Forense para Concursos de TI

Manipulando Arquivos e Códigos

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Gustavo Vilar – Mini CV

- PCF / DPF – Perito Criminal Federal
- Pós-Graduado em Docência do Ensino Superior – UFRJ
- Graduado em Ciência da Computação e Processamento de Dados – ASPER/PB
- Aprovações: PRF 2002, PPF-PF 2004, PCF-PF 2004, MPU 2010, ABIN 2010, PCF-PF 2013

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Gustavo Vilar

- Contatos:

http://www.itnerante.com.br/profile/GustavoPintoVilar

http://www.provasdeti.com.br/index.php/por-professor/gustavo-vilar.html

gustavopintovilar@gmail.com

p3r1t0f3d3r4l@yahoo.com.br

ITnerante

Provas de TI
TUDO PARA VOCÊ PASSAR

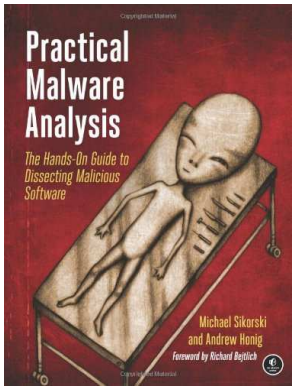
Escopo

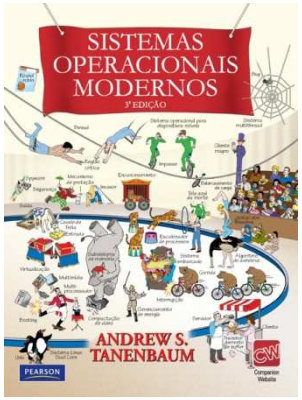
- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais frequentes.
- Abordar as metodologias de resolução de questões das principais bancas

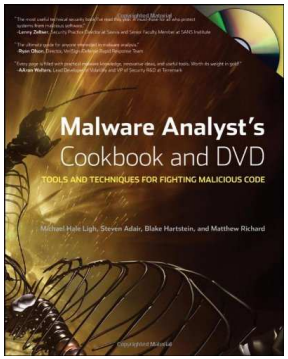
ITnerante

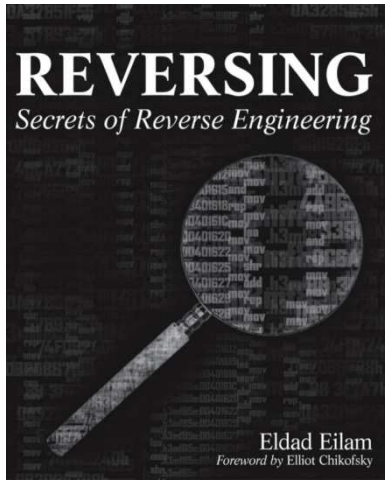
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Bibliografia









FUNDAÇÃO CESGRANRIO

cespeUnB

Google

Fundação Carlos Chagas

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos 2 – Carga Horária

- **14 vídeo aulas (04h19m23s / 00h18m32s)**
  - Fundamentação do armazenamento e formatação de discos
  - Entendendo o apagamento, recuperadores de arquivos, apagadores definitivos
  - Windows:
    - Lixeira
    - Registro
    - Logs e visualizador de eventos
  - Cracking e Anticracking
  - Tamperproof, Marca D'água
  - Natureza dos EXE, Debugging, Breakpoints
  - Virtualização x Emulação
  - Engenharia Reversa de Malware
  - Prisões e Chroot, VMI, Kelnel Callback, Driver Callback, comandos relacionados
  - Hooking, DKOM, Ferramentas
  - Duas baterias de questões de aprendizagem

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

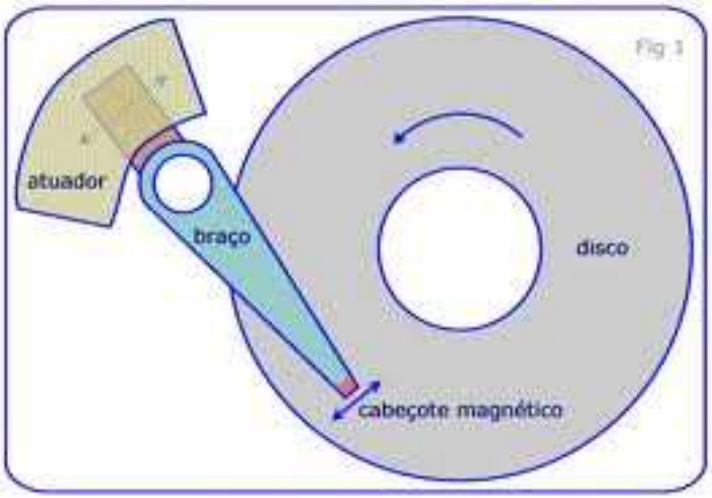
Forense para Concursos de TI

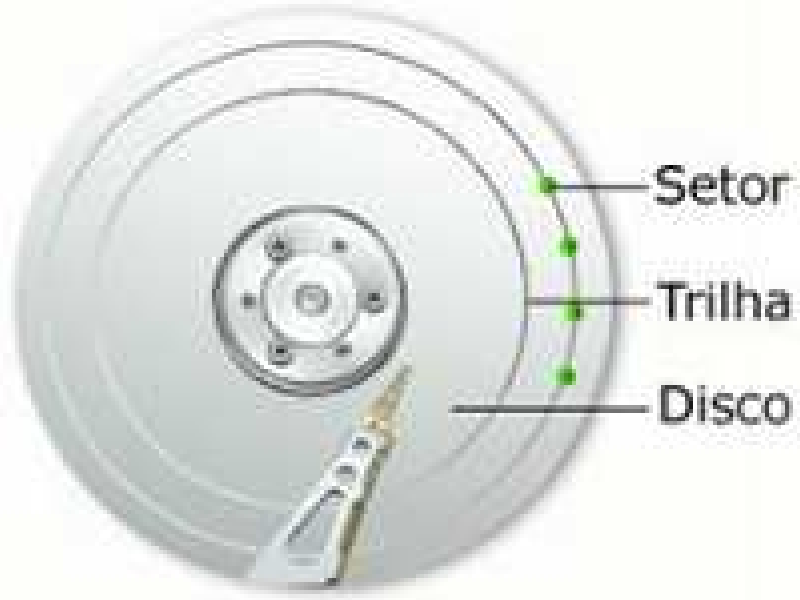
Técnicas de Recuperação de Arquivos Apagados

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Organização Física do Disco Rígido





ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

- ÍNDICE

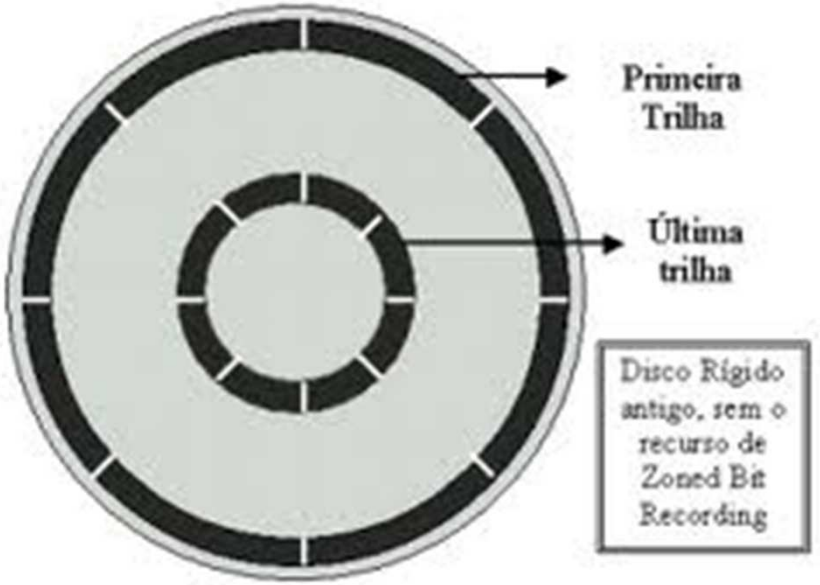
- CAPÍTULOS
  - Subcapítulos
- TEMAS
  - Subtemas
- TÓPICOS
  - Subtópicos

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Organização Lógica de um HD

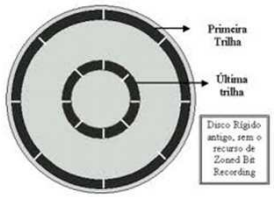
- Superfície dos discos é dividida em trilhas e setores
- As trilhas são círculos concêntricos
  - Cada trilha recebe um número
  - A trilha mais externa recebe o número 0



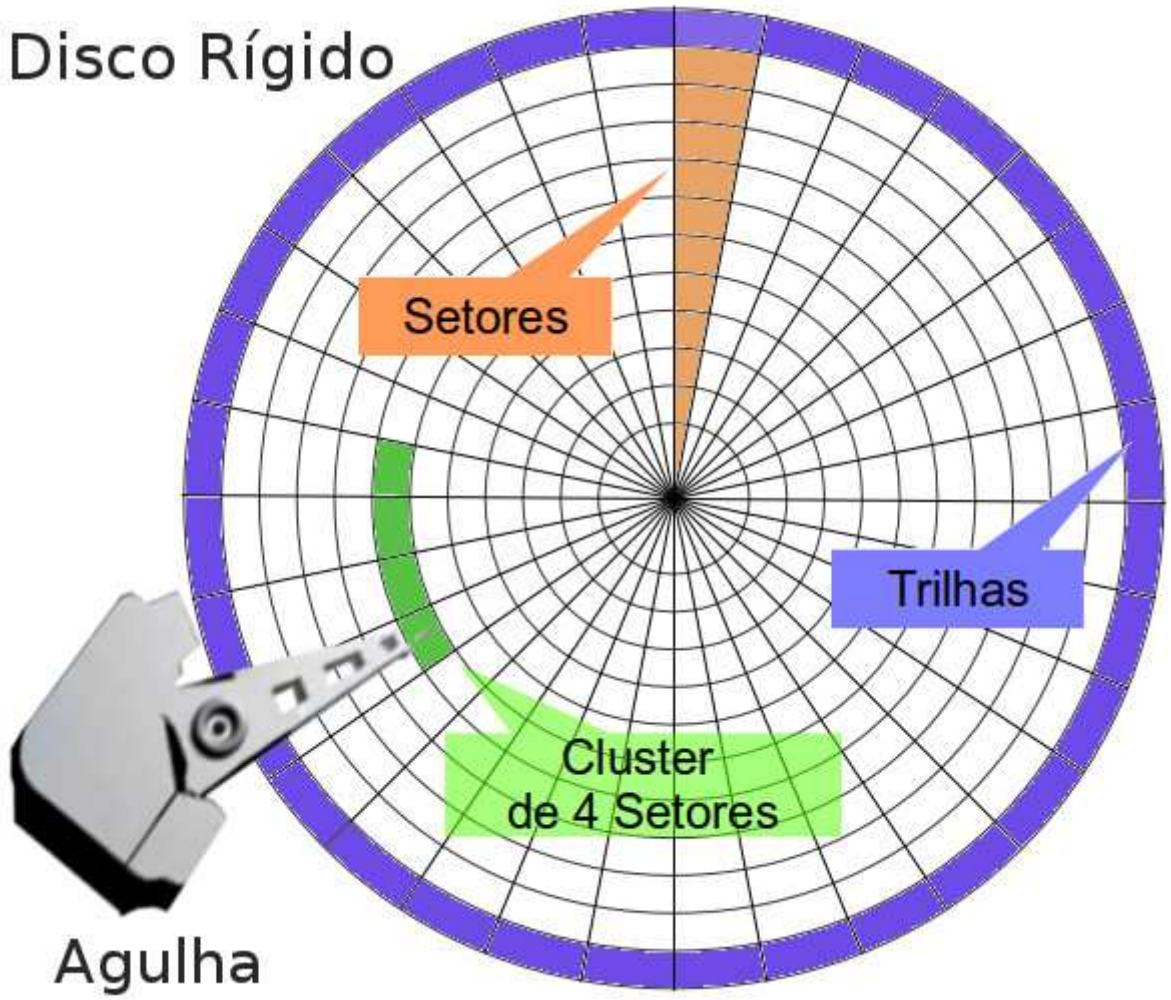
ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Discos e Memórias

