4º EPEX
ENCONTRO DE ENSINO, PESQUISA E EXTENSÃO
4° EGRAD – ENCONTRO DE ENSINO DE GRADUACÃO
11° ENIC – ENCONTRO DE INICIACÃO CIENTÍFICA
11° SEMEX – SEMINÁRIO DE EXTENSÃO UNIVERSITÁRIA

ANÁLISE DE COMPORTAMENTO DE *EXPLOITS* LOCAIS

Leandro Machado Siqueira[1]; Fabrício Sérgio de Paula[2]

[1]Aluno do curso de Ciência da Computação, bolsista da UEMS; [2]Professor do curso de Ciência da Computação.

RESUMO

Esta pesquisa contém a análise de *exploits* utilizados em ataques locais com objetivo de conhecer quais as principais técnicas empregadas durante os ataques. Toda a parte de análise do projeto só foi possível de se realizar graças ao ambiente seguro e isolado, o qual foi proporcionado pela máquina virtual VirtualBox. As execuções desses *exploits* foram monitoradas usando as ferramentas *strace* e *ltrace*. Para tornar possível a execução dos *shellcode* contidos nos *exploits* locais foi criado um programa auxiliar o qual foi compilado da seguinte maneira "gcc -z execstack -o teste teste.c", este método de compilação tornou possível a execução de programas sobre a pilha do sistema operacional Linux. Foram analisados os *exploits* locais conhecidos como *Buffer Overflow*, o mesmo ocorre quando um determinado programa que está sendo executado, tenta escrever dados em uma parte indevida da memória, deste modo, ao invés de apontar para uma parte indevida da memória e devolver o controle ao SO o *exploit* desvia o ponteiro para o programa invasor, o qual passa a obter o controle. Durante a análise desses *exploits* pôde-se concluir que todos executam as chamadas ao sistema *access*, *close*, *open*, *fstat* e *execve*, sendo as quatro primeiras relacionadas com arquivos, diretórios e *links* e a última referente a processos no sistema.

Palavras-chave: *Malware*, Ataque, Segurança.