Honeynets: Automatizando a Restauração de Honeypots de Alta Interatividade

Ricardo Makino[1], Luiz Otávio Duarte[1], Renato Yuzo[1]

[1] Divisão de Segurança de Sistemas de Informação
Centro de Tecnologia da Informação Renato Archer
Ministério da Ciência e Tecnologia

GTS.13

Objetivo

Apresentar e discutir algumas soluções que podem ser empregadas na automatização do processo de restauração de *Honeypots* de alta interatividade.

Motivação

Limitada disseminação do uso de *Honeynets* em organizações privadas. Causas:

- Desconhecimento sobre a tecnologia;
- **Manutenção, alta demanda de RH em esforços efetivos;**
- **Necessidade de mão de obra qualificada.**

Motivação

Limitada disseminação do uso de *Honeynets* em organizações privadas. Causas:

- Desconhecimento sobre a tecnologia;
- Manutenção, alta demanda de RH em esforços efetivos;
- Necessidade de mão de obra qualificada.

Motivação

Limitada disseminação do uso de *Honeynets* em organizações privadas. Causas:

- Desconhecimento sobre a tecnologia;
- **Manutenção, alta demanda de RH em esforços efetivos;**
- Necessidade de mão de obra qualificada.

Motivação

Limitada disseminação do uso de *Honeynets* em organizações privadas. Causas:

- Desconhecimento sobre a tecnologia;
- **Manutenção, alta demanda de RH em esforços efetivos;**
- **Necessidade de mão de obra qualificada.**

Honeynets e *Honeypots*

- *Honeypots*;
  - Alta Interatividade;
  - Baixa Interatividade.
- *Honeynets*.

Honeynets e *Honeypots*

- *Honeypots*;
  - Alta Interatividade;
  - Baixa Interatividade.
- *Honeynets*.

Honeynets e *Honeypots*

- *Honeypots*;
  - Alta Interatividade;
  - Baixa Interatividade.
- *Honeynets*.

Restauração de Sistemas

Restaurar: (lat restaurare) vtd 1 Instaurar de novo. vtd 2 Repor no primitivo estado. vpr 3 Restabelecer-se. vtd 4 Tornar a pôr em vigor. vtd 5 Dar novo esplendor a. vtd 6 Consertar, reparar, retocar. vtd 7 Restituir ao poder. vtd 8 *Inform* Retornar um arquivo a sua condição inicial antes de qualquer modificação ser efetuada. ***Fonte:*** *Michaelis*

Métodos de Restauração

Existem diversos métodos de restauração de Sistemas Operacionais.

- Congelamento de Estado
  - Funciona criando um ponto de restauração do sistema revertendo arquivos de configuração, arquivos e programas.
- Imagem
  - Funciona através da realização de imagens do disco, partição ou sistema de arquivos, dessa forma podendo restaurar o computador a um estado anterior.
- Virtual Twin OS
  - Cria um sistema operacional virtual gêmeo onde as alterações executadas no Sistema Operacional são aplicadas apenas ao sistema virtual.

Métodos de Restauração

Existem diversos métodos de restauração de Sistemas Operacionais.

- Congelamento de Estado
  - Funciona criando um ponto de restauração do sistema revertendo arquivos de configuração, arquivos e programas.
- Imagem
  - Funciona através da realização de imagens do disco, partição ou sistema de arquivos, dessa forma podendo restaurar o computador a um estado anterior.
- Virtual Twin OS
  - Cria um sistema operacional virtual gêmeo onde as alterações executadas no Sistema Operacional são aplicadas apenas ao sistema virtual.

Métodos de Restauração

Existem diversos métodos de restauração de Sistemas Operacionais.

- Congelamento de Estado
  - Funciona criando um ponto de restauração do sistema revertendo arquivos de configuração, arquivos e programas.
- Imagem
  - Funciona através da realização de imagens do disco, partição ou sistema de arquivos, dessa forma podendo restaurar o computador a um estado anterior.
- Virtual Twin OS
  - Cria um sistema operacional virtual gêmeo onde as alterações executadas no Sistema Operacional são aplicadas apenas ao sistema virtual.

Métodos de Restauração

Existem diversos métodos de restauração de Sistemas Operacionais.

- Congelamento de Estado
  - Funciona criando um ponto de restauração do sistema revertendo arquivos de configuração, arquivos e programas.
- Imagem
  - Funciona através da realização de imagens do disco, partição ou sistema de arquivos, dessa forma podendo restaurar o computador a um estado anterior.
- Virtual Twin OS
  - Cria um sistema operacional virtual gêmeo onde as alterações executadas no Sistema Operacional são aplicadas apenas ao sistema virtual.

