GBC083 - Segurança da Informação
Aula 0 - Panorama

Prof. Marcelo Keese Albertini

4 de Abril de 2017

Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Em inglês: confidentiality, integrity and availability (CIA)

Como proteger uma rede e seus sistemas

- Como proteger sua rede do ponto de vista do atacante (NSA)
- `https://www.youtube.com/watch?v=bDJb8WOJYdA`
- Seis fases:
  1. Reconhecimento
  2. Exploitation ("abuso") inicial
  3. Estabelecer persistência
  4. Instalar ferramentas
  5. Mover lateralmente
  6. Coletar, vazar, explorar ou destruir dados
- Ciclo de defesa: Avaliar, Defender e Melhorar

Fase: reconhecimento

- Objetivo: encontrar primeiras “rachaduras” na segurança

Fase: reconhecimento

- Objetivo: encontrar primeiras “rachaduras” na segurança
  - Ameaça permanente avançada

Fase: reconhecimento

- Objetivo: encontrar primeiras “rachaduras” na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente

Fase: reconhecimento

- Objetivo: encontrar primeiras “rachaduras” na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?

Fase: reconhecimento

- Objetivo: encontrar primeiras “rachaduras” na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados
  - Descobrir níveis de acesso

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados
  - Descobrir níveis de acesso
  - Saber se pessoas usam rede a distância

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados
  - Descobrir níveis de acesso
  - Saber se pessoas usam rede a distância
- Manter vigilância constante

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados
  - Descobrir níveis de acesso
  - Saber se pessoas usam rede a distância
- Manter vigilância constante
- 3 vetores principais

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados
  - Descobrir níveis de acesso
  - Saber se pessoas usam rede a distância
- Manter vigilância constante
- 3 vetores principais
  - Email (spearfishing)

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados
  - Descobrir níveis de acesso
  - Saber se pessoas usam rede a distância
- Manter vigilância constante
- 3 vetores principais
  - Email (spearfishing)
  - Web sites

Fase: reconhecimento

- Objetivo: encontrar primeiras "rachaduras" na segurança
  - Ameaça permanente avançada
- Examinar rede fisicamente
  - Existem pontos de acesso disponíveis sem vigilância?
- Examinar rede eletronicamente
  - Mapear rede: nmap
- Descobrir e entender quem são os usuários mais importantes e pessoas associadas
- Avaliar pessoas
  - Quais emails elas tem e que são mais usados
  - Descobrir níveis de acesso
  - Saber se pessoas usam rede a distância
- Manter vigilância constante
- 3 vetores principais
  - Email (spearfishing)
  - Web sites
  - Removable media

Como se proteger

- Tornar decisões de segurança independentes dos usuários
- Política de atualização automática
  - Microsoft Enhanced Mitigation Experience Toolkit (EMET)
  - Secure Host Baseline: imagem de SO pré-pronta para segurança
- NSA Information Assurance website
- Usar "melhores práticas de segurança"
- Two/Multi factor authentication (caixas automáticos)
- Evitar vulnerabilidades "pass the hash"
- Remover o uso de protocolos antigos
- Ativar e usar logs
- Controle de privilégios: princípio do privilégio mínimo
  - Segmentar rede de acordo com níveis de confiança
- Serviços de autenticação de software (hash antes de executar)

Recomendações e melhores práticas

- Seja um pouco paranóico: suspeite de tudo.
- Use e garanta o uso de boas senhas:
  - Usuário: chun, senha: lee
  - Usuário: arduino, senha: 4rdu1n0
  - Usuário: jnash, senha: jn091101!@
  - Usuário: dpedro1, senha: o rato roeu a roupa do rei de roma e da rainha raimunda
  - Qual desses é seguro?

Recomendações e melhores práticas

- Seja um pouco paranóico: suspeite de tudo.
- Use e garanta o uso de boas senhas:
  - Usuário: chun, senha: lee
  - Usuário: arduino, senha: 4rdu1n0
  - Usuário: jnash, senha: jn091101!@
  - Usuário: dpedro1, senha: o rato roeu a roupa do rei de roma e da rainha raimunda
  - Qual desses é seguro?
- Software: `pwgen`, `apg`
- Dica: sequência de palavras não relacionadas transformada em mnemônico
  - Um tigre roeu a roupa de trigo da rainha com três pratos.
  - 1Tgr\rhoEUlaroupaDcevadaHAinhaMIT3pratos.

Recomendações e melhores práticas

- Seja um pouco paranóico: suspeite de tudo. Sério!
- Criptografe o seu disco rígido
- Use sites criptografados
- Conheça e use as permissões de arquivos corretas
- Não confie em software proprietário com código-fonte não disponível
- Não confie em hardware de terceiros (exemplo: pendrive, teclado com firmware malicioso)

Recomendações e melhores práticas

- Seja um pouco mais paranóico: previna-se contra problemas!
- Limite a quantidade de processos e previna `fork bombs`: `/etc/security/limits.conf`.
- Limite o uso do `root`
- Use políticas de segurança de controle de acesso (Mandatory Access Control)
- Conheça e configure o *kernel*
- Use aplicações de Sandboxing (firejail, chroot, virtualização)
- Firewall e parâmetro de rede do kernel, ssh, dns e proxies
- Autenticação e assinatura de softwares instalados
- Garanta a segurança física: cadeados, trave a ordem de boot e ponha senha na BIOS, senha no bootloader
- Mantenha-se informado

Ok. Segurança de informação. O que é informação?

