**FACULDADE METROCAMP**

**ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

**SEGURANCA E AUDITORIA DA INFORMACAO**

**DEMONSTRANDO O USO DO KALI LINUX PARA ATACAR OUTRA MAQUINA**

**PROFESSOR: CYRO CIOLFI**

**Danilo Cesar Missio RA — 42207662861**

**Gabriel Piccolo RA — 41416446842**

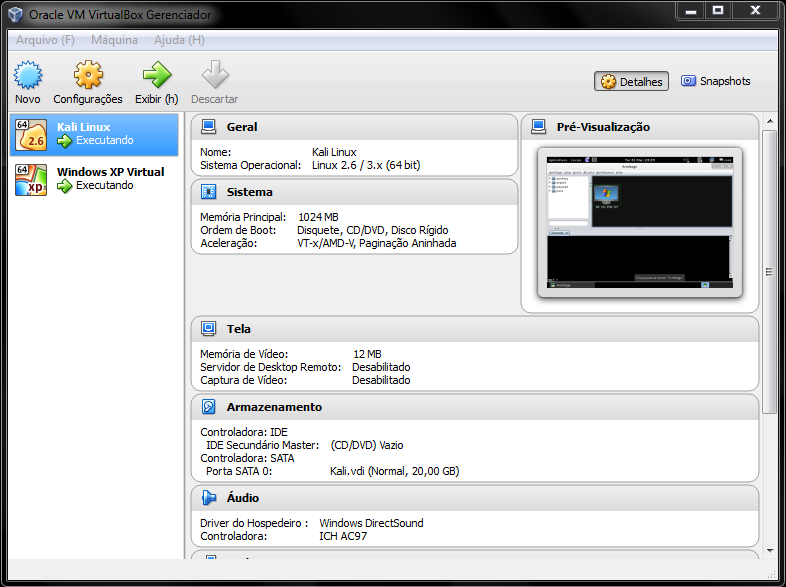
**Pedro Gimenes RA — 3998934869**

**Vinícius Romão RA — 38737711873**

**CAMPINAS**

**01/04/2015**

1. **Montando as maquinas virtuais, uma para o Kali Linux (Invasor) e outra para o Windows XP (Vitima):**



**OBS:** Software utilizado para criação das maquinas virtuais: VirtualBox (Oracle).

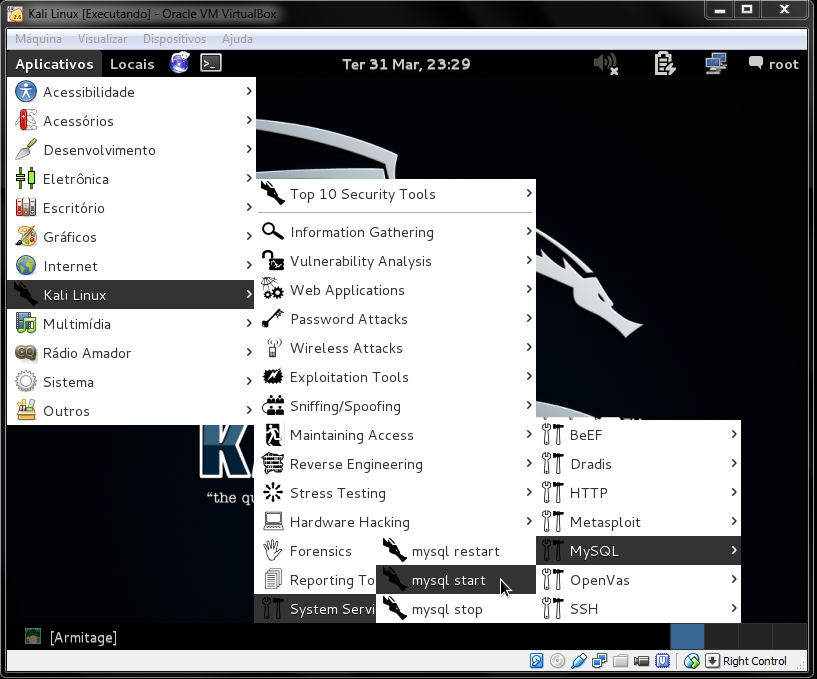
* **Tela da máquina virtual do Kali Lixux**

