria dos entrevistados não acredita que os criminosos possam ser julgados

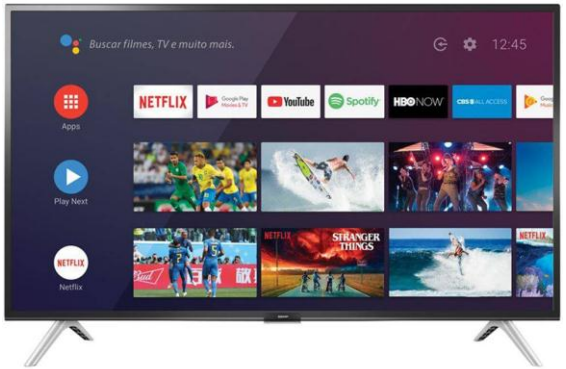
Cybercrime

- **Mundialmente, o custo dos crimes na web é calculado em US$ 200 bilhões/ano.**

- **Cerca de 50 milhões de brasileiros foram vítimas dos crimes na Internet, resultando um prejuízo financeiro de mais de R$ 20 bilhões.**

Fonte: Convergência Digital

Dispositivos Perturbadores Que Comprovadamente Espionam Você!



https://www.youtube.com/watch?v=67fZVsHomr0

Vulnerabilidade - Invasão

Hacker x Cracker

- Perito em informática que explora as fragilidades do sistema.

Classificação

- Classificação conforme a sua intenção: hats

Testes de Invasão

Testes de Invasão ou Pentest

- Sistemas podem apresentar falhas
- Esse tipo de teste é realizado para identificar vulnerabilidades através de diversas técnicas e explorá-las com o objetivo de ganhar acessos não autorizados simulando o que atacantes fariam
- É possível avaliar o que um atacante conseguiria realizar ao conseguir explorar uma falha
- **Pentest** = *Penetration Test*

Testes de invasão ou Pentest

- Simulação de ataques reais para avaliar os riscos associados e as potenciais falhas de segurança nos sistemas corporativos
- Testes metodológicos com o objetivo de expor as possíveis vulnerabilidades em redes e sistemas operacionais
- Pode ser estendida para websites, redes sem fio, banco de dados, aplicativos e programas

Testes de Invasão ou Pentest

- tem as seguintes sete fases: preparação, coleta de informações, modelagem das ameaças, análise de vulnerabilidade, exploração de falhas, pós-exploração de falhas, documentação

Testes de Invasão - Preparação

- Interação com o cliente
- Escopo:
  - quais endereços IP’s ou hosts estão incluídos;
  - permissões para utilizar exploits e engenharia social;
  - deixar claro que dependendo do teste; servidores podem ser desativados;
  - saber se ao encontrar uma vulnerabilidade, o teste deve continuar para saber o que pode ser obtido ao explorar esta falha, pois dependendo das vulnerabilidades podem ser expostas informações estratégicas;
- Janela de testes: Definição de dias e horários em que os testes poderão ser executados;

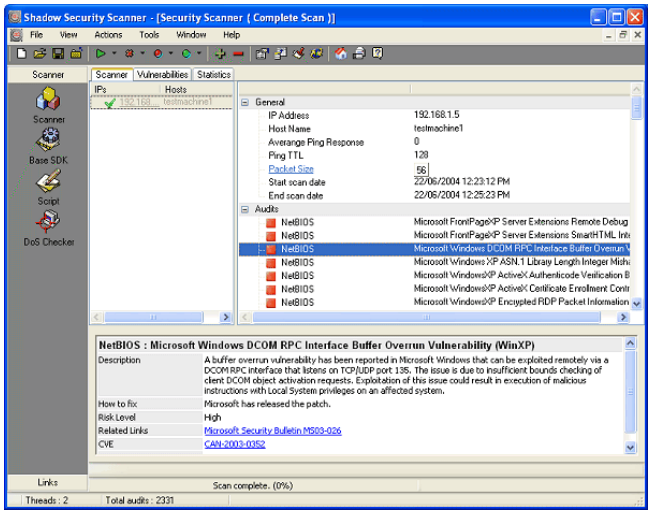
Testes de Invasão - Preparação

- **Informações de Contato**: quem deve ser alertado caso algo crítico seja encontrado ou aconteça, como servidores desativarem depois de um teste;
- **Cartão para "Sair da Cadeia Livremente**" : Autorização para a realização do teste. Caso a empresa tenha serviços de terceiros, é necessário ter a aprovação de todos e certificar que haja no contrato uma cláusula especificando o limite da responsabilidade para se resguardar caso algo crítico ocorra;
- **Termos de Pagamento**: Referente ao valor a ser pago pelo serviço prestado, bem como a definição do acordo de confidencialidade