Ferramentas Atuais

Atualmente existem diversas ferramentas, tanto em *Hardware* como em *Software* para restaurar sistemas entre elas:

- *ShadowUser Professional*;
- *Symantec Ghost*;
- *Deep Freeze*;
- *Acronis True Image*;
- *HDD Sheriff*;
- *EWF*;
- *g4u (Ghost for Unix)*.

Ferramentas Atuais

Atualmente existem diversas ferramentas, tanto em *Hardware* como em *Software* para restaurar sistemas entre elas:

- *ShadowUser Professional*;
- *Symantec Ghost*;
- *Deep Freeze*;
- *Acronis True Image*;
- *HDD Sheriff*;
- *EWF*;
- *g4u (Ghost for Unix)*.

Requisitos Interessantes

Para um sistema de restauração de *Honeypots* são requisitos interessantes:

- Execução sem interação com usuário e remota para o armazenamento ou restauração do Sistema Operacional.
- Adição de scripts para modificar o ambiente a seu gosto;
- Baixo custo de implantação do ambiente;
- Solução independente do Sistema Operacional do *Honeypot*;
- Funcionamento em diferentes tipos de hardwares, sem a necessidade do uso de tecnologias específicas.

Requisitos Interessantes

Para um sistema de restauração de *Honeypots* são requisitos interessantes:

- Execução sem interação com usuário e remota para o armazenamento ou restauração do Sistema Operacional.
- Adição de scripts para modificar o ambiente a seu gosto;
- Baixo custo de implantação do ambiente;
- Solução independente do Sistema Operacional do *Honeypot*;
- Funcionamento em diferentes tipos de hardwares, sem a necessidade do uso de tecnologias específicas.

Requisitos Interessantes

Para um sistema de restauração de *Honeypots* são requisitos interessantes:

- Execução sem interação com usuário e remota para o armazenamento ou restauração do Sistema Operacional.
- Adição de scripts para modificar o ambiente a seu gosto;
- Baixo custo de implantação do ambiente;
- Solução independente do Sistema Operacional do *Honeypot*;
- Funcionamento em diferentes tipos de hardwares, sem a necessidade do uso de tecnologias específicas.

Requisitos Interessantes

Para um sistema de restauração de *Honeypots* são requisitos interessantes:

- Execução sem interação com usuário e remota para o armazenamento ou restauração do Sistema Operacional.
- Adição de scripts para modificar o ambiente a seu gosto;
- Baixo custo de implantação do ambiente;
- Solução independente do Sistema Operacional do *Honeypot*;
- Funcionamento em diferentes tipos de hardwares, sem a necessidade do uso de tecnologias específicas.

Requisitos Interessantes

Para um sistema de restauração de *Honeypots* são requisitos interessantes:

- Execução sem interação com usuário e remota para o armazenamento ou restauração do Sistema Operacional.
- Adição de scripts para modificar o ambiente a seu gosto;
- Baixo custo de implantação do ambiente;
- Solução independente do Sistema Operacional do *Honeypot*;
- Funcionamento em diferentes tipos de hardwares, sem a necessidade do uso de tecnologias específicas.

Requisitos Interessantes

Para um sistema de restauração de *Honeypots* são requisitos interessantes:

- Execução sem interação com usuário e remota para o armazenamento ou restauração do Sistema Operacional.
- Adição de scripts para modificar o ambiente a seu gosto;
- Baixo custo de implantação do ambiente;
- Solução independente do Sistema Operacional do *Honeypot*;
- Funcionamento em diferentes tipos de hardwares, sem a necessidade do uso de tecnologias específicas.

O Ambiente Proposto

Foram definidas duas propostas baseadas no método de restauração por imagem:

- Ambiente *Standalone*;
- Ambiente Cliente x Servidor.

O Ambiente Proposto

Foram definidas duas propostas baseadas no método de restauração por imagem:

- Ambiente *Standalone*;
- Ambiente Cliente x Servidor.