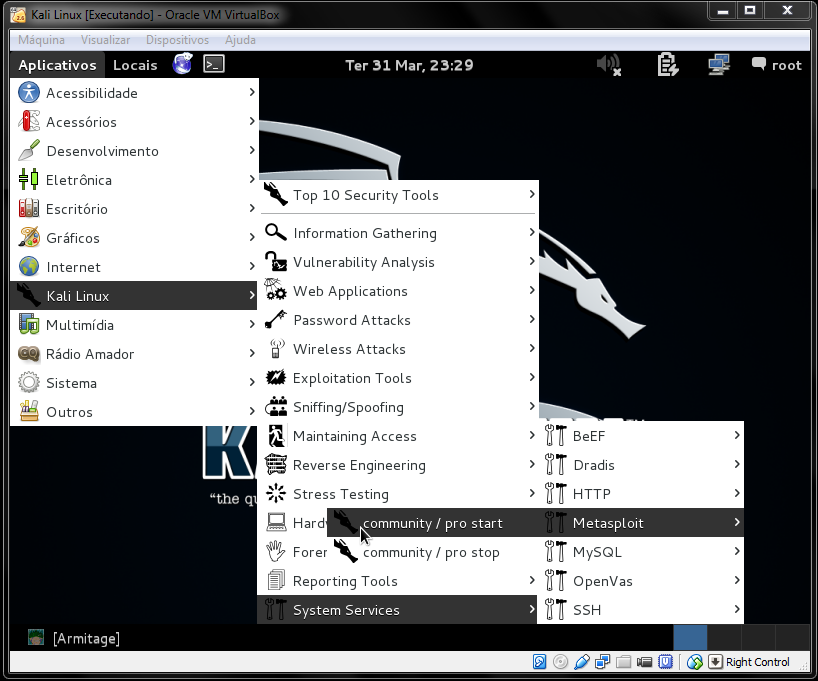
****

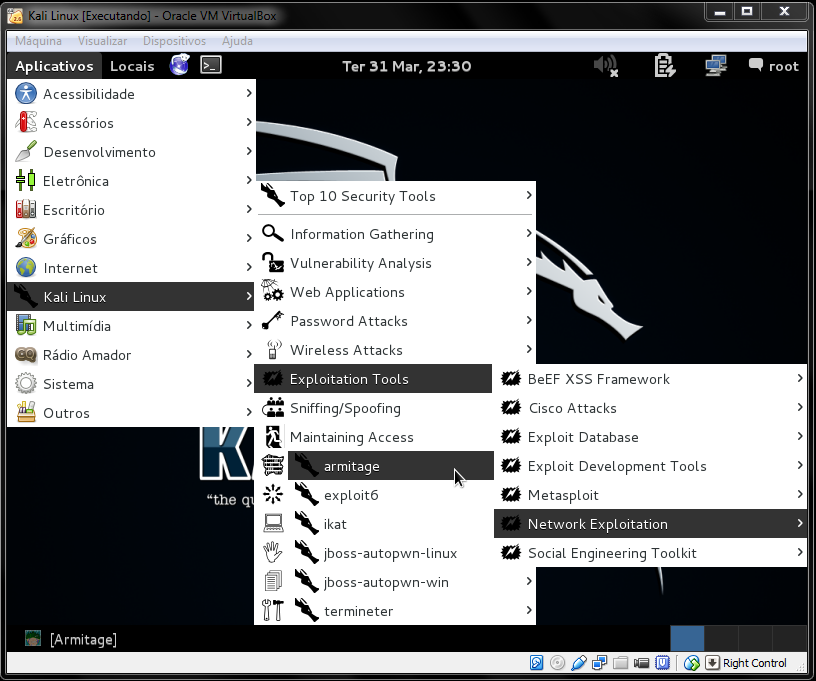
* **Tela da máquina virtual do Windows XP**



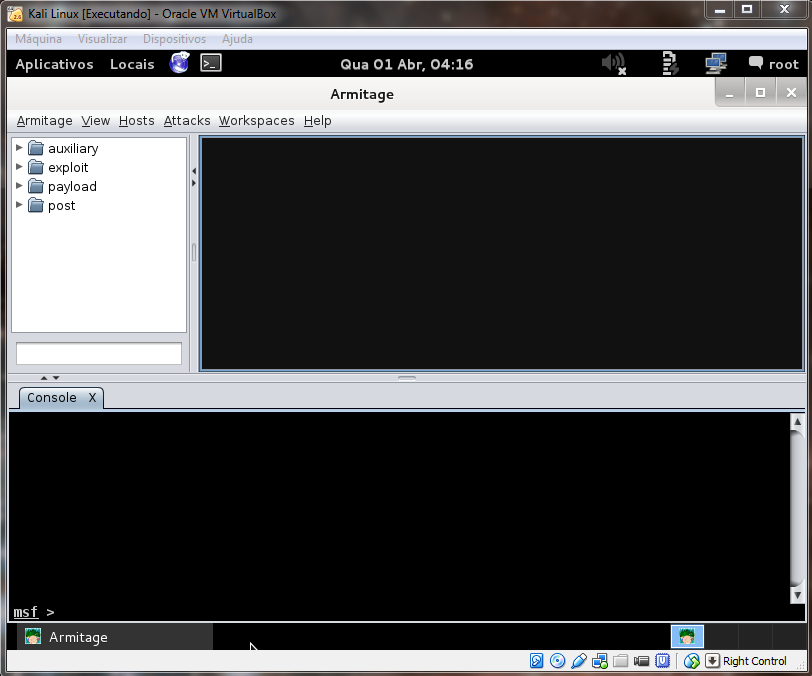
1. **Inicializando o Armitage para atacar o Windows Xp**