Testes de Invasão - Coleta de Informações

- **Coleta de Informações**: Esta fase envolve pesquisa sobre a empresa. Essa pesquisa pode ser através de buscadores como Google ou através do OSINT (*Open Source Intelligence*). Nesta fase, será iniciado o uso de ferramentas como scanners de porta

GFI LanGuard™



Testes de Invasão - Modelagem das ameaças

- **Modelagem das ameaças**: Esta fase, tem o objetivo de pensar em como um invasor poderia utilizar as informações adquiridas na fase anterior para realizar um ataque. Dessa forma, estratégias são definidas para simular ataques e tentar invadir o sistema. Também conhecido como *Threat Modeling*
- "*It's an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application*." - Microsoft em seu material de estudo de SDLC
- "*Threat modeling is the use of abstractions to aid in thinking about risks*." - Adam Shostack

Testes de Invasão – Análise da vulnerabilidade

- **Análise da Vulnerabilidade**:
- são realizados os testes e descobertas as vulnerabilidades
- Geralmente alguns bancos de dados de vulnerabilidades são utilizados
- é de igual importância a realização de testes manuais
- E análises que podem levar a novas estratégias de simulação de ataques

Testes de Invasão – Exploração de falhas

- Exploração de Falhas:
- as vulnerabilidades encontradas na fase anterior serão exploradas, geralmente com a utilização de uma ferramenta.
- Existem diversas ferramentas no mercado

Testes de Invasão – Pós-exploração de falhas

- Pós-Exploração de Falhas:
- Analisadas as informações sobre o sistema invadido
- Verificado o que é possível realizar com o acesso adquirido — acessar arquivos ou elevar nível de privilégio do usuário, por exemplo, e analisar até onde é possível chegar
- Após a realização desta fase, é necessário avaliar quais dessas vulnerabilidades são relevantes para o cliente, pois pode acontecer de um sistema invadido não dar acesso a nenhum alvo relevante possível.

Testes de Invasão – Documentação

- **Documentação:**
- construído um relatório contendo todas as vulnerabilidades descobertas, contendo as análises com relação às melhorias que devem ser implementadas. Geralmente esse relatório é dividido em:
- 1. Sumário executivo: descreve os objetivos do teste e oferece uma visão geral dos resultados levando em consideração que o público-alvo são os executivos responsáveis pelo projeto;
- 2. Relatório técnico: nesta seção, estão presentes todos os detalhes técnicos da realização dos testes, considerando que o público-alvo são os responsáveis por implementar as melhorias.

Testes de Invasão – Profissional Hacker Ético/Ethical Hacker

Testes de Invasão – Profissional Hacker Ético/Ethical Hacker

- O **profissional Hacker Ético** é um sinônimo para Pentesters
- Aplica técnicas **Hackers** que envolve a simulação de ataques reais em redes de computadores e sistemas, afim de avaliar os riscos associados a potenciais falhas de segurança
- Todos estes testes são regidos devidamente mediante contrato entre o Hacker Ético e a empresa solicitante, para resguardar ambas as partes, pois existem quesitos legais para realização destes testes, leia Art. 154-A.

Testes de Invasão – Profissional Hacker Ético/Ethical Hacker

- Para realização de testes de invasão o Hacker Ético pode atuar de duas formas:
- **Interno**: realizando teste de aplicações, aplicando técnicas de engenharia social ou até mesmo atuando como alguém de dentro se passando por um funcionário ou um invasor que já tenha comprometido o acesso físico
- **Externo**: teste em que o Hacker Ético simulará um ataque por meio da Internet, aplicar engenharia social e assim por diante, até efetivamente conseguir acesso ao sistema ou a rede

Testes de Invasão – Profissional Hacker Ético/Ethical Hacker

- **Tipos de Testes de Invasão:**
  - **Black Box**: Um dos tipos mais difíceis de teste, pois será realizado o teste de invasão em um sistema remoto partindo sem nenhum conhecimento do alvo.
  - **Gray Box**: Este tipo por sua vez realiza teste com conhecimento parcial da infra-estrutura, como departamentos ou sub-redes.
  - **White Box**: Por fim temos o tipo que realizado o teste já com conhecimento total do alvo em questão, dispositivos, endereços, serviços e aplicações são conhecidos.