- Discos são formados, basicamente, por trilhas divididas em setores.
- As projeções verticais das trilhas nos diversos pratos formam os cilindros
- Partições de disco precisam ser formatadas logicamente para receberem dados
- Formatar logicamente é estabelecer um filesystem
  - Na verdade, formatar logicamente é reorganizar a área de controle
  - Formatar, geralmente, não altera a área de dados
  - Deletar não apaga a área de dados
    - esforço computacional



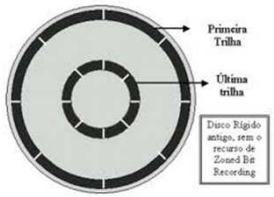
ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR



ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Discos e Memórias

- Na memória (RAM) também não é comum ocorrer uma real deleção de algo. As áreas são declaradas livres para poderem ser superpostas.
- A maioria dos arquivos possui patterns, que são padrões que os identificam
  - Todo JPG inicia com 0xFFD8FFE0
  - Todo bytecode inicia com 0XCAFEBABE



ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Por trás das cortinas do apagamento

- Quando apagamos um arquivo do disco, o sistema operacional não apaga fisicamente o arquivo do disco
  - O sistema não "zera" os setores do disco que o arquivo ocupava
- Em nome da velocidade, quando você apaga um arquivo, o sistema operacional simplesmente troca a primeira letra do nome do arquivo pelo símbolo marcador

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Por trás das cortinas do apagamento

- Quando visualizamos um diretório, o sistema ignora qualquer nome de arquivo que comece com esse símbolo, não mostrando, portanto, os arquivos que foram "apagados"
- Além disso, o sistema marca os setores que o arquivo ocupava como livre no índice
- Desde que nenhum outro arquivo tenha sido gravado na mesma área em que o arquivo apagado ocupava, é possível recuperá-lo
  - Desfazer a transformação da primeira letra

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Por trás das cortinas do apagamento

- Da mesma forma que ocorre com arquivos, durante a formatação do disco rígido os setores do disco não são "zerados"
  - Leitura da superfície
  - Marcação dos Bad blocks
  - Não há a sobreposição com nova informação

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Por trás das cortinas do apagamento

- Na formatação o sistema operacional marca, em vez de um, TODOS os arquivos como deletados
- Comandos tradicionais de formatação somente verificam se não há erros na superfície do disco, "zerando" somente a FAT

ITnerante

Provas de TI
TUDO PARA VOCÊ PASSAR

Por trás das cortinas do apagamento

- Todos os comandos de formatação de disco do sistema operacional em vez de preencherem com 0 ou 1 os setores do disco rígido durante a formatação, simplesmente apagam a tabela que informa o espaço ocupado pelos arquivos
- Desde que a área ocupada pelo arquivo a recuperar já não tenha sido sobreposta por novos arquivos, é possível recuperar o conteúdo

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Arquivos Subscritos

- É o arquivo que teve sua informação sobreposta por um novo arquivo
  - Todo
  - Parte

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Reparador de arquivos

- Software que manipula um arquivo subscrito a fim de torná-lo parcialmente utilizável
  - Música sem um trecho
  - Filme sem uma cena
  - Texto sem algumas páginas
- Dados em sistemas de arquivo de alto desempenho são mais fáceis de recuperar
  - por conta da alocação contígua dos setores
  - pouca fragmentação
    - Ext2 Ext3

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Reparador de arquivos

- Para rodar esse tipo de programa você deverá instalar uma outra unidade de armazenamento (com espaço suficiente), que é onde os arquivos recuperados serão gravados, evitando a sobreposição
- Exame de superfície
  - Identificar os padrões magnéticos antigos que persistem em uma trilha de disco
  - Utiliza técnicas de microscopia eletrônica
  - Pode recuperar dados que foram sobrescritos
    - pois, o meio de gravação no hd é analógico

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Apagando de verdade

- Para realmente apagar o arquivo do disco, o sistema operacional teria de preencher com zeros (ou com um outro valor qualquer) todos os setores ocupados pelo arquivo
  - Tempo elevado
- Utilizar os formatadores de baixo nível
  - Preenchimento com 0s
  - Preenchimento com 1s
  - Preenchimento com dados

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Apagando de verdade

- Exemplos
  - Wipe e derivados apagam somente os dados (específico para arquivos), quando aplicados em arquivos. Os inodes permanecem
  - Wipe e dd (dcfldd) podem ser aplicados em dispositivos inteiros.
  - Com dd ou dcfldd, podese criar um arquivo com conteúdo não significativo que preencha toda a área livre de um filesystem. Ex: # dcfldd if=/dev/zero of=/teste.txtfilesystem
    - Slacks spaces de blocos ocupados permanecem

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Moral da História

- Apagar dados, na ampla concepção da ideia, não é uma ação natural
- Formatar um disco é, na verdade, reestabelecer a área de controle
  - Área de dados permanece
- Há boas possibilidades de arquivos apagados ou discos formatados acidentalmente serem recuperados
  - Paciência
  - Técnica
- Fragmentos ou arquivos completos apagados poderão ser preservados por anos, principalmente em HDs grandes

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Lixeira do Windows

- Mecanismo usado para armazenar objetos excluídos de forma que podem ser restaurados mais tarde. Tais objetos podem ser arquivos, pastas, links e outros.
- Apesar de ser um espaço temporário, o conteúdo da Lixeira pode ser armazenado durante muito tempo.

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Lixeira Windows – Recuperar Arquivo

- - Dar um duplo clique sobre a lixeira para visualizar seu conteúdo.
- - Selecionar o(s) arquivo(s) desejado(s)
- - No menu Arquivo, clicar em "Restaurar".
  - Os arquivos voltarão para a pasta onde estavam ao serem deletados.
- É possível arrastar com o mouse para qualquer pasta

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Lixeira Windows – Deletar Arquivos

- Forma 01
  - Dar um duplo clique sobre a lixeira para visualizar seu conteúdo.
  - No menu Arquivo, clicar em Esvaziar Lixeira
- Forma 02
  - Dar um clique simples sobre a lixeira, com o botão direito do mouse .
  - Clicar em Esvaziar Lixeira
- Cuidado....clicar com o botão direito do mouse e selecionar "excluir", exclui o ícone da lixeira. Esta opção inexiste no windows 7, mas existe no vista

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Lixeira Windows – Configurações

- Dar um clique simples sobre a lixeira, com o botão direito do mouse .
- Clicar em Propriedades
- Pode-se definir
  - Se os arquivos deletados devem ser guardados temporariamente na Lixeira ou sumariamente deletados
  - Tamanho da área de disco que poderá ser utilizada pela Lixeira.
  - Se deve aparecer a pergunta confirmando a exclusão.

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Lixeira Windows – Dicas finais

- Cada partição tem seu espaço de lixeira. Somente os Discos Rígidos (internos ou externos) usam a lixeira.
  - Discos rígidos externos possuem lixeira
    - Somente existe lixeira para disco rígido
  - Discos removíveis não possuem lixeira
    - Não existe lixeira para disco flexível / pen drive
- O que é deletado pela rede não passa pela lixeira.
- Se o arquivo a ser deletado for maior do que o espaço livre da lixeira, será excluído permanentemente.
- A lixeira é uma FIFO quando enche.

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Lixeira Windows – Dicas finais

- Shift + Del = Não passa pela lixeira
- Binários não são executados, nem arquivos abertos dentro da lixeira
- Elementos deletados pelo prompt de comando não passam pela lixeira

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos de TI

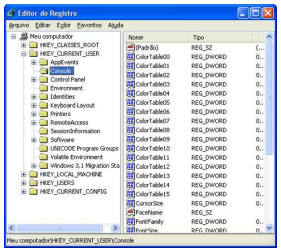
O Registro do Windows

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Finalidade

- Serve para controle do sistema Operacional
- Condensa as configurações de controle do sistema operacional
- Controla hardware, software e usuários
  - Usado para armazenar as informações necessárias à configuração do sistema
  - Refletido para um ou mais usuários

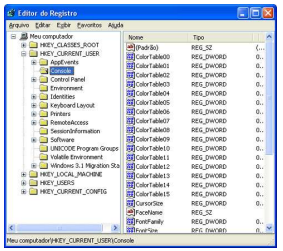


ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Nascimento

- Usado a partir do windows 95
  - Antes disso era um conjunto de arquivos .ini
    - Não existe boot.ini no Windows 7 para ser editado
    - O controle passa a ser feito pelo ícone sistema >> Configurações avançadas de segurança
  - Substitui a maioria dos arquivos .ini com base em texto usados nos arquivos de configuração do Windows 3.x e do MS-DOS
    - Exemplo: Autoexec.bat e o Config.sys

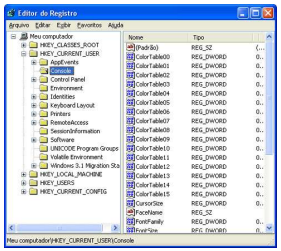


ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Atuação

- O Windows faz referência continuamente ao registro durante a sua operação
  - perfis de cada usuário
  - aplicativos instalados
  - tipos de documentos que cada aplicativo pode criar
  - configurações da folha de propriedades para ícones de pastas e aplicativos
  - o hardware existente no sistema
  - portas que são usadas



ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Estrutura

- Chaves (entradas(valor[nome, tipo, dado]))
- Coleção de chaves (diretórios) com subdiretórios ou entradas
  - Na hierarquia inferior estão as entradas chamadas valores
  - Cada valor contém 3 partes: Nome, tipo, dado

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Estrutura

- Chaves (entradas(valor[nome, tipo, dado]))
- Coleção de chaves (diretórios) com subdiretórios ou entradas
  - Na hierarquia inferior estão as entradas chamadas valores
  - Cada valor contém 3 partes: Nome, tipo, dado

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Localização

- Quando o sistema é desligado, a maioria das info fica armazenada nos arquivos chamados colmeias (hives)
  - Existem cópias de segurança destes arquivos
  - Transações atômicas
- Perda do registro = reinstalação de todos os softwares
- path do registro: C:\Windows\System32\config

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Acesso

- REGEDIT – Editor de registro do windows
  - Existem outras ferramentas com mesma finalidade.
  - Algumas estão disponíveis na mídia de instalação do Windows.