****

****

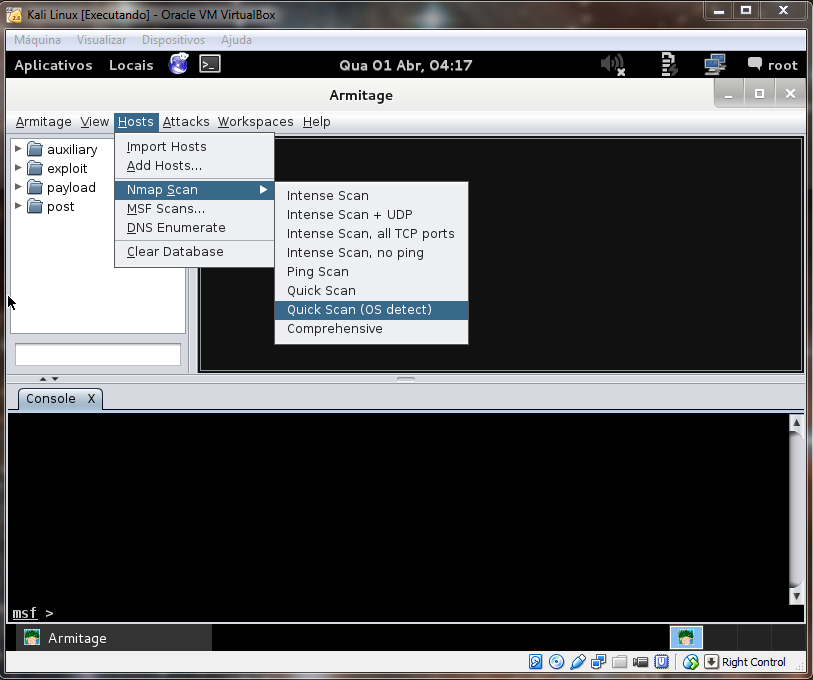
****

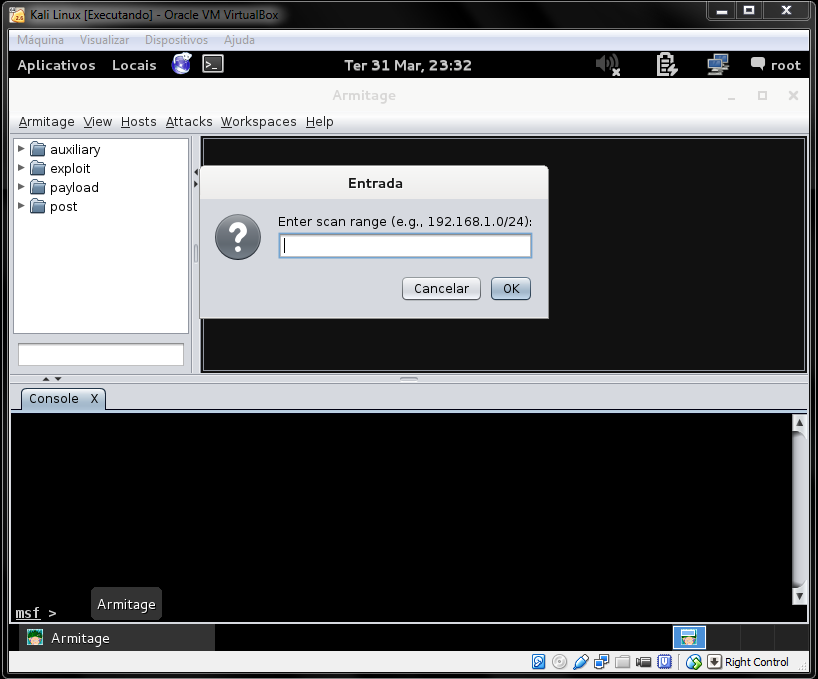
**Armitage iniciado**

****

A aplicação **Armitage** tem como regra para o seu funcionamento que o MySQL e o Metasploit sejam inicializados.