- Código fonte e binários
- Documentos institucionais
  - planilhas
  - documentos
  - apresentações
- Dados de acesso (login, senha)
- Informações organizacionais
- Meta-dados de comunicações
  - quem fala com quem
  - duração
  - periodicidade
- Dados pessoais
- Em geral, registros em bancos de dados

Segurança da Informação - Metas

- Confidencialidade
  - Criptografia antiga
- Integridade
  - Criptografia moderna = Confidencialidade + Integridade
- Disponibilidade
  - Prevenção contra ataques de negação de serviços
  - Prevenção contra perda de dados

Aplicações de criptografia

- Comunicação segura (SSH, HTTPS)
- Armazenamento seguro (TrueCrypt)
- Assinatura digital (RSA)
- Comunicação anônima (mix net, tor)
- Dinheiro digital anônimo (bitcoin)
- Contratos inteligentes (ethereum)
- Protocolos de eleição (Neff e Chaum) e leilões privados
- Computação segura entre múltiplos atores (homomorfismos)

Oportunidades de mercado

- Chief Information Security Officer (CISO)
- Analista de Segurança
- Analista de Riscos em Segurança de Informação
- Analista de Incidentes de Segurança da Informação
- Analista Clínico de TI
- Arquiteto de Segurança da Informação
- Especialista de Segurança
- Especialista em Vendas de Soluções de Segurança
- Especialista Forense de Segurança em TI
- Pesquisador em Segurança
- Técnico de Respostas a Incidentes em Ciber-segurança
- Engenheiro de Segurança de Informação
- Engenheiro de Segurança de Redes
- Engenheiro de Cyber-segurança

Lugares e Pessoas

- Bletchley Park (Londres)
- NSA Headquarters (Fort Meade, Maryland)
- National Cryptologic Museum (NSA, Maryland)
- Unidade 61398 (Shanghai)
- Government Communications Headquarters (GCHQ)

- Alan Turing
- Gordon Welchman (análise de meta-dados)
- John Nash (cartas sobre criptografia para NSA)
- Ann Caracristi – biografia

Organizações, sociedades e grupos

- National Institute of Standards and Technology (NIST)
- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança `cert.br`
- Computer Emergency Response Team- CERT `cert.org`
- Chaos Computer Club – `ccc.de`
- Cult of Dead Cow
- 2600 Magazine http://www.2600.com/

Eventos

- DEF CON
- USENIX Enigma – `https://www.youtube.com/channel/UCIdV7bE97mSPTH1mOi_yUrw`
- Chaos Communication Congress – `https://www.youtube.com/user/CCCen`
- Real World Cryptography Workshop
- Mais: `https://www.concise-courses.com/security/conferences-of-2015/`

Programação

- Secure C coding
  - Segurança também deve estar no compilador (exemplo GCC)
  - Otimização pode criar problemas de segurança – STACK
- Crypto++
  - `https://cryptopp.com/wiki/Main_Page`

Ferramentas

- The Hackers Arsenal Tools Portal
  - `https://www.toolswatch.org`
- hashcat - Recuperação de senhas
  - `https://hashcat.net/oclhashcat/`
- Armitage - Testes de vulnerabilidades
  - `https://www.fastandeasyhacking.com/`
- Wifite - Auditoria de wireless
  - `https://code.google.com/p/wifite/`
- Wireshark - Monitoramento de redes
  - `https://www.wireshark.org/`

Livros, Textos e Sites

- The code breakers, David Kahn (1996)
- The Hut Six Story: Breaking the Enigma Codes de Gordon Welchman (1997)
- Relatório Mandiant sobre espionagem chinesa – `https://intelreport.mandiant.com/Mandiant_APT1_Report.pdf`
- `http://cryptopals.com/`

Objetivos da Disciplina

- Conhecer os principais serviços relacionados com a segurança da informação e sua implementação através de técnicas de criptografia.
- Conhecer e entender fundamentos de criptografia. Conhecer funcionamento de algoritmos simétricos e assimétricos.
- Adquirir capacidade de escolher técnicas de criptografia conforme a necessidade
- Conhecer e implementar serviços de segurança utilizado a JCA (Java Cryptographic Architecture)

Programa - Parte 1

- Conceitos de Segurança
- Tipos de Ataques
- Serviços e Mecanismos de Segurança
- Criptografia e Criptoanálise
- Algoritmos simétricos
  - Técnicas clássicas
  - Block Ciphers
  - Advanced Encryption Standard (AES)
  - Modos de Operação

Programa - Parte 2

- Cifradores Assimétricos
  - Conceitos e aplicações
  - RSA
- Message Authentication Codes (MAC)
  - Algoritmos Hash
  - Assinaturas digitais
- Infraestrutura de Chave Pública
- Segurança Camada de Aplicação da Arquitetura TCP/IP
- Implementação de Serviços de Segurança
- Java Cryptographic Extension para cifradores simétricos