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Chaves

- Desde Windows 2000 são 6 chaves:
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_PERFORMANCE_DATA
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_CONFIG
  - HKEY_CURRENT_USER

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_LOCAL_MACHINE (info sis local)

- HARDWARE
  - hardware e driver controlador
  - Construída em momento de carga pelo gerenciador plug-and-play
  - Não fica armazenada em disco

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_LOCAL_MACHINE (info sis local)

- SAM
  - Usuários, senhas, grupos, etc...
  - Segurança necessária para o acesso dos usuários ao sistema
  - Arquivos de suporte
    - Sam, Sam.log, Sam.sav
      - LOG – um log de transação das mudanças nas chaves e os valores das hives;
      - SAV – cópia da hive feita logo após o fim do modo texto do setup do Windows.

-

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_LOCAL_MACHINE (info sis local)

- SECURITY
  - Política geral de segurança (tamanho da senha, tentativas de acesso antes do bloqueio, etc...
  - Arquivos de suporte
    - Security, Security.log, Security.sav

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_LOCAL_MACHINE (info sis local)

- SOFTWARE
  - Fabricantes de software armazenam suas preferências
  - Arquivos de suporte
    - Software, Software.log, Software.sav

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_LOCAL_MACHINE (info sis local)

- SYSTEM
  - Info sobre inicialização do sistema
  - Arquivos de suporte
    - System, System.alt, System.log, System.sav
      - Arquivo .ALT – uma cópia de backup da hive HKEY_LOCAL_MACHINE\SYSTEM (o Windows 2003 não tem este arquivo);

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- Contém a relação de aplicativos inicializados automaticamente ao ligar a máquina
- Não são necessariamente os presentes no menu inicializar
- Não são necessariamente os presentes em MSconfig
  - MSCONFIG relaciona os RUN + menu inicializar
- Executarão automaticamente

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services

- Lista serviços relacionados na aba serviços
- Não necessariamente inicializados automaticamente

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_USERS

- Fica armazenado em disco
- Perfil de todos usuários
- Arquivos de suporte
  - Default, Default.log, Default.sav

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_PERFORMANCE_DATA

- Não é lido do disco
- Contadores de desempenho
- Não é visível via regedit, mas sim por ferramentas específicas

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_CLASSES_ROOT

- Não existe
- Atalho para HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES
- Associação de extensões e programas

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_CURRENT_CONFIG

- Não existe
- Atalho para configuração atual do hardware HKEY_LOCAL_MACHINE\SYSTEM\XXXXXX

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

HKEY_CURRENT_USER

- Não existe
- Aponta para o usuário atualmente conectado, visando encontrar as preferências

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Registro do Windows - Chaves

- Desde Windows 2000 são 6 chaves:
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_PERFORMANCE_DATA
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_CONFIG
  - HKEY_CURRENT_USER

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos de TI

Log de Eventos do Windows

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Para que serve?

- O Log de eventos do Windows é um repositório de informações importantes sobre programas, segurança, eventos do sistema, usuário, etc
- Ferramenta de visualização: "Painel de Controle > Ferramentas Administrativas > Visualizador de Eventos

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Event Viewer

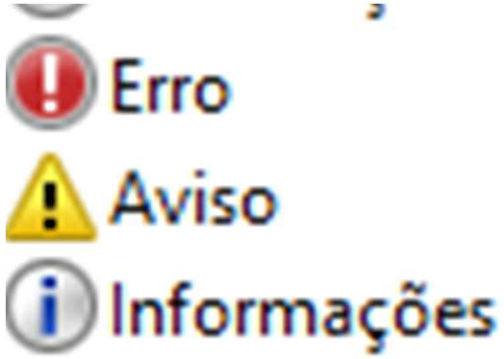
- Padrão
  - Application
  - System
  - Security
- Opcionais
  - Variam de acordo com os recursos instalados na máquina

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Event Viewer

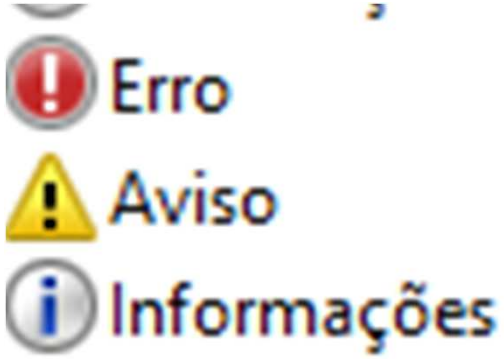
- Application
  - Programas
  - Eventos de outras aplicações <> do S.O.
  - Eventos de aplicativo (programa). Os eventos são classificados como erro, aviso ou informações



ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Event Viewer

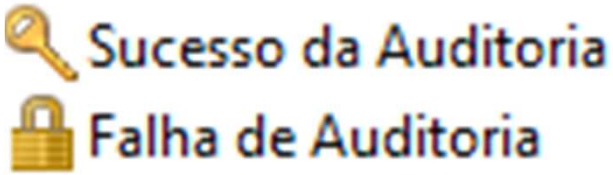
- system
  - Eventos do SO e serviços.
  - Os eventos são classificados como erro, aviso ou informações



ITnerante
Provas de TI
TUDO PARA VOCÊ PASSAR

Event Viewer

- Security
  - Eventos relacionados à segurança. Esses eventos são chamados de auditorias e são classificados como bem-sucedido ou com falha
  - Sucesso na auditoria
    - A ação foi bem sucedida, bem como seu registro
  - Falha de auditoria
    - A ação falhou, mas o registro foi bem sucedido
  - Visível somente ao Adm



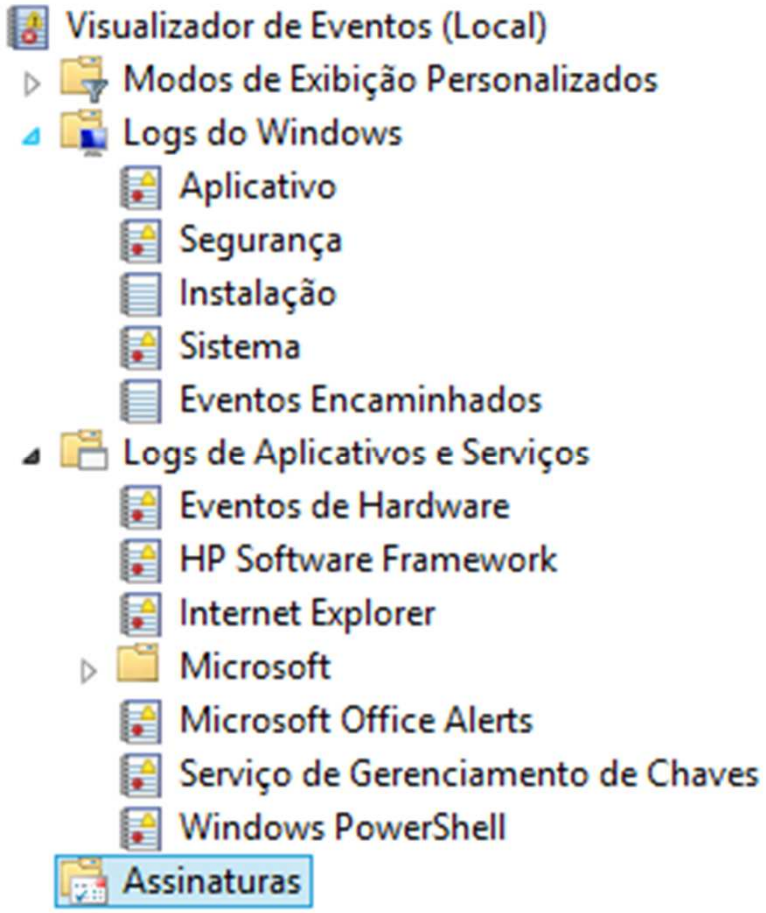
ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Event Viewer

- Opcionais Variam de acordo com os recursos instalados na máquina
  - Internet Explorer já possui sua própria entrada no event viewer
  - ForwardedEvents
    - Eventos encaminhados. Esses eventos são encaminhados a esse log por outros computadores.
  - Eventos de instalação.
    - Os computadores que são configurados como controladores de domínio terão logs adicionais exibidos aqui

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR



ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

ETW (Event Tracing for Windows)

- Reúne a API de debug avançado para desenvolvedores e os logs tradicionais do windows
- Englobou o event viewer do windows

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Exemplos de Eventos auditáveis

- Logon/Logoff
- Gerenciamento de usuários
  - Inclusão, alteração, remoção
- Acesso a objetos
  - Objeto no Windows é tudo que possui uma ACL
    - Arquivo, diretório, chave de registro, impressora
  - Deve ser habilitada a diretiva para auditoria de acesso a objetos
  - Além da diretiva, deve ser especificado em cada objeto que será auditado quais usuários/grupos serão monitorados
- Alteração de diretivas
- Processos
- Alteração nas configurações do sistema
  - Data/hora, desligamento

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Arquivos Relacionados

- Até o Windows 2003
  - C:\Windows\System32\config
    - AppEvent.evt
    - SysEvent.evt
    - SecEvent.evt
- "Juntos com o registro"

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Arquivos Relacionados

- A partir do Windows Vista e Windows 7, 8
  - C:\Windows\System32\Winevt\Logs
    - Application.evtx
    - System.evtx
    - Security.evtx
- “Separados do registro”

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos de TI

Cracking & Anticracking

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Metodologias Anticracking

- Existem várias soluções para se proteger um código computacional
- Nenhuma técnica isolada provê tanta segurança e dificuldades de reversão, quanto a combinação das várias técnicas
- Técnicas de segurança, como a ofuscação de código podem dificultar ou até mesmo inviabilizar a análise do código, tornando o software mais confiável e seguro

