**2º. SEMESTRE DE 2012**

|  |
| --- |
| **Identificação do Aluno:**  **Álvaro Vilobaldo Rios da Silva** |
| **Orientador(A):**  **Ivete Irene dos Santos** |
| **Tema Proposto:**  **antiforense** |
| **Justificativa:**  *Orientações: Na justificativa busca-se colocar, de maneira clara e objetiva, quais são os elementos teórico-práticos que demonstram a relevância para a realização da pesquisa, bem como as possíveis contribuições resultantes do trabalho proposto.*  Por que invadir um país armado arriscando vidas de centenas se você pode destruir centrífugas de enriquecimento de urânio de forma sigilosa do outro lado do planeta? Conforme o mundo se digitalizou se digitalizaram-se também as suas ameaças, onde antes se podia ver mesmo que por instantes mísseis ou bombas sendo lançada hoje temos inúmeras ameaças invísiveis que podem causar tanto estrago quanto, contudo pelo príncipio de Locard o problema dessas ameaças invisíveis é que elas podem não ser tão invisíveis assim, levando a procura de metodos antiforense mais eficazes.  O perito deve estar preparado para a ação de um usuário avançado que conheça bem o sistema operacional atacado,comprometido ou usado. Mesmo que não seja algo corriqueiro na rotina da grande maioria dos profissionais, encontrar um atacante de alto nível trará novos desafios e obstáculos tão poucos corriqueiros. Saber como dificultar ou impossibilitar o trabalho do perito é como ele poderá evitar a armadilha de achar que no corpo (corpo de delito) investigado não existe nada.  Sendo assim, esse trabalho poderá ajudar a traçar um processo bem elaborado de trabalho que seja rápida e eficiente sem deixar brechas que permitam ou ajudem ações antiforenses. Com um processo bem definido o perito tende a diminuir o tempo de análise e um melhor aproveitamento das mesmas. Provendo mais qualidade com mais precisão. |
| **O Problema de Pesquisa:** *(definir o problema na forma de uma pergunta)*  *Orientações: O problema de pesquisa constitui a questão central a ser respondida pela pesquisa e deve ser coerente com os objetivos propostos, bem como apresentar relação com a justificativa desenvolvida.*  Técnicas podem ser usadas para ocultar processos ou ações. Para definir e estabelecer padrões de análise e melhorar os procedimentos de detecção da ação de um atacante avançado, é preciso enter como e o que ele pode fazer.  Qual a questão de pesquisa? Você apresentou o problema, mas esse será o foco da pesquisa formule a questão de pesquisa. |

|  |
| --- |
| **OBJETIVOS**  **Objetivos Gerais:**  *Orientações: É necessário apresentar o objetivo geral da pesquisa, ou seja, a meta proposta para a investigação, que deve ser coerente com a questão de pesquisa.*  Apresentar o funcionamento de rootkits voltados para antiforense.  **Objetivos Específicos:**  *Orientações: De forma complementar, os objetivos específicos, também presentes nesse item, constituem as etapas de trabalho que permitem alcançar o objetivo geral. Como os objetivos traduzem ações que serão executadas ao longo da pesquisa; a apresentação destes no texto requer a utilização de verbos no infinitivo.*  Expor o que é um rootkit;  Como o rootikit pode impedir a formação de provas;  Mostrar o que ele pode fazer usando se possível com exemplos reais;  Desenvolver em cima da análise do funcionamento do rootkit e do seu potencial fatores que devem ser levados em conta antes de qualquer análise; e  Contemplar o trabalho com um estudo de caso. |
| **Delimitações do Estudo:**  *Orientações: Apresentar o recorte estabelecido para a pesquisa.O foco.*  Análise de rootkits em ambientes Windows 7 voltados para restringir ou destruir provas. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TIPO DE PESQUISA CIENTÍFICA**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   |  | | --- | | ******Quanto à sua Natureza**  **( ) Pesquisa Pura** *Busca ampliação do conhecimento através do Método Científico, sem preocupação quanto à sua aplicabilidade prática.*  **( x ) Pesquisa Aplicada**  *Busca a solução de problemas práticos através do Método Científico.* | | ******Quanto à Forma de Abordagem do Problema**  **( ) Pesquisa Quantitativa** *Baseada em cálculos e medidas objetivas.*  **( x ) Pesquisa Qualitativa** *É de caráter mais subjetivo. Há predomínio de classificações e análises dissertativas.* | | ******Quanto aos Fins**  **( x ) Pesquisa Exploratória** *Busca familiaridade com o problema. Visa explicitar o problema ou construir hipóteses.*  **( ) Pesquisa Descritiva** *Busca descrever as características de um fenômeno. Pode buscar também estabelecer relações entre variáveis.*  **( ) Pesquisa Explicativa** *Busca identificar os fatores que determinam ou contribuem para a ocorrência de algum fenômeno.*  **( ) Pesquisa Metodológica** *Voltada para caminhos, formas, maneiras e procedimentos para atingir um determinado fim.*  **FINS PRÁTICOS**  **( ) Pesquisa de Avaliação** *Análise de programas, projetos, políticas, etc., para verificar sua efetividade.*  **( ) Pesquisa Diagnóstico** *Busca nortear o caminho a ser seguido por uma Organização em relação a um dado assunto.*  **( ) Pesquisa Propositiva:** *Propõe planos, programas, política, projetos, metodologias, etc., associadas a um assunto.* | | ******Quanto aos Meios**  **( ) Pesquisa Bibliográfica** *Busca conhecimento na literatura sobre um assunto em estudo.*  **( ) Pesquisa Documental** *Baseada na consulta a documentos de Organizações.*  **( x ) Estudo de Caso** *Estudo investigativo profundo envolvendo uma ou mais Organizações.*  **( ) Pesquisa de Laboratório** *Experiência realizada em local delimitado, sob condições de laboratório.*  **( ) Pesquisa de Campo** *Levantamento de dados no local onde ocorre o fenômeno em estudo.* | | **Justificativa:** *Orientações: Apresentar as justificativas pertinentes aos tipos de pesquisa assinalados nos* ***quatro*** *conjuntos de opções anteriores.* | |

**CRONOGRAMA DE ATIVIDADES**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ATIVIDADE | MÊS | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 |
| Apresentar as ações para o desenvolvimento da pesquisa  Exemplos:  -Levantamento bibliográfico  -Fichamento das obras  -Revisão do projeto  -Entrevistas???  -Teste ?  -Escrita do capítulo 1 sobre...  -Escrita do capítulo 2 sobre....  Etc etc...  -Revisão da monografia... |  |  |  |  |  |  |