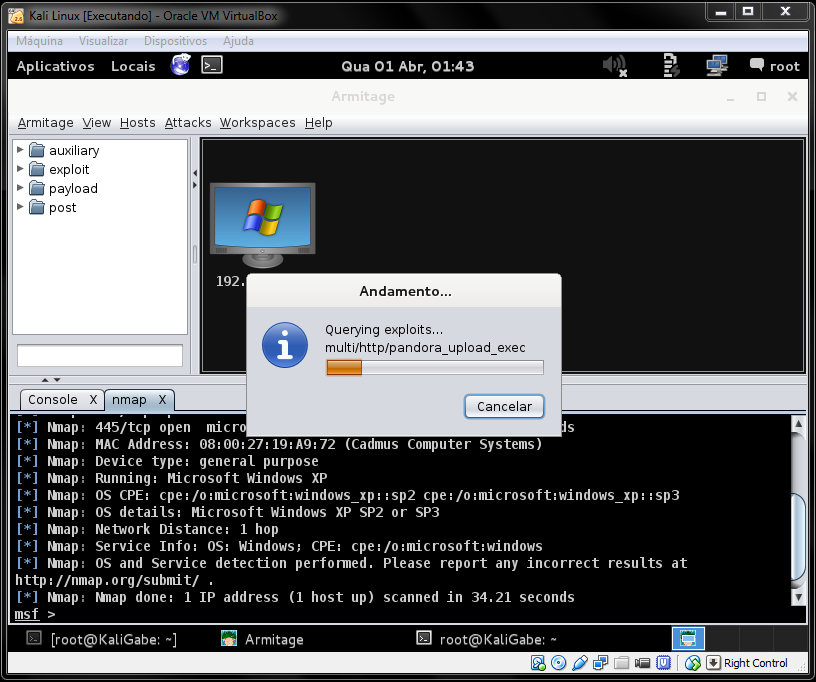
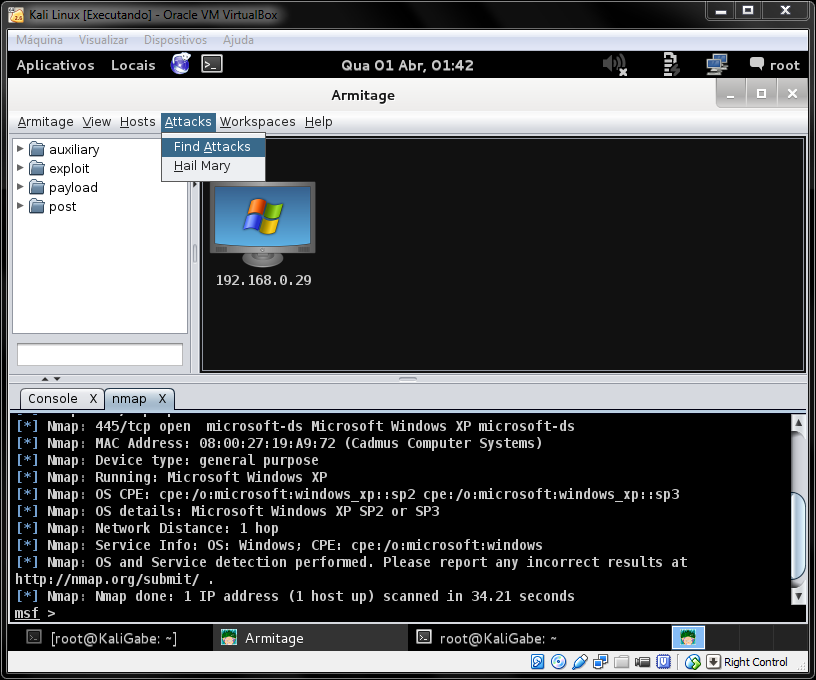
1. **Verificação se o IP da máquina alvo é valido**