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Algumas Metodologias Anticracking

1. Ofuscação de Código
2. Técnicas de Tamper-proofing
3. Inserção de Marcas D’água

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação de Código

- Técnica usada para aumentar a resistência de compreensão de um código
- Consiste em modificar o layout do programa, a lógica e os dados, resultando num código reorganizado, menos legível, mas fiel à funcionalidade original.
- Ofuscar um código significa convertê-lo em outro menos compreensível para o ser humano, inserindo ou modificando instruções, entretanto, mantendo a sua funcionalidade.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Atividades Desenvolvidas na Ofuscação

- Repetição/Alteração de nomes de identificadores
  - Impedir ou dificultar que usuários obtenham conhecimento da estrutura do código, como por exemplo, nome de variáveis, nome de métodos ou nome de campos
  - Alterar os nomes das estruturas do programa por código sem sentido, dificultando a interpretação do usuário
- Cifragem de strings
  - Strings, que teoricamente ficariam intactas, são modificadas
- Mudanças no fluxo de execução
  - Prejudicando a análise estática do código
- Inserção de conteúdo inerte
  - Consiste em adicionar falsos dados no código fonte do programa, porém sem alterar suas funcionalidades, mas que dificultem a engenharia reversa do código

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação de Código - Implicações

- Tornar a tarefa de solucionar os problemas na aplicação muito complexa, aumentando os custos de manutenção.
- A ofuscação pode ser utilizada em um contexto malicioso, especificamente para desenvolvedores de código malicioso onde se fazem uso da técnica para ofuscar códigos de natureza pervertida.
- Afeta de alguma forma a gerência do código
  - Desenvolvimento da aplicação / execução / manutenção

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação Estática de Código - Técnicas

1. Transformações de layout
   - Remoção de informações de formatação de arquivos normalmente presentes em arquivos ‘.class’
   - Renomeação dos identificadores

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação Estática de Código - Técnicas

2. Transformações de controle
   - Consistem na inserção, reordenação ou eliminação de blocos básicos no fluxo de execução do programa
   - Consiste na adição de saltos condicionais ou incondicionais para que estes códigos sejam incorporados no fluxo de controle do programa
   - Os saltos condicionais são normalmente vinculados com PREDICADOS OPACOS
     - Expressões cujos valores são de conhecimento do programador ou ofuscador, porém de difícil discernimento para um analisador estático ou um analista

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação Estática de Código - Técnicas

3. Transformações de dados
   - Envolvem a conversão de uma representação de uma estrutura de dados, tipo de dados ou instruções em outra representação que seja mais difícil para um atacante entendê-la
   - Ex. Em vez de chamar a função JMP explicitamente, chama-se uma outra função que direciona para a mesma linha pretendida com o JMP

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação Dinâmica de Código - Técnicas

1. Aplicação de criptografia / compactação
   - Não eficaz diante de ataques Man-at-the-end, pois em algum momento de execução, o código torna-se visível para um adversário
2. Transformação constante do fluxo de execução
   - Troca de uma sequência de instruções originais por uma sequência de instruções falsas e vice versa
   - O objetivo é deixar instruções originais o menor tempo possível na memória e disfarçá-las com instruções falsas para evitar que um analista descubra propriedades importantes do programa
   - Antes de executar uma instrução falsa, a instrução verdadeira é colocada no endereço da instrução falsa, e após executar a instrução verdadeira, a instrução falsa é recolocada no endereço da instrução verdadeira.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação maliciosa de Código

- Programadores de código malicioso também aplicam técnicas de ofuscação de código
- Visam a se evadir da detecção pelos varredores de código malicioso, pois uma boa parte da “inteligência” destes varredores é baseada no padrão de bits, chamado de assinatura
  - ofuscações alteram o padrão de bits

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Ofuscação maliciosa de Código - Técnicas

- **Polimorfismo**
  - Constituído de duas partes: rotinas de criptografia e uma parte constante de código
  - A natureza polimórfica se dá através de transformações aplicadas no par de rotinas de criptografia, podendo gerar diferentes métodos para criptografar a parte constante do código a cada replicação do código do programa
  - O corpo decriptografado do código malicioso permanece inalterado durante as gerações
- **Metamorfismo**
  - Um código metamórfico é constituído de uma rotina que transforma todo o código do programa, incluindo a rotina de transformação
  - Assim, não existem especificadamente rotinas de criptografia e uma parte constante de código como nos códigos polimórficos
  - Cada replicação de um código metamórfico pode gerar versões totalmente diferentes da anterior, podendo adicionar inclusive novas funcionalidades

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Deofuscação de Código

- O deofuscador é o programa que realiza uma série de análises de fluxo de dados e de execução no código ofuscado até que possa retirar o código original (ou bem próximo deste), removendo instruções irrelevantes.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Tamper-proofing

- As técnicas de tamper-proofing visam a assegurar que um determinado programa execute como esperado, adicionando certo nível de resiliência ao mesmo
- Além de estarem atreladas à detecção de violações de integridade, também possuem funcionalidades de resposta em situações de modificação ou monitoração
- Estas técnicas estão correlacionadas com as técnicas de ofuscação de código, dado que para que um código seja modificado, o mesmo precisa ser entendido.
  - Ex: Shareware com execução de 15 dias

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Tamper-proofing

- Estratégias de tamper-proofing para detectar violações a integridade consistem na auto-verificação de trechos de código do programa ou na inspeção lógica do mesmo
- A verificação de integridade pode ser
  - Estática em que a verificação é feita em tempo de carregamento
  - Dinâmica em que a verificação é feita durante tempo de execução

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Tamper-proofing - Técnicas

- Auto-verificação de código
  - uso de hash
  - de uma determinada região ou do código inteiro
  - As funções que calculam o hash também podem ser alvos de ataque de varredura por padrão, assim, é extremamente importante que estas funções estejam escondidas
- Inspeção da lógica de execução
  - Visam a atender as deficiências dos métodos de auto-verificação de hash
  - Os hashes são basicamente calculados sobre valores de variáveis e no resultado de predicados de fluxo de controle

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Tamper-proofing – Reações dadas

- Entre as estratégias comuns para a ação (resposta)
  - terminar a execução do programa
  - restaurar o programa substituindo os trechos de código adulterados por trechos originais
  - retornar resultados incorretos
  - degradar o desempenho da aplicação,
  - contatar o desenvolver
  - punir o sistema do adversário, por exemplo, apagando seus documentos pessoais
  - Sejam quais forem a forma de verificação e a resposta a ser tomada, é importante que as mesmas estejam distantes em tempo e espaço para aumentar a dificuldade de subversão
    - execução não simultânea
    - não próximas no código do programa

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Marca d’água

- Fornece subsídios para se identificar o uso indevido de um software
- Pode ser interpretada como o último estágio na defesa de um software
- Embora a marca d'água não impeça o uso indevido de um software, permite que ações legais— sejam tomadas.
- Difere da esteganografia, pois não se preocupa se a informação de marca é ou não detectável
- **Resumo**: uma vez que a ofuscação falha em seu objetivo de dificultar a análise e as ferramentas de tamper-proofing falham em seu objetivo de impedir a execução indevida, ainda assim, é possível identificar que um determinado software, em execução em um dispositivo, está sendo utilizado indevidamente

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos de TI

Análise Dinâmica de Código Malicioso

ITnerante

Provas de TI
TUDO PARA VOCÊ PASSAR

Natureza dos arquivos executáveis

- Os executáveis (DLL, EXE, etc...) possuem as instruções que serão executadas, bem como os códigos de chamamento de rotinas auxiliares
- Apesar dessas instruções serem bastante claras para a arquitetura computacional subjacente, são de difícil compreensão para o ser humano.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Debugging

- Para obter um comportamento de malware é preciso executá-lo em um sistema especialmente projetado para a tarefa de monitoração
- As ações realizadas pelo binário
  - abrir um arquivo
  - realizar alterações em registros
  - Abrir portas de comunicação de rede
  - Alterar entradas em registros
  - Enviar /receber conteúdos remotamente

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Debugging

- Na análise dinâmica de códigos maliciosos, pode ser utilizada para mapear características e atividades do do malware
- Favorece criação de métodos de detecção por identidade ou semelhança, facilitando a identificação e prevenção de contaminações futuras.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Debugging

- Consiste em acompanhar a execução de determinado programa, adicionando pontos de parada em sua execução e avaliando valores internos, a fim de obter uma análise dinâmica do exemplar;
- Normalmente é executada por desenvolvedores com finalidade de depuração e teste.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Debugging

- As paradas se dão por uso de breakpoints, que nada mais são do que a inserção de instruções “ilegais” em determinados pontos do programa, forçando sua parada
- Grupos
  - Software
  - Hardware
  - Memória

ITnerante
Provas de TI
TUDO PARA VOCÊ PASSAR

Breakpoints

- **Software breakpoints**
  - Modificam o código da aplicação através da inserção de um marcador em determinados pontos do programa;
  - São sensíveis à detecção de violação, uma vez que modificam o código original, se tornam sensíveis a testes de integridade.
    - **modo trap** - executa instrução a instrução
    - **modo debugging** - Coloca o marcador na posição específica

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Breakpoints

- **Hardware breakpoints**
  - Utilizam os recursos do processador, por isso não são detectados no modo de usuário, mas passíveis de detecção no modo núcleo
  - Mesmo que o código sob análise tente se valer de requisições ao sistema para avaliar se está sob análise, o debugger pode interceptar estas requisições e retornar uma resposta falsa e esperada, não revelando assim que o programa está sob análise.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Breakpoints

- **Breakpoint de memória**
  - Posições de memória são analisadas no sentido de detectar operações de RW específicas

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Debugging

- Programas
  - IDA PRO
    - Pago
    - Dispõe de mais recursos
  - OLLY Dbg
    - Gratuito

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos de TI

Técnicas de Análise Dinâmica de Código Malicioso

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Roteiro

- Emulação x Virtualização
- Engenharia Reversa de Malware
- Prisões e chroot()
- Virtual Machine Introspection
- Kernel Callbacks e Filter Driver Callbacks
- Hooking
  - Usuário
  - Kernel
- Direct Kernel Object Manipulation (DKOM)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Emulação x Virtualização

- Emulação simula o hardware
- Usado para promover a separação do ambiente analisado, impedido que ações promovidas no ambiente hóspede, tenha efeitos no ambiente hospedeiro.
- É possível emular várias categorias de dispositivos (processador, hds, etc....) permitindo a simulação das mais variadas arquiteturas, abrangendo vários sistemas operacionais.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Emulação x Virtualização

- O código sob análise pode detectar que está sendo monitorado? **Sim**, a detecção pode ser feita através de uma chamada de instrução que provoque determinado comportamento, seja com ou sem falhas.
- Um dos modos utilizados para realizar tal verificação é por meio de bugs conhecidos em processadores de determinadas arquiteturas que fazem com que certas instruções tenham determinadas assinaturas
- Se o emulador for muito “perfeito” e apresentar algum comportamento fora do esperado, o malware pode mudar de comportamento e comprometer a análise.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Emulação x Virtualização

- Tanto a emulação quanto a virtualização têm a mesma finalidade no contexto de análise de malware: Isolar os ambientes envolvidos no contexto da análise
- Na virtualização, as instruções são executadas no hardware real da máquina. Na emulação, isso ocorre na camada de abstração criada no processo emulativo.
  - Virtualização se torna mais rápida que a emulação
  - Virtualização é mais limitada por permitir a instalação de sistemas compatíveis com a arquitetura subjacente.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Roteiro

- Emulação x Virtualização
- Engenharia Reversa de Malware
- Prisões e chroot()
- Virtual Machine Introspection
- Kernel Callbacks e Filter Driver Callbacks
- Hooking
  - Usuário
  - Kernel
- Direct Kernel Object Manipulation (DKOM)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Engenharia Reversa de Malware

- Extrair informações do código malicioso a fim de entender seu funcionamento interno e suas interações externas
- Ferramentas automatizadas ajudam no trabalho, mas não conseguem resolvê-lo de forma automática e direta.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Engenharia Reversa de Malware

- Normalmente é aplicado em códigos com indisponibilidade dos códigos fonte, possibilitando assim um maior entendimento sobre as ações executadas durante sua execução.