Testes de Invasão – Profissional Hacker Ético/Ethical Hacker

Fases de Teste de Invasão

- de forma organizada algumas etapas que são de extrema importância a serem preenchidas de forma a conhecer seu alvo antes de realmente realizar um ataque, essa avaliação permite ao Hacker Ético desenvolver um plano de ação e métodos de ataque

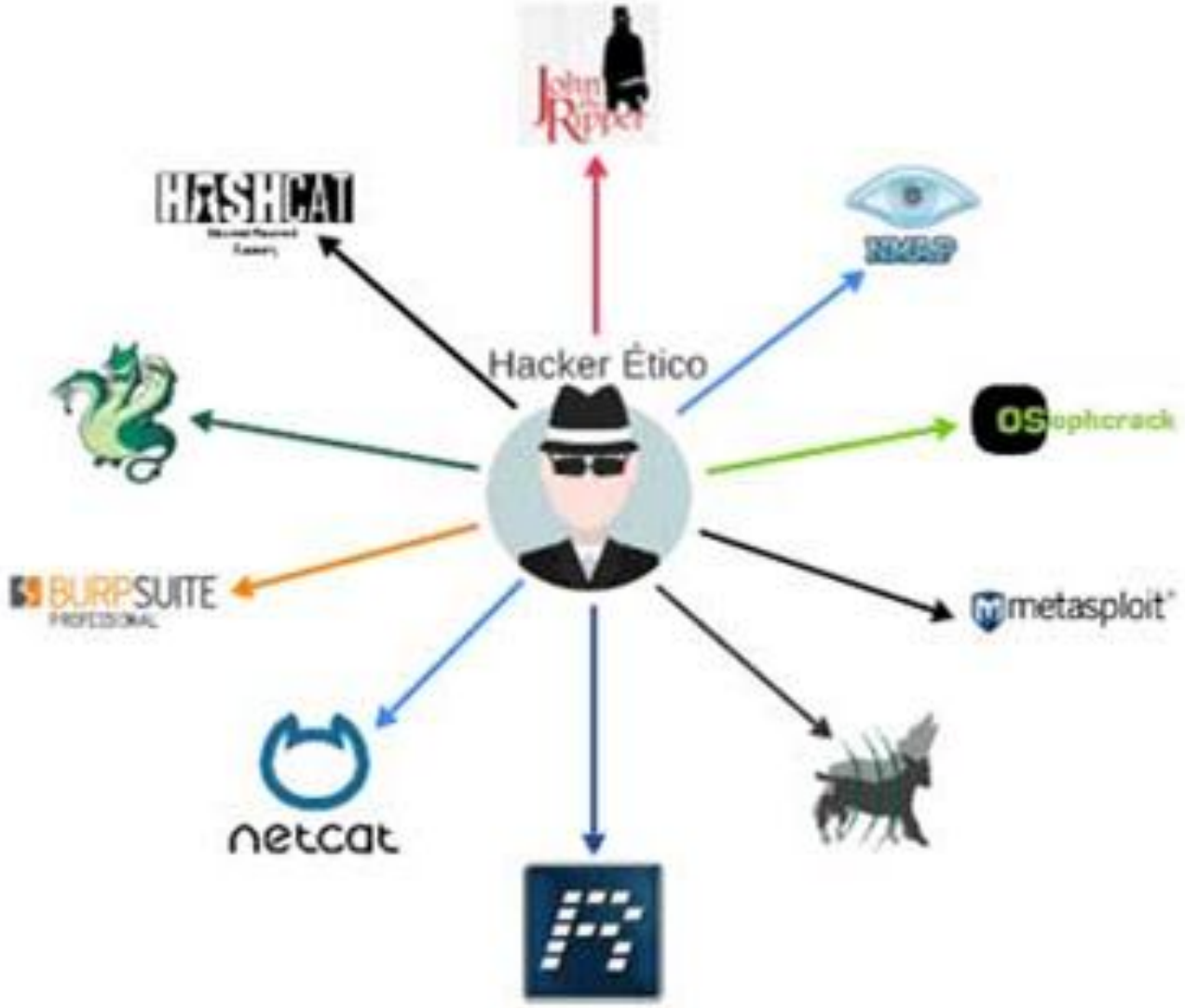
Testes de invasão – Profissional Hacker Ético/Ethical Hacker