****

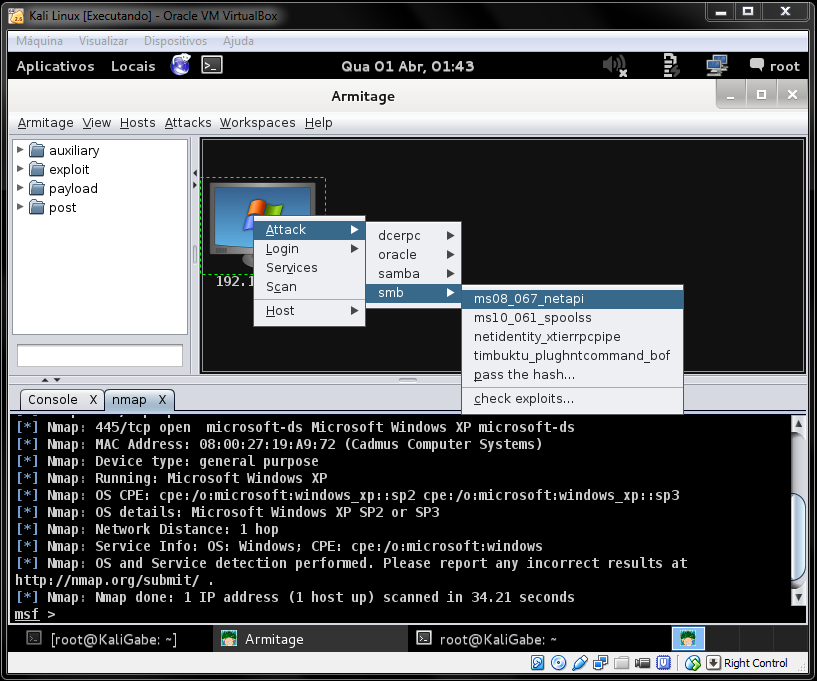
****

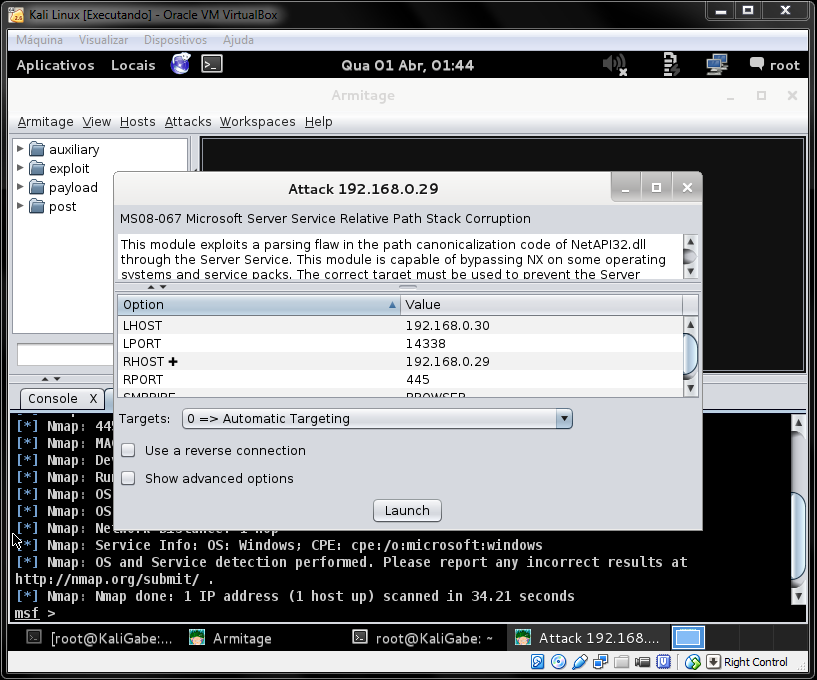
Logo após a tela do **Armitage** abrir, é necessário verificar se o IP da máquina alvo é valido e qual é o sistema operacional utilizado para iniciar uma conexão com o invasor, utilizando o Quick Scan (OS Detected).

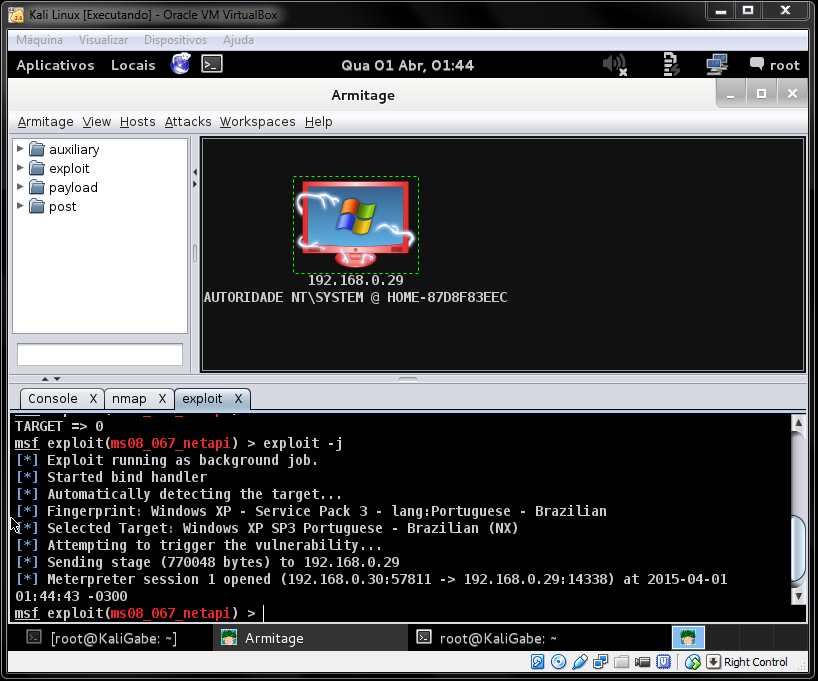
1. **Carregando exploits (vulnerabilidades) para saber quais são os tipos de ataques disponíveis no alvo**