ITnerante

Provas de TI
TUDO PARA VOCÊ PASSAR

Engenharia Reversa de Malware

- Algumas questões a serem respondidas na análise de malware:
  - Quais técnicas foram usadas para comprometer o sistema?
  - Quais são as técnicas furtivas por ele usadas após a execução?
  - Quais dados do sistema comprometido são capturados e/ou transmitidos?

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Engenharia Reversa de Malware

- A partir da resposta aos quesitos exemplificativos acima, poderemos mapear a ação do malware e compor um padrão de comportamento para composição de bases (assinaturas ou comportamentais)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Engenharia Reversa de Malware

- Outro objetivo da engenharia reversa de malware é compreender as formas criptográficas utilizadas pelo exemplar (polimorfose ou metamorfose)
  - Criptografia aplicadas para que os dados não fiquem “claros” no binário.
    - Ex: Uma referência a um endereço utilizada pelo malware para referenciar outro componente
    - E-mail para envio dos dados capturados

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Roteiro

- Emulação x Virtualização
- Engenharia Reversa de Malware
- Prisões e chroot()
- Virtual Machine Introspection
- Kernel Callbacks e Filter Driver Callbacks
- Hooking
  - Usuário
  - Kernel
- Direct Kernel Object Manipulation (DKOM)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Prisões e chroot()

- Prisões
  - Visa ao confinamento do processo, não deixando-o interagir com outros recursos do sistema
  - Um processo dentro de uma prisão não tem acesso a processos, arquivos e outros objetos fora da prisão.
  - Mesmo sendo executado em modo superusuário não tem permissão de atualizar parâmetros de configuração de kernel nem manipular módulos. A prisão tem finalidade impeditiva.
  - O kernel é compartilhado entre prisões e ambientes não-prisão
  - Não possui o overhead de software que as VMs possuem
    - porém, por compartilharem o kernel possuem o mesmo grau de segurança das VMs

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Prisões e chroot()

- chroot()
  - É uma chamada de sistema do UNIX que restringe o acesso ao sistema de arquivos modificando o diretório raiz do processo
  - Limita apenas o acesso ao sistema de arquivos, não fornecendo nenhum isolamento com relação a processos ou outros objetos do sistema
  - Um invasor pode escapar facilmente desse método por meio de outras chamadas de sistema
  - Não recomendado

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Roteiro

- Emulação x Virtualização
- Engenharia Reversa de Malware
- Prisões e chroot()
- Virtual Machine Introspection
- Kernel Callbacks e Filter Driver Callbacks
- Hooking
  - Usuário
  - Kernel
- Direct Kernel Object Manipulation (DKOM)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

VMI - Virtual Machine Introspection

- A modificação de um programa de virtualização ou emulação com o objetivo de se obter informações internas ao hóspede a partir do hospedeiro.
- A principal desvantagem da VMI é que um malware pode detectar que está sendo executado em um ambiente emulado/virtual, evitando a análise como um todo ou apresentando um comportamento alternativo ao malicioso

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

VMI - Virtual Machine Introspection

- Técnica onde se cria uma camada entre o sistema de análise (guest) e o ambiente de processamento (host), de forma que todas as ações que ocorrem dentro do sistema guest não são propagadas para o host
- Possibilita a captura das ações que estão sendo executadas dentro do ambiente de análise, sem que haja qualquer interferência dentro do ambiente onde está sendo executado, possibilitando assim que um malware seja analisado sem qualquer tipo de modificação no sistema host

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

VMI - Virtual Machine Introspection

- Com esta técnica é possível obter informações de mais baixo nível sobre a execução do binário, como por exemplo, as chamadas de sistema (system calls) executadas e o estado da memória e dos registradores do processador

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Virtual Machine Introspection

- A grande limitação desta abordagem é justamente a necessidade do ambiente de análise virtualizado
  - Como não há modificação no sistema guest, a análise fica transparente para o malware, impossibilitando qualquer tentativa de identificação do componente de captura
  - Existem alguns tipos de malware que, a fim de burlar a análise e identificação de suas ações, realizam diversas checagens para verificar se estão executando em ambiente virtual e que, ao notarem a presença deste tipo de ambiente, modificam seu comportamento de forma a ocultar o fluxo de execução malicioso

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Virtual Machine Introspection

- Com a utilização desta técnica é possível alcançar um nível de privilégio adicional na camada de abstração intermediária entre o host e o guest
- Torna possível a análise de malware cuja execução ocorre no nível do kernel, tais como os rootkits
  - O que às vezes não é possível com as técnicas de hooking
- Um tipo de informação que pode ser capturada do sistema guest são as syscalls que o malware executou durante a análise

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Roteiro

- Emulação x Virtualização
- Engenharia Reversa de Malware
- Prisões e chroot()
- Virtual Machine Introspection
- Kernel Callbacks e Filter Driver Callbacks
- Hooking
  - Usuário
  - Kernel
- Direct Kernel Object Manipulation (DKOM)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Kernel Callbacks

- Funções disponibilizadas pelos S.Os às aplicações com finalidade de notificações de alterações no sistema
- Por serem bem documentadas, se apresentam de forma bastante consistente, apesar das sutis variantes existentes entre as versões dos S.Os (Windows p.ex.)

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Kernel Callbacks

- Principal limitação: Permite a captura apenas das funções disponibilizadas pela versão do Sistema Operacional.
- O Sistema Operacional é quem fornece o menu de chamadas, não é o analista que as constrói.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Driver Callbacks

- A captura pode ser melhorada com uso de filter drivers.
  - Seu funcionamento é similar ao de um filtro, interceptando todas as requisições feitas a um determinado dispositivo do sistema
  - Se posicionam entre o driver de dispositivo, no qual estão sendo interceptadas as requisições, e o nível de usuário, tendo acesso assim a todas as chamadas feitas ao dispositivo interceptado
  - Seu uso em conjunto com kernel callbacks possibilita que seja capturado um número maior de informações, apesar de ainda limitados.
  - Como resultado, poderemos ter uma análise incompleta e/ou inconclusiva

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Comandos relacionados com o conceito de callback

- strace
  - Linux
  - Rastreador genérico de chamada de sistema
  - Se anexa em um processo já em execução
- ttywatch
  - Linux
  - Grampeia sessões de login diretamente a uma porta de terminal do usuário
- OBS: Só pode haver um processo de rastreamento por processo rastreado
  - É possível que um invasor torne um processo não rastreável "grampeando-o" antes dos investigadores

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Roteiro

- Emulação x Virtualização
- Engenharia Reversa de Malware
- Prisões e chroot()
- Virtual Machine Introspection
- Kernel Callbacks e Filter Driver Callbacks
- Hooking
  - Usuário
  - Kernel
- Direct Kernel Object Manipulation (DKOM)

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Contextualização

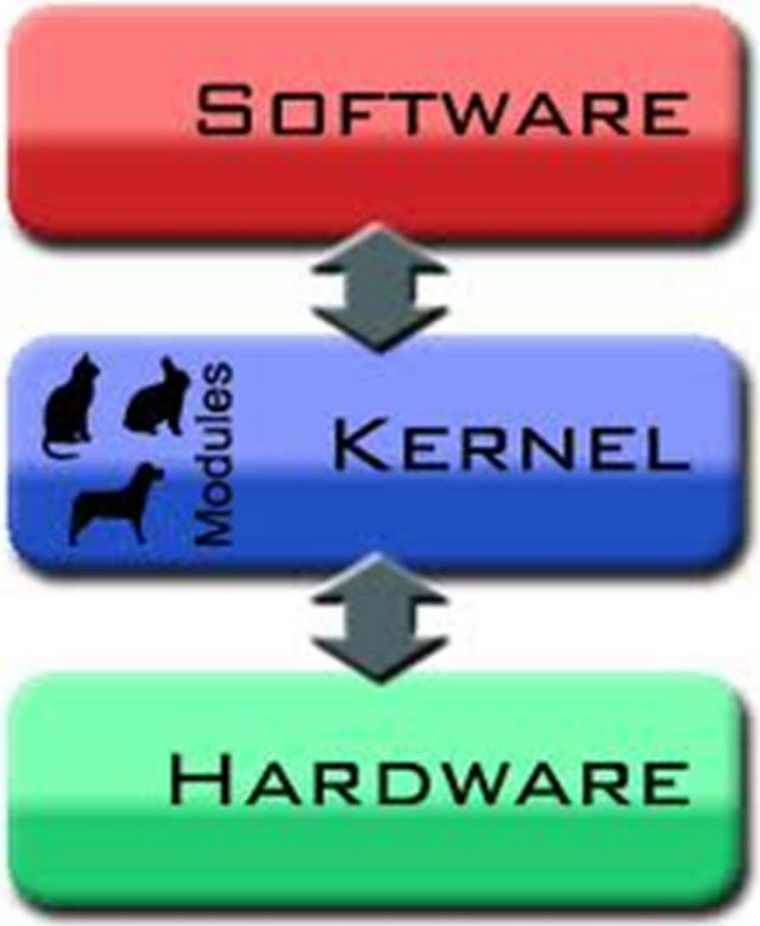
- Códigos maliciosos usam essa categoria de técnicas para capturar e/ou modificar informações que estejam transitando numa aplicação e/ou no sistema operacional
  - Ocultação de atividades, criando barreiras no processo de identificação de sua presença
  - Técnica empregada por rootkits (objetivando se camuflar no sistema alvo)

