MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
DIRETORIA DE ENSINO (DIREN)
DEPARTAMENTO DE ENSINO SUPERIOR (DEPES)
DEPARTAMENTO DE INFORMÁTICA (DEPIN)
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO (BCC)

DEPARTAMENTO	PLANO DE CURSO DA DISCIPLINA
CCGBCC – Coordenação do Curso de Bacharelado em Ciência da Computação	**Fundamentos de Análise de Softwares Maliciosos**

CÓDIGO	PERÍODO	ANO	SEMESTRE	PRÉ-REQUISITOS
GCC1944	N/A	2012	2	GCC 1103 Projeto de Algoritmos Computacionais GCC 1205 Sistemas Operacionais

CRÉDITOS	AULAS/SEMANA			TOTAL DE AULAS NO SEMESTRE
	TEÓRICA	PRÁTICA	ESTÁGIO	
4	4	0	0	72

EMENTA

Introdução a Análise de Malware. Análise Estática. Análise Comportamental. Introdução às Arquiteturas x86 e x86-64. Análise Estática de Código Utilizando Disassembler. Análise Dinâmica de Código Utilizando um Debugger. Funcionalidades Desempenhadas por Malwares. Métodos de Persistência Utilizados Por Malwares. Injeção de Código e Hooking. Técnicas de Ofuscação.

BIBLIOGRAFIA

Bibliografia básica

1. K A, Monnappa, Learning Malware Analysis: Packt, 2018.
2. Barker, Dylan. Malware Analysis Techniques: Packt, 2021.
3. Kleymenov, Alexey; Thabet, Amr. Mastering Malware Analysis: Packt, 2019.

Bibliografia complementar

1. Sikorski, Michael; Honig, Andrew. Practical Malware Analysis: no starch press, 2012.
2. Mohanta, Abhijit; Saldanha, Anoop. Malware Analysis and Detection Engineering: Apress, 2020.
3. Eagle, Chris; Nance, Kara. The Ghidra Book: no starch press, 2020.
4. Andriesse, Dennis. Practical Binary: no starch press, 2019
5. Gazet, Bruce Dang; Bachaalany, Elias. Practical Reverse Engineering: Wiley, 2014
6. Mercês, Fernando. Fundamento de Engenharia Reversa. Disponível em https://mentebinaria.gitbook.io/engenharia-reversa/ (Último acesso: 20/05/2022)

OBJETIVO GERAL

Apresentar ao aluno técnicas, metodologias e ferramentas utilizadas para analisar softwares maliciosos.

METODOLOGIA

- Aulas expositivas, com auxílio de recursos audiovisuais
- Estudos de caso com amostras de malwares reais utilizando ambiente de virtualização

CRITÉRIO DE AVALIAÇÃO

No início do curso os alunos serão divididos em grupos. A cada grupo será atribuído um malware real que deverá ser analisado ao longo do curso. Essa análise será dividida em três atividades pontuadas:

1. (RP1) Em grupo, os alunos deverão apresentar, na forma de um relatório parcial, quais informações relevantes foram descobertas durante a fase de análise estática. O relatório deve incluir quais informações podem ser utilizadas como Indicadores de Comprometimento.
2. (RP2) Em grupo, os alunos deverão apresentar, na forma de um relatório parcial, quais informações relevantes foram descobertas durante a fase de análise comportamental.
3. (RF) Por fim, cada aluno deverá produzir, de forma individual, um relatório final que deverá incluir todas as informações obtidas sobre o malware durante o curso.

A média parcial (MP) do aluno será calculada da seguinte maneira:

$$\mathrm{MP} = \mathrm{RP1} * 0{,}25 + \mathrm{RP2} * 0{,}25 + \mathrm{RF} * 0{,}5$$

Segundo o regimento do CEFET-RJ, caso o aluno obtenha média parcial inferior a 3,0 (três e zero) estará reprovado diretamente. Graus MP maiores ou iguais a 7,0 (sete e zero) aprovam diretamente o aluno. Em situações onde o aluno tenha grau MP entre 3,0 inclusive e 7,0 exclusive, terá direito a uma prova final (PF), que, juntamente com a média parcial gerará uma nova média, denominada média final (MF). Essa média é calculada da seguinte forma:

$$MF = (MP + PF) / 2$$

Para ser aprovado, o aluno deve alcançar uma MF maior ou igual a 5,0 (cinco e zero). Caso contrário, estará reprovado, devendo repetir a componente curricular.

CHEFE DO DEPARTAMENTO

NOME	ASSINATURA

PROFESSOR RESPONSÁVEL PELA DISCIPLINA

NOME	ASSINATURA
Igor Cesar Gonzalez Ribeiro	

PROGRAMA

1. Introdução à Análise de Malware
   - 1.1. O que é um malware?
   - 1.2. O que é a análise de malware?
   - 1.3. Por que analisar um malware?
   - 1.4. Tipos de análise de malware
   - 1.5. Configuração do ambiente de laboratório

2. Análise Estática
   2.1. Verificando o tipo de um arquivo
   2.2. Identificando um malware
   2.3. Analisando um malware no VirusTotal
   2.4. Extraindo Strings
   2.5. Determinando Técnicas de Ofuscação
   2.6. Inspecionando Informações do Cabeçalho PE
   2.7. Comparando e Classificando Malwares

3. Análise Comportamental
   3.1. Etapas na Execução da Análise Comportamental
   3.2. Monitoramento do Sistema e da Rede
   3.3. Análise de DLL (Dynamic-Link Library)

4. Introdução à Arquiteturas x86 e x86-64
   4.1. Registradores
   4.2. Instruções de Movimentação de Dados
   4.3. Operações Aritméticas e Lógicas
   4.4. Condições e Instruções de Desvio
   4.5. Loops
   4.6. Funções
   4.7. Arrays e Strings
   4.8. Estruturas

5. Análise Estática de Código Utilizando Disassembler
   5.1. Ferramentas de Análise de Código
   5.2. Analisando a API do Windows
   5.3. Patching de Binários
   5.4. Automatização com Scripts

6. Análise Dinâmica de Código Utilizando um Debugger
   6.1. Anexando um processo ao debugger
   6.2. Controlando a Execução de um Processo
   6.3. Interrompendo a Execução com Breakpoints
   6.4. Realizando Tracing de um Programa
   6.5. Analisando Malware em um Debugger

7. Funcionalidades Desempenhadas por Malwares
   7.1. Downloader
   7.2. Dropper
   7.3. Keylogger
   7.4. Replicação via Mídia Removível
   7.5. Comando e Controle (C2)

8. Métodos de Persistência Utilizados Por Malwares
   8.1. Chave de Registro Run
   8.2. Tarefas Agendadas
   8.3. Diretório de Inicialização
   8.4. Entradas de Registro Winlogon
   8.5. Image File Execution Options
   8.6. Programas de Acessibilidade
   8.7. AppInit_DLLs
   8.8. DLL Search Order Hijacking
   8.9. COM Hijacking
   8.10. Serviços

9. Injeção de Código e Hooking
   9.1. Visão Geral sobre Memória Virtual
   9.2. Modos de Operação e Chamadas de Sistema no Windows
   9.3. Técnicas de Injeção de Código
   9.4. Técnicas de Hooking

10. Técnicas de Ofuscação
   10.1. Encoding simples
   10.2. Criptografia do Malware
   10.3. Encoding Personalizado
   10.4. Malware Unpacking