****

1. **Iniciando o ataque/invasão na máquina alvo**

****

****

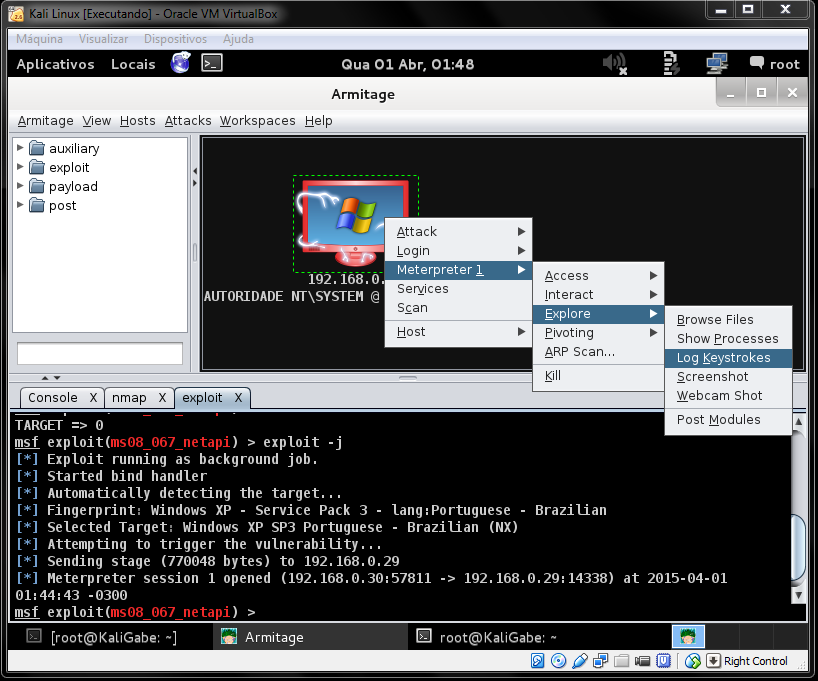
****

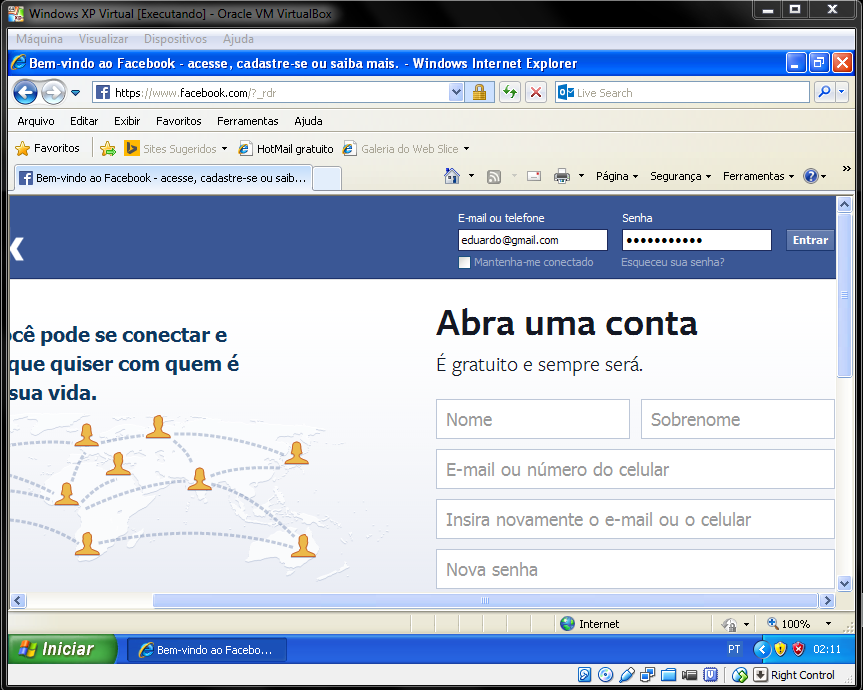
Para efetuar o ataque utilizamos a maneira mais usual, via **SMB** (*Server Message Block*, serviço que é usado principalmente para fornecer acesso compartilhado a arquivos, impressoras, portas seriais e comunicações diversas entre os nós de uma rede) com o exploit de Windows **MS08\_067\_NETAPI**,falha que permite ao atacante executar um código remotamente se uma chamada RPC (Remote Procedure Call) for enviada diretamente ao alvo. O nome dessa vulnerabilidade é **MS08\_067** e a **API NetBIOS** é onde o SMB (que atua sobre TCP) é rodado para posteriormente executar vários transportes (UDP e NBF), assim usando o nome de **MS08\_067\_NETAPI** como tarefa no **Armitage**.