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Hooking

- Consistem em técnicas de alteração das requisições e respostas resultantes das interações realizadas em um sistema operacional e suas aplicações através da interceptação das funções ou eventos
  - Análogo ou MITM
  - Também conhecido como spoofing de system call
- Subespécies
  - Em nível de Usuário
  - Em nível de Kernel

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

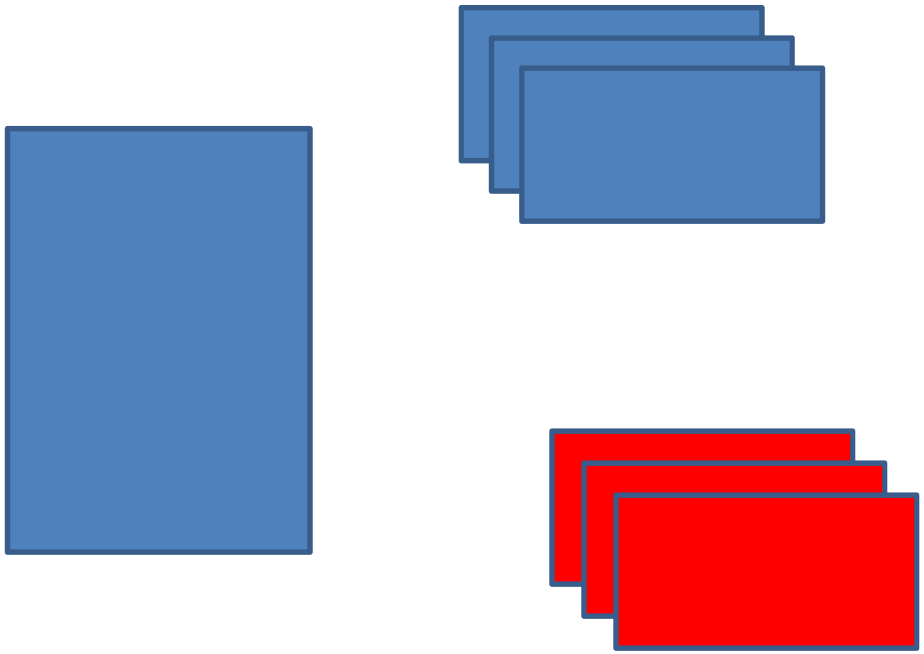


ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Hooking em Nível de Usuário

- Código sob análise sofre modificação nos endereços das APIs, apontando agora para as APIs “falsas“ responsáveis pela interceptação e/ou alteração das requisições e respostas
  - Procedimento ocorre em tempo de carga, onde as DLLs requeridas são verificadas para fins de obtenção dos endereços das APIs que se quer modificar. Após esse passo, troca-se os endereços

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR



ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Hooking em Nível de Usuário

- Vantagens:
  - Fácil de implementar;
  - Resultados mais precisos;
  - Softwares comerciais fazem uso exaustivo das API dos S.O
- Desvantagens:
  - Código analisado pode fazer auto-checagem
  - Se o código realizar chamadas diretas para o kernel, sem passar pela API, a técnica se torna ineficaz.
  - Captura parcial das atividades, comprometendo a análise

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Hooking em Nível de Kernel

- Executa em um nível mais privilegiado, utilizando técnicas mais complexas que não são trivialmente detectadas por malware
  - torna a sua detecção mais difícil, caso a ferramenta analisadora rode em nível de usuário.
- Hooking em nível de kernel de um código que opera em nível de usuário torna a análise mais confiável.

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Roteiro

- Emulação x Virtualização
- Engenharia Reversa de Malware
- Prisões e chroot()
- Virtual Machine Introspection
- Kernel Callbacks e Filter Driver Callbacks
- Hooking
  - Usuário
  - Kernel
- Direct Kernel Object Manipulation (DKOM)

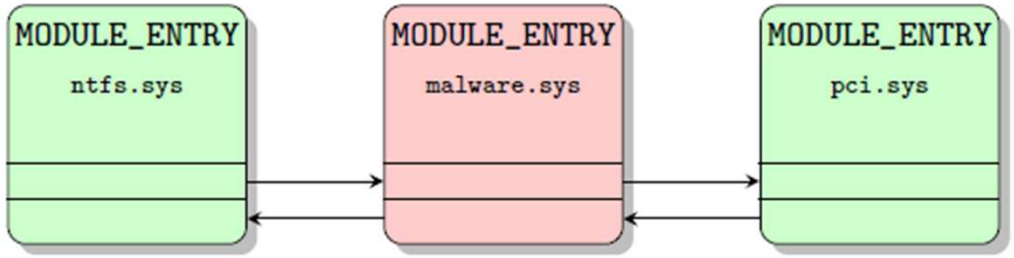
ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

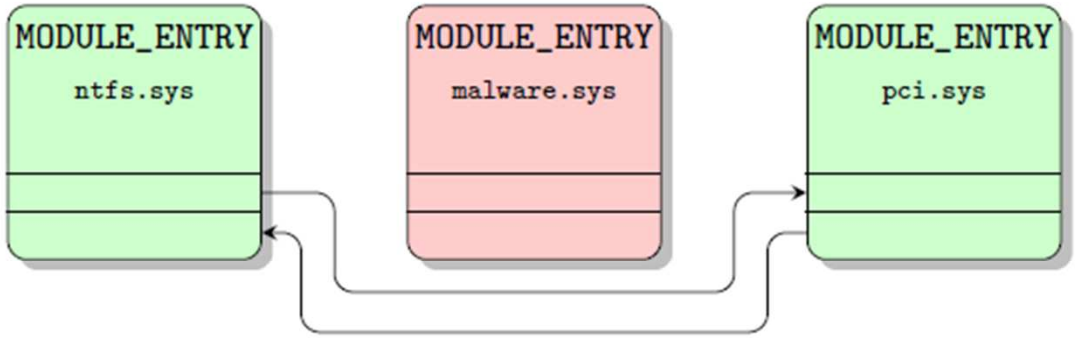
Técnicas de DKOM

- Direct Kernel Object Manipulation (DKOM)
- Kernel é alterado enquanto carregado na memória
- Não há necessidade de patch ou hook
- Objetivo: Software malicioso desaparece da lista de processos ativos

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR




```
C:\WINDOWS> drivers.exe
  ModuleName     Code     Data      Bss    Paged     Init          LinkDate
-------------------------------------
          ...
     ntfs.sys    96000     7040        0   412544    14080   Wed Aug 04 08:15:06 2004
 malware.sys     3903        0        0        0        0   Sat Mar 13 02:22:32 2010
     pci.sys    16000     1664        0    34176     5632   Wed Aug 04 08:07:45 2004
```




```
C:\WINDOWS> drivers.exe
  ModuleName     Code     Data      Bss    Paged     Init          LinkDate
-------------------------------------
          ...
     ntfs.sys    96000     7040        0   412544    14080   Wed Aug 04 08:15:06 2004
     pci.sys    16000     1664        0    34176     5632   Wed Aug 04 08:07:45 2004
```

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Softwares de VMI e Hooking - Exemplos

- Anubis
  - Virtual Machine Introspection (VMI)
  - Windows
- CWSandbox
  - userland hooking
  - Windows
- Cuckoobox
  - inline hooking
  - Windows
- Ether
  - Virtual Machine Introspection (VMI)
  - aplicada ao Xen
- Joebox
  - hooking
    - Userland
    - Kernel
  - Windows
- JSand
  - utiliza um emulador para processar as páginas
  - Análise web
- PhoneyC
  - utiliza um emulador para processar as páginas
  - Análise web
- Capture-HPC
  - Utiliza ambiente virtualizado
  - Análise web
- ReVirt
  - Virtual Machine Introspection (VMI)
  - permite que um investigador reproduza um incidente e retroceda, pause ou avance a VM para um ponto qualquer no tempo
  - reconstrói cada ciclo da CPU

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Softwares de Recuperação de Arquivos - FTK

- Software de análise forense de computador feito pela empresa AccessData
- Faz a varredura de uma unidade de armazenamento procurando por várias informações
  - E-mails
  - Docs
  - Imagens
  - strings específicas

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Softwares de Recuperação de Arquivos – FTK

- Varre o disco e localiza strings que serão usadas em ataques de dicionário
- Utilitário interno: Disk Image
  - Cria imagem de disco
    - Arquivo
    - segmentos
    - outro disco
- Calcula os valores de hash MD5 e confirma a integridade dos dados antes de fechar os arquivos
- Gera relatórios, indexa conteúdo, gera cd imagem com o conteúdo indexado
- Abrange todos os tipos de filesystem

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Softwares de Recuperação de Arquivos – GetDataBack

- Software de análise forense de computador feito pela empresa Runtime Software
- Possui versões específicas para sistemas de arquivos distintos
  - Somente NTFS
  - Somente FAT

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Softwares de Recuperação de Arquivos – Outros

- RStudio
- Easy Recovery
- Encase
- WinHex
- Recuva
- Foremost
- undelete
- Pandora Recovery
- Photorec (Apesar do nome, não é específico para imagens)
- Coroner's Toolkit

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Softwares de Desmontagem

- Windows
  - Win32Program Disassembler
  - IDA PRO
  - Hopper Disassembler
  - OBJ2ASM
  - PE Explorer
  - OllyDbg
  - Capstone
  - BORG Disassembler
- Linux
  - Bastard Disassembler
  - LIDA
  - Ndidasm
  - Verteron Disassembler Engine (VDE)
  - EmilPRO
  - Ldasm
  - Llvm
  - ciasdis

ITnerante
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos

Primeira Bateria de Questões de Aprendizagem

ITnerante

Provas de TI
TUDO PARA VOCÊ PASSAR

1. Acerca dos sistemas operacionais Windows e Linux, julgue os itens abaixo.

[99] O ramo HKEY_LOCAL_MACHINE, nos registros do Windows, contém informações sobre as extensões dos arquivos, associações entre arquivos e aplicativos para suportar a funcionalidade de arrastar/soltar, informações sobre os atalhos do Windows e aspectos centrais da interface do usuário do Windows.