- **Níveis Profissionais de Pentesters**
- A profissão de Hacker Ético e dividida em 3 níveis, estes níveis são para saber como esta o conhecimento do profissional.
  - **NÍVEL 1 – PENTESTER JUNIOR**: Neste nível já é um profissional que conhece as ferramentas básicas para realizar o pentest, não consegue desenvolver suas próprias técnicas e ferramentas.
  - **NÍVEL 2 – PENTESTER PLENO**: Neste nível ele desenvolve suas próprias ferramentas e scripts para realização dos penetration tests, mais ainda utiliza muitos recursos já prontos como o Metasploit para acelerar o processo de teste das vulnerabilidades. Neste nível e necessário conhecimento pelo menos em algoritmos e linguagens básicas de programação.
  - **NÍVEL 3 – PENTESTER SÊNIOR**: Neste nível tem conhecimento avançado preferem debugar o funcionamento de softwares e protocolos em busca de falhas do 0-day, e muitos são contratados por empresas com essa finalidade.

Testes de Invasão – Profissional Hacker Ético/Ethical Hacker

- **Principais Certificações Hacker Ético**
- Existem várias certificações para um profissional Hacker Ético, enumerei aqui as 3 principais:
  - EXIN ETHICAL HACKING FOUNDATION: 1 hora, múltipla escolha, inglês/português, US$ 207,00
  - CEH – Certified Ethical Hacking: diversos cursos, 4 horas, 125 questões múltipla escolha, inglês, US $ 250,00
  - OSCP – Offensive Security Certified Profissional: diversos cursos, 24 horas, prática, inglês, US $?

Testes de Invasão – Ferramentas Pentesters



Testes de Invasão – Ferramentas Pentesters

- Usa as mesmas ferramentas utilizadas pelos invasores
- Precisa conhecer essas ferramentas tanto na visão sistêmica, como em sua aplicação prática
- Vou apresentar algumas ferramentas mais utilizadas por Pentesters

Testes de Invasão – Ferramentas Pentesters

- Criada para administradores, auditores e profissionais de segurança
- Da suporte a script Luna fornecendo assim recursos adicionais de exploração de sistemas
- Opera realizando escaneamento de alvos, os quais podem ser subredes e hosts. Também escaneia portas de serviços que estão abertas, determina o tipo de serviço, versão e possíveis sistemas operacionais
- Com Nmap você faz uma varredura na rede e obtêm respostas de todos os computadores que estão ligados (método pingscan)
- O Nmap Security Scanner Project criou um site scanme.nmap.org especifico para fazer varreduras em busca de vulnerabilidades. Isso para realizar testes em um ambiente controlado

Testes de Invasão – Ferramentas Pentesters

- O Metasploit é uma ferramenta que possui uma versão open-source. A Rapid7 através da versão gratuita desenvolveu um produto profissional denominado de Metasploit Pro. O que difere as a versão Pro da gratuita é a possibilidade de se fazer integração com Nextpose
- Possui um conjunto de módulos para investigar vulnerabilidades em plataformas servidores e sistemas operacionais

Testes de Invasão – Ferramentas Pentesters

- O objetivo dele é prover um ambiente de pesquisa de exploração de vulnerabilidades. Na versão Pro possui um IPS (Intrusion Prevention System) nativo que ignora payloads, uma interface web e capacidades multiusuário
- Com as informações das vulnerabilidades é realizado o desenvolvimento do exploit, aplicando técnicas de engenharia reversa ou programação. Assim o exploit é executado em vários cenários, provando a existência de vulnerabilidades

Testes de Invasão – Ferramentas Pentesters

- Veil chamado de “Lobo em pele de cordeiro”. Com esta analogia visualizamos a sua função que é mascarar um conteúdo malicioso em uma informação aparentemente legitima
- Possui vários métodos para gerar e mascarar a área de dados de um pacote, usados para burlar os sistemas de antivírus. Ele pode até mesmo fazer a criptografia destas áreas de dados com algoritmo AES (*Advanced Encryption Standard*), codifica-los e randomizar nomes de variáveis.