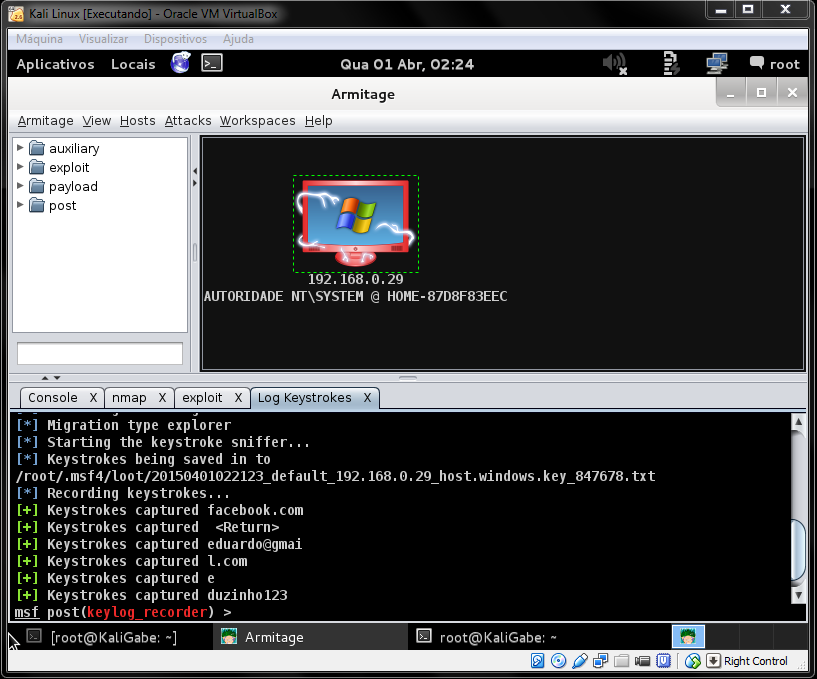
Para detectar se um alvo está com vulnerabilidade no serviço **SMB**, podemos usar de um script para fazer a detecção. Basta chamar o **Nmap** (mostrado no passo 3) para fazer o scan que faz a checagem do **SMB** e verifica se a porta 445 está disponível e vulnerável. Em caso de disponibilidade, a conexão bem sucedida é representada pelo monitor vermelho no **Armitage**.