O Ambiente Proposto

Foram definidas duas propostas baseadas no método de restauração por imagem:

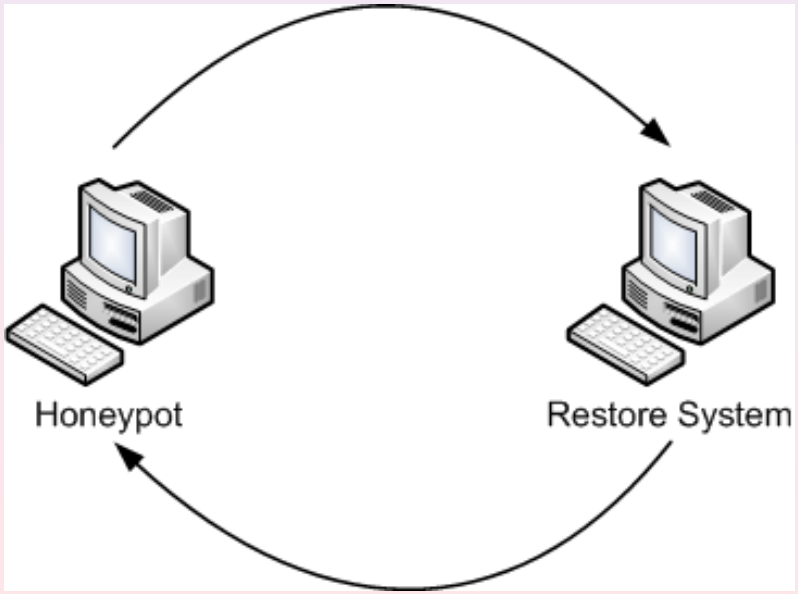
- Ambiente *Standalone*;
- Ambiente Cliente x Servidor.

Standalone

O Ambiente *Standalone*

Arquitetura

Esta arquitetura é baseada em um computador, que faz o papel tanto do *Honeypot* quanto do Sistema de Restauração.



Particionamento

No ambiente *standalone* o disco rígido é dividido em três partições:

- hda1 - Sistema Operacional do *Honeypot*;
- hda2 - Ambiente de Restauração (GNU/Linux);
- hda3 - Armazenamento de Imagens.

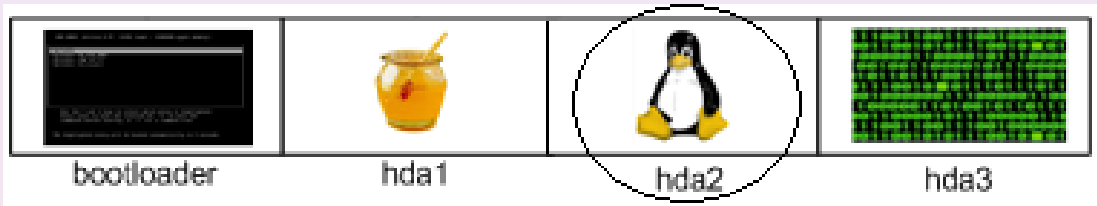
Particionamento

No ambiente *standalone* o disco rígido é dividido em três partições:

- hda1 - Sistema Operacional do *Honeypot*;
- hda2 - Ambiente de Restauração (GNU/Linux);
- hda3 - Armazenamento de Imagens.

Particionamento

No ambiente *standalone* o disco rígido é dividido em três partições:



- hda1 - Sistema Operacional do *Honeypot*;
- hda2 - Ambiente de Restauração (GNU/Linux);
- hda3 - Armazenamento de Imagens.

Particionamento

No ambiente *standalone* o disco rígido é dividido em três partições:

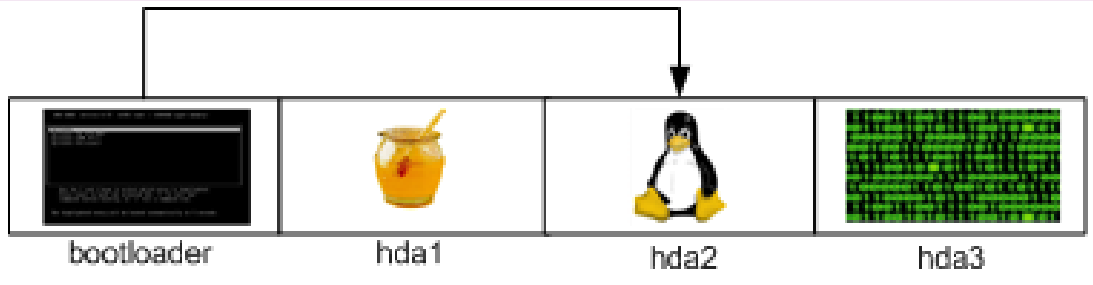
- hda1 - Sistema Operacional do *Honeypot*;
- hda2 - Ambiente de Restauração (GNU/Linux);
- hda3 - Armazenamento de Imagens.

Executar *Honeypot*

Na execução normal do computador o *bootloader* chama o Sistema Operacional do *Honeypot*.