Testes de Invasão – Ferramentas Pentesters

- O Burp é uma ferramenta-padrão quando se trata de proxies transparentes
- Utilizado para interagir e manipular diretamente os fluxos de tráfego na web enviados e recebidos de seu navegador
- Por padrão pode causar várias submissões em fóruns, e-mails e outras interações

Testes de Invasão – Ferramentas Pentesters

- O Hydra e bastante usado para fazer ataque de força bruta em um determinado serviço. O atacante força entrada em um local protegido por senha, por exemplo SSH (Secure Shell). Ele usa o Hydra para fazer comparações de senhas passando a credencial de root e uma lista de possíveis senhas

Testes de Invasão – Ferramentas Pentesters

- tem como característica principal ser um cracker de senha baseada de ataque de dicionário em modo online, ou seja, executados em hosts remotos. Seja com lista de credenciais é lista de palavras (Word List)
- é multitarefa, múltiplas credenciais e senhas podem ser usadas sobre um serviço (exemplo o SSH). Assim ele acelera significantemente o ataque. Mas isso pode ocasionar em detecção por um sistema IPS(Intrusion Prevention System)

Testes de Invasão – Ferramentas Pentesters

- É um dos melhores crackers de senha do mercado, como Hydra ele opera com ataque de dicionário em modo offline. Ele pode ser executado sobre um arquivo de senhas como o /etc/passwd (linux). O primeiro modo é simples, o segundo modo usa lista de palavras e no terceiro modo incremental (números e símbolos)
- Um dos recursos exclusivos é a capacidade de gerar senhas adicionais a partir de uma lista de palavras existente. O que pode ajudar a construir lista de quebra de senhas sólidas, especialmente quando usadas com outra ferramenta Cewl

Testes de Invasão – Ferramentas Pentesters

- O OclHashcat é um cracker de senhas assim como o John
- bastante utilizado quando você tem um sistema com uma forte GPU (Graphical Process Unit)
- pode quebrar rapidamente hashes de senha tirando proveito do poder de processamento da GPU
- possui capacidades poderosas de força bruta, adicionando caracteres coringas deixando mais dinâmica a quebra de senhas especificas

Testes de Invasão – Ferramentas Pentesters

- Direcionada para ataque de disco de inicialização, por exemplo MBR (Master Boot Record).
- não esta limitado à somente este tipo de ataque, pode ser usado como um cracker de senhas independente. Ele pode ser adicionado a um CD ou pendrive inicializáveis, gerando assim um Live CD. Ele executado em um sistema Windows sem criptografia completa de disco (FDE Full Disk Encryption), ele extrai os hashes do sistema operacional
- Ele tentará fazer a quebra dos hashes. Caso ele não consiga ainda pode ser copiado os hashes de senha é usar outras ferramentas como John e OclHashcat

Testes de Invasão – Ferramentas Pentesters

- O canivete suíço para administradores de redes, auditores e inclusive Pentesters
- também é conhecido como “nc”, uma das mais antigas formas de auditoria é ferramentas administrativas
- projetada para interagir com portas de serviços diretamente através do fornecimento de um endereço IP, porta e um protocolo
- com está ferramenta pode também transferir arquivos e estabelecer sessões de host a host.

Testes de Invasão – Ferramentas Pentesters

- RECON-NG está relacionada ao OSINT (*Open Source Intelligence*) inteligência de fontes abertas
- focada na identificação de dados coletados a partir de mecanismos de busca e mídias sociais
- uma alternativa usada caso não funcione e o TheHarvester.

Campeonato de Invasão – Hackaflag

- No estilo "capture the flag", um ambiente é disposto aos participantes com inúmeros desafios, de vários tipos, níveis e especialidades. Desde crypto até web, todos podem participar, não importa sua área, experiência ou idade!
- Cada desafio quebrado dá mais pontos aos participantes no placar. Quem fizer mais pontos, vence!
- Em equipes e individual
- https://roadsec.com.br/hackaflag

Exercício

Conclusão

- Conhecemos um pouco sobre análise de risco de TI.
- Riscos surgem a cada instante portanto o estudo não para aqui.

Referências

WEBER, Raul Fernando. Fundamentos de arquitetura de computadores. 4. ed. Porto Alegre: Bookman, 2012. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788540701434

STALLINGS, William. Arquitetura e organização de computadores. 8.ed. São Paulo: Pearson, 2010. E-book. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/459/epub/0

HOGLUND, Greg. Como quebrar códigos: a arte de explorar (e proteger) software. São Paulo: Pearson, 2006. E-book. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/179934/epub/0

Fim