1. **Exemplos de ataque após invasão bem sucedida**

* **Utilizando Keylogger/keystrokes**

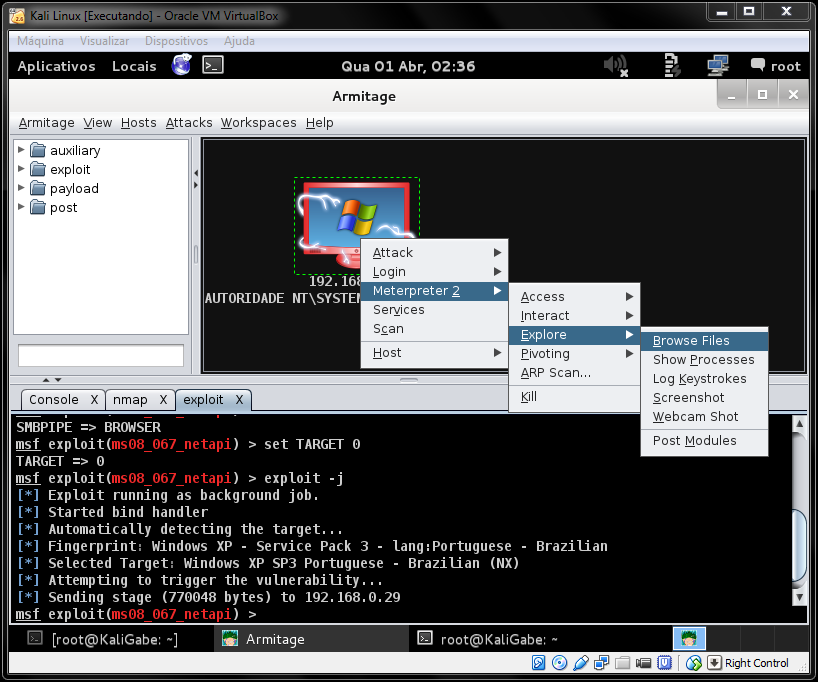
****

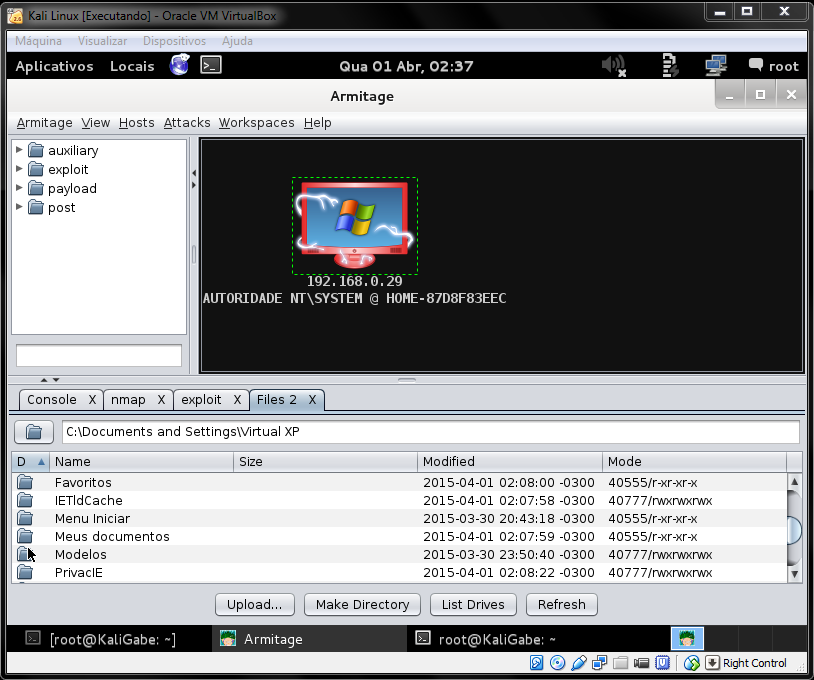


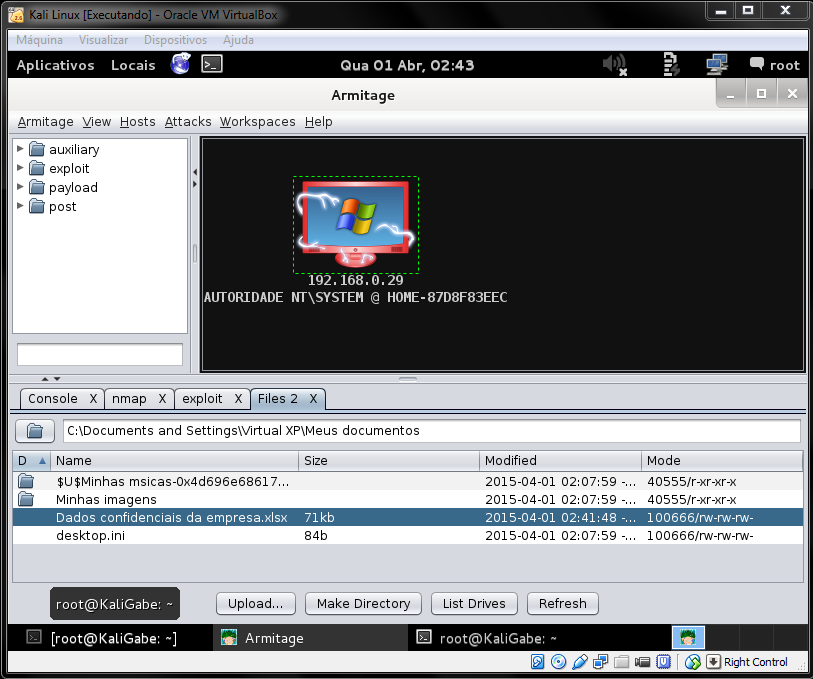
****

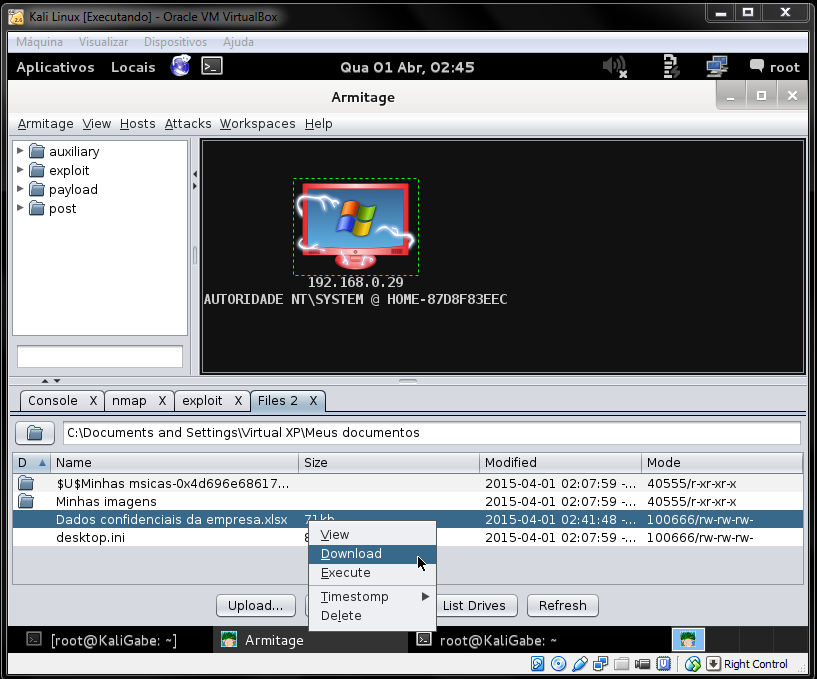
Com a invasão bem sucedida, podemos escolher por exemplo, um ataque por **Keylogger** onde tudo que o usuário digitar será recebido pelo **Armitage** e armazenado (log). No exemplo acima a vítima acessa o site do Facebook para digitar suas informações de credencial. Como podemos notar no log exibido em tempo real, é possível ver todas as informações digitadas na sua esperada sequência (link do website e dados de login e senha).

* **Acessando arquivos da máquina alvo**

****

****

****

****

Nesta opção podemos acessar os arquivos da vítima. É possível navegar entre os diversos diretórios do sistema invadido podendo também fazer o download dos arquivos.