1. Acerca dos sistemas operacionais Windows e Linux, julgue os itens abaixo.

~~[99] O ramo HKEY_LOCAL_MACHINE, nos registros do Windows, contém informações sobre as extensões dos arquivos, associações entre arquivos e aplicativos para suportar a funcionalidade de arrastar/soltar, informações sobre os atalhos do Windows e aspectos centrais da interface do usuário do Windows.~~

2. Sobre MS Windows Server 2003, assinale a alternativa correta.

A. Todos os serviços devem ser inicializados manualmente, por intermédio de comandos no prompt do MS DOS.

B. A base de dados, de usuários registrados, pode ser encontrada na árvore HKEY_CURRENT_CONFIG.

C. O Event Viewer permite visualizar os logs gerados pelo sistema.

D. O Kerberos é utilizado como protocolo de serviço de arquivos.

E. O seu kernel é monolítico e, por isso, os serviços rodam enjaulados pelos usuários do sistema.

3. Sobre a utilização do editor de registros do Sistema Operacional Windows XP Professional (configuração padrão), analise:

I. O Editor do Registro é uma ferramenta avançada para exibir e alterar as configurações no registro do sistema, e que contém informações sobre como o computador deve funcionar.

II. O Editor de Registro do Microsoft Windows pode ser acessado, clicando-se no menu Iniciar - Executar... - msconfig.

III. HKEY_CURRENT_USER: contém a base das informações de configuração para o usuário que estiver conectado no momento. As configurações de pastas, de cores de tela e do painel de controle do usuário são armazenadas aqui. Essas informações são chamadas de perfil do usuário.

IV. HKEY_LOCAL_MACHINE: contém informações sobre o perfil de hardware usado pelo computador local na inicialização do sistema.

Estão corretas apenas as afirmativas:

A. I, II, III, IV
B. I, III
C. I, II, IV
D. I, III, IV
E. I, IV

3. Sobre a utilização do editor de registros do Sistema Operacional Windows XP Professional (configuração padrão), analise:

I. O Editor do Registro é uma ferramenta avançada para exibir e alterar as configurações no registro do sistema, e que contém informações sobre como o computador deve funcionar.

II. O Editor de Registro do Microsoft Windows pode ser acessado, clicando-se no menu Iniciar - Executar... - msconfig.

III. HKEY_CURRENT_USER: contém a base das informações de configuração para o usuário que estiver conectado no momento. As configurações de pastas, de cores de tela e do painel de controle do usuário são armazenadas aqui. Essas informações são chamadas de perfil do usuário.

IV. HKEY_LOCAL_MACHINE: contém informações sobre o perfil de hardware usado pelo computador local na inicialização do sistema.

Estão corretas apenas as afirmativas:

A. I, II, III, IV

B. I, III

C. I, II, IV

D. I, III, IV

E. I, IV

4. Indique corretamente qual das seguintes seções do registro do sistema operacional Windows XP não é armazenada em disco, sendo gerada dinamicamente ao iniciar o computador.

A. HKEY_CURRENT_USER

B. HKEY_CURRENT_CONFIG

C. HKEY_LOCAL_MACHINE\SOFTWARE

D. HKEY_LOCAL_MACHINE\SYSTEM

E. HKEY_CLASSES_ROOT

4. Indique corretamente qual das seguintes seções do registro do sistema operacional Windows XP não é armazenada em disco, sendo gerada dinamicamente ao iniciar o computador.

A. HKEY_CURRENT_USER

B. HKEY_CURRENT_CONFIG

C. HKEY_LOCAL_MACHINE\SOFTWARE

D. HKEY_LOCAL_MACHINE\SYSTEM

E. HKEY_CLASSES_ROOT

5. O registro do Windows contém informações referenciadas continuamente durante a operação, como os perfis de cada usuário, os aplicativos instalados no computador e os tipos de documentos que cada um pode criar, configurações da folha de propriedades para ícones de pastas e aplicativos, o hardware existente no sistema e as portas que são usadas. A chave de registro pré-definida HKEYLOCALMACHINE usada pelo sistema contém

A. a raiz das informações de configuração para o usuário que está conectado no momento.

B. as informações de configuração específicas para o computador (para qualquer usuário).

C. as informações que garantem que o programa correto seja aberto quando se clica no arquivo correspondente usando o Windows Explorer.

D. informações sobre o perfil de hardware usado pelo computador local na inicialização do sistema.

5. O registro do Windows contém informações referenciadas continuamente durante a operação, como os perfis de cada usuário, os aplicativos instalados no computador e os tipos de documentos que cada um pode criar, configurações da folha de propriedades para ícones de pastas e aplicativos, o hardware existente no sistema e as portas que são usadas. A chave de registro pré-definida HKEYLOCALMACHINE usada pelo sistema contém

A. a raiz das informações de configuração para o usuário que está conectado no momento.

B. as informações de configuração específicas para o computador (para qualquer usuário).

C. as informações que garantem que o programa correto seja aberto quando se clica no arquivo correspondente usando o Windows Explorer.

D. informações sobre o perfil de hardware usado pelo computador local na inicialização do sistema.

6. Quando o Registro do sistema Windows XP é acessado de um computador remoto, aparecem somente as chaves predefinidas

A. HKEY_LOCAL_MACHINE e HKEY_CLASSES_ROOT.

B. HKEY_CURRENT_CONFIG e HKEY_LOCAL_MACHINE.

C. HKEY_CURRENT_USER e HKEY_CURRENT_CONFIG.

D. HKEY_ USERS e HKEY_CURRENT_USER.

E. HKEY_ USERS e HKEY_LOCAL_MACHINE

6. Quando o Registro do sistema Windows XP é acessado de um computador remoto, aparecem somente as chaves predefinidas

A. HKEY_LOCAL_MACHINE e HKEY_CLASSES_ROOT.

B. HKEY_CURRENT_CONFIG e HKEY_LOCAL_MACHINE.

C. HKEY_CURRENT_USER e HKEY_CURRENT_CONFIG.

D. HKEY_ USERS e HKEY_CURRENT_USER.

E. HKEY_USERS e HKEY_LOCAL_MACHINE

7. Considere que você está analisando a cópia forense do disco rígido de um computador, com o sistema operacional Windows XP Home Edition instalado, devidamente licenciado e atualizado. Quando você desejar obter informações constantes no registro, irá executar o editor (regedit.exe). Assinale a alternativa que contempla a relação CORRETA entre chave de registro e conteúdo.

A. HKEY_CLASSES_ROOT, chave onde são armazenadas informações relativas ao usuário administrador da máquina.

B. HKEY_USERS, chave onde são armazenadas as informações relativas ao perfil de hardware do equipamento.

C. HKEY_LOCAL_MACHINE, chave onde são armazenadas as informações relativas ao hardware e software instalados no equipamento.

D. HKEY_USERS, chave onde são armazenadas as informações relativas a informações dinâmicas da sessão.

E. HKEY_CLASSES_ROOT, chave onde são armazenadas informações relativas aos usuários locais.

8. No registro do Windows 2000 Server, as associações entre extensões de arquivo e o tipo de arquivo que representam estão contidas na sub-árvore

A. HKEY_USERS.

B. HKEY_CURRENT_USER.

C. HKEY_CURRENT_CONFIG.

D. HKEY_LOCAL_MACHINE.

E. HKEY_CLASSES_ROOT.

8. No registro do Windows 2000 Server, as associações entre extensões de arquivo e o tipo de arquivo que representam estão contidas na sub-árvore

A. HKEY_USERS.

B. HKEY_CURRENT_USER.

C. HKEY_CURRENT_CONFIG.

D. HKEY_LOCAL_MACHINE.

E. HKEY_CLASSES_ROOT.

9. As informações relativas ao perfil do *hardware atual são armazenadas no registro do Windows XP, na subárvore*

A. HKEY_CURRENT_CONFIG.

B. HKEY_LOCAL_HOST.

C. HKEY_CLASSES_ROOT.

D. HKEY_USERS.

E. HKEY_CURRENT_USER

9. As informações relativas ao perfil do *hardware atual são armazenadas no registro do Windows XP, na subárvore*

A. HKEY_CURRENT_CONFIG.

B. HKEY_LOCAL_HOST.

C. HKEY_CLASSES_ROOT.

D. HKEY_USERS.

E. HKEY_CURRENT_USER

10. As associações entre aplicativos e tipos de arquivo são feitas no editor de registro *Regedit do Windows XP por meio da subárvore*

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USER

C. HKEY_LOCAL_MACHINE

D. HKEY_CURRENT_CONFIG

E. HKEY_USERS

10. As associações entre aplicativos e tipos de arquivo são feitas no editor de registro *Regedit do Windows XP por meio da subárvore*

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USER

C. HKEY_LOCAL_MACHINE

D. HKEY_CURRENT_CONFIG

E. HKEY_USERS

GABARITO

1. E
2. C
3. B
4. B
5. B
6. E
7. C
8. E
9. A
10. A

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

Forense para Concursos

Segunda Bateria de Questões de Aprendizagem

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR

1. O utilitário de configuração do sistema é uma forma de gerenciar os programas iniciados com o Windows XP, que pode ser executado, digitando-se o comando, por meio do menu Iniciar > Executar o comando

A. SYSTEM.INI
B. BOOT.INI
C. WIN.INI
D. MSCONFIG
E. REGEDIT

1. O utilitário de configuração do sistema é uma forma de gerenciar os programas iniciados com o Windows XP, que pode ser executado, digitando-se o comando, por meio do menu Iniciar > Executar o comando

A. SYSTEM.INI
B. BOOT.INI
C. WIN.INI
D. MSCONFIG
E. REGEDIT

02. O utilitário do Windows XP que permite que você exiba, procure e altere as configurações no Registro do seu sistema é o:

A. visualizar eventos.
B. gerenciador de dispositivos.
C. regedit.exe
D. cmd.exe
E. svchost.exe

02. O utilitário do Windows XP que permite que você exiba, procure e altere as configurações no Registro do seu sistema é o:

A. visualizar eventos.
B. gerenciador de dispositivos.
C. regedit.exe
D. cmd.exe
E. svchost.exe

03. Utilizando o sistema operacional Windows XP professional, instalação padrão português-Brasil, qual conjunto de teclas (atalho) o usuário deve usar para excluir um arquivo do disco sem que o mesmo vá para lixeira ?

Obs.: A utilização do caractere + é apenas para interpretação.

A. ctrl+shift+delete
B. delete
C. shift+delete
D. ctrl+delete
E. alt+delete

03. Utilizando o sistema operacional Windows XP professional, instalação padrão português-Brasil, qual conjunto de teclas (atalho) o usuário deve usar para excluir um arquivo do disco sem que o mesmo vá para lixeira ?

Obs.: A utilização do caractere + é apenas para interpretação.

A. ctrl+shift+delete
B. delete
C. shift+delete
D. ctrl+delete
E. alt+delete

04. Acerca das aplicações de informática, julgue os itens a seguir

[66] Com o auxílio de aplicativo de recuperação de dados, é possível recuperar arquivo que foi enviado para a lixeira.

04. Acerca das aplicações de informática, julgue os itens a seguir

[66] Com o auxílio de aplicativo de recuperação de dados, é possível recuperar arquivo que foi enviado para a lixeira.

05. Analise as afirmativas a seguir, relativas ao Windows 2000.

1. O Windows 2000 armazena as ocorrências de eventos em quatro tipos de logs: Application Log, Security Log, Webserver Log e System Log.
2. O Event Viewer exibe os seguintes tipos de eventos: Error, Warning, Information, Success Audit e Failure Audit.
3. O único log que pode ser visualizado somente pelos Administradores do sistema é o Security Log, já que todos os demais logs podem ser visualizados por todos os usuários.
4. O Registro é o local onde o Windows 2000 armazena grande parte dos dados relativos às configurações do sistema. Os Administradores podem mudar os dados destas configurações manualmente no registro visando ajustá-los.
5. Os arquivos excluídos da lixeira não poderão ser recuperados pelo Windows.

Assinale a alternativa *correta:*

A. Apenas uma afirmativa está correta.
B. Apenas duas afirmativas estão corretas.
C. Apenas três afirmativas estão corretas.
D. As afirmativas 1, 2, 3, 4 e 5 estão corretas.
E. Apenas quatro afirmativas estão corretas.

05. Analise as afirmativas a seguir, relativas ao Windows 2000.

1. O Windows 2000 armazena as ocorrências de eventos em quatro tipos de logs: Application Log, Security Log, Webserver Log e System Log.
2. O Event Viewer exibe os seguintes tipos de eventos: Error, Warning, Information, Success Audit e Failure Audit.
3. O único log que pode ser visualizado somente pelos Administradores do sistema é o Security Log, já que todos os demais logs podem ser visualizados por todos os usuários.
4. O Registro é o local onde o Windows 2000 armazena grande parte dos dados relativos às configurações do sistema. Os Administradores podem mudar os dados destas configurações manualmente no registro visando ajustá-los.
5. Os arquivos excluídos da lixeira não poderão ser recuperados pelo Windows.

Assinale a alternativa *correta:*

A. Apenas uma afirmativa está correta.
B. Apenas duas afirmativas estão corretas.
C. Apenas três afirmativas estão corretas.
D. As afirmativas 1, 2, 3, 4 e 5 estão corretas.
E. Apenas quatro afirmativas estão corretas.

06. Em relação ao sistema operacional Windows 2000 Professional, em sua configuração padrão, julgue os itens seguintes

[85] Deve-se ter cuidado extremo ao enviar um arquivo para a lixeira, pois, nesse caso, o arquivo será excluído do disco.

06. Em relação ao sistema operacional Windows 2000 Professional, em sua configuração padrão, julgue os itens seguintes

~~[85] Deve-se ter cuidado extremo ao enviar um arquivo para a lixeira, pois, nesse caso, o arquivo será excluído do disco.~~

07. As ferramentas de antivírus devem ser constantemente atualizadas para poder reconhecer os novos códigos maliciosos e as variantes de códigos maliciosos antigos. Dentre as principais formas de camuflagem adotadas pelos códigos maliciosos, podemos destacar a técnica de criptografia para esconder a carga maliciosa e a mutação contínua do código de decriptação com a técnica de ruído. Essas técnicas são utilizadas em conjunto pelo vírus

A. multipartite
B. ofuscado
C. criptográfico
D. oligomórfico
E. polimórfico

07. As ferramentas de antivírus devem ser constantemente atualizadas para poder reconhecer os novos códigos maliciosos e as variantes de códigos maliciosos antigos. Dentre as principais formas de camuflagem adotadas pelos códigos maliciosos, podemos destacar a técnica de criptografia para esconder a carga maliciosa e a mutação contínua do código de decriptação com a técnica de ruído. Essas técnicas são utilizadas em conjunto pelo vírus

A. multipartite
B. ofuscado
C. criptográfico
D. oligomórfico
E. polimórfico

08. Analise as afirmativas a seguir, relativas à reengenharia de sistemas, descompilação de programas, suas técnicas e ferramentas.

1. A descompilação de programas é realizada através de compiladores convencionais, desde que estejam configurados para obter o código fonte do programa em alto nível a partir da compilação do código que foi programado pelo usuário em alguma linguagem de baixo nível (como assembly, por exemplo).
2. Disassembler é o programa utilizado para gerar o código na linguagem assembly a partir do código binário (linguagem de máquina).
3. Win32 Program Disassembler e IDA são exemplos de disassemblers compatíveis com o Windows, enquanto que Bastard Disassembler e LIDA são exemplos de disassemblers compatíveis com o Linux.
4. Os debuggers podem ser utilizados em conjunto com os disassemblers, possibilitando que os desenvolvedores observem o comportamento da CPU durante a execução do código obtido, além de permitir a execução de uma instrução por vez e a definição de breakpoints.
5. A descompilação de programas executáveis obtém código fonte em alto nível, preservando os nomes de variáveis e estruturas de dados presentes no código-fonte utilizado para gerar o programa executável, sempre que o executável for gerado utilizando a funcionalidade de code obfuscation presente em alguns compiladores.

Está(ão) *correta(s):*

A. Apenas uma afirmativa está correta.
B. Apenas duas afirmativas estão corretas.
C. Apenas três afirmativas estão corretas.
D. Apenas quatro afirmativas estão corretas
E. As afirmativas 1, 2, 3, 4 e 5 estão corretas.

08. Analise as afirmativas a seguir, relativas à reengenharia de sistemas, descompilação de programas, suas técnicas e ferramentas.

1. A descompilação de programas é realizada através de compiladores convencionais, desde que estejam configurados para obter o código fonte do programa em alto nível a partir da compilação do código que foi programado pelo usuário em alguma linguagem de baixo nível (como assembly, por exemplo).
2. Disassembler é o programa utilizado para gerar o código na linguagem assembly a partir do código binário (linguagem de máquina).
3. Win32 Program Disassembler e IDA são exemplos de disassemblers compatíveis com o Windows, enquanto que Bastard Disassembler e LIDA são exemplos de disassemblers compatíveis com o Linux.
4. Os debuggers podem ser utilizados em conjunto com os disassemblers, possibilitando que os desenvolvedores observem o comportamento da CPU durante a execução do código obtido, além de permitir a execução de uma instrução por vez e a definição de breakpoints.
5. A descompilação de programas executáveis obtém código fonte em alto nível, preservando os nomes de variáveis e estruturas de dados presentes no código-fonte utilizado para gerar o programa executável, sempre que o executável for gerado utilizando a funcionalidade de code obfuscation presente em alguns compiladores.

Está(ão) *correta(s):*

A. Apenas uma afirmativa está correta.
B. Apenas duas afirmativas estão corretas.
C. Apenas três afirmativas estão corretas.
D. Apenas quatro afirmativas estão corretas
E. As afirmativas 1, 2, 3, 4 e 5 estão corretas.

09. Em relação às técnicas de computação forense, assinale a alternativa correta.

A. O processo de investigação forense envolve técnicas Live Analysis, que têm como premissa a preservação de todas as evidências armazenadas nos discos rígidos e outras mídias.

B. Em uma perícia forense computacional, pode-se realizar a análise de artefatos ligados (Live Analysis), análise de artefatos desligados (Post Mortem Analysis), porém não é recomendado fazer uma análise de pacotes trocados entre o artefato e outros dispositivos de rede (Network Analysis), pois neste caso não é possível coletar dados com prova legal.

C. Um elemento importante em qualquer investigação de tipo forense é a manutenção da "cadeia de custódia", que consiste em salvaguardar a amostra (dados digitais), de forma documentada, de modo a que não se possa alegar que foi modificada ou alterada durante o processo de investigação. A garantia da integridade dos dados digitais coletados requer a utilização de ferramentas que aplicam algum tipo de algoritmo hash.

D. Como a cópia bit-a-bit dos dados (imagem) necessita mais espaço de armazenamento e consome muito mais tempo para ser realizada, uma boa prática na coleta de dados da perícia forense é fazer somente uma cópia lógica (backup) dos dados não voláteis.

E. Um perito forense pode utilizar diversas ferramentas computacionais para coleta de dados (p.ex. o Disk Definition - dd), para exame dos dados (p.ex. Encase, Autopsy); porém, não existem ferramentas que auxiliam a análise dos dados. A correta execução da etapa de análise depende exclusivamente da experiência e o conhecimento técnico do perito.

09. Em relação às técnicas de computação forense, assinale a alternativa correta.

A. O processo de investigação forense envolve técnicas Live Analysis, que têm como premissa a preservação de todas as evidências armazenadas nos discos rígidos e outras mídias.

B. Em uma perícia forense computacional, pode-se realizar a análise de artefatos ligados (Live Analysis), análise de artefatos desligados (Post Mortem Analysis), porém não é recomendado fazer uma análise de pacotes trocados entre o artefato e outros dispositivos de rede (Network Analysis), pois neste caso não é possível coletar dados com prova legal.

C. Um elemento importante em qualquer investigação de tipo forense é a manutenção da "cadeia de custódia", que consiste em salvaguardar a amostra (dados digitais), de forma documentada, de modo a que não se possa alegar que foi modificada ou alterada durante o processo de investigação. A garantia da integridade dos dados digitais coletados requer a utilização de ferramentas que aplicam algum tipo de algoritmo hash.

D. Como a cópia bit-a-bit dos dados (imagem) necessita mais espaço de armazenamento e consome muito mais tempo para ser realizada, uma boa prática na coleta de dados da perícia forense é fazer somente uma cópia lógica (backup) dos dados não voláteis.

E. Um perito forense pode utilizar diversas ferramentas computacionais para coleta de dados (p.ex. o Disk Definition - dd), para exame dos dados (p.ex. Encase, Autopsy); porém, não existem ferramentas que auxiliam a análise dos dados. A correta execução da etapa de análise depende exclusivamente da experiência e o conhecimento técnico do perito.

10. Sobre obtenção de informações forenses em mídias magnéticas e sólidas, assinale a alternativa INCORRETA.

A. É impossível executar a análise forense de um dispositivo do tipo pen drive com o sistema de alocação FAT 32 de 128 MB de capacidade de armazenamento, que não está protegido por senha ou sistemas de criptografia.

B. Um disquete de três e meia polegadas, em perfeito estado de conservação, é passível de duplicação forense de seu conteúdo.

C. É possível a análise forense do conteúdo da memória de trabalho de um computador que esteja em funcionamento.

D. O procedimento de análise forense do conteúdo da memória volátil de um computador em utilização é chamado de "despejo" de memória e pode ser executado a partir da aplicação de diversas ferramentas forenses existentes no mercado.

E. A inicialização controlada e o espelhamento são os nomes de duas técnicas de análise forense

GABARITO

1. D
2. C
3. C
4. C
5. E
6. E
7. E
8. C
9. C
10. A
11. A

ITnerante

PROVAS DE TI
TUDO PARA VOCÊ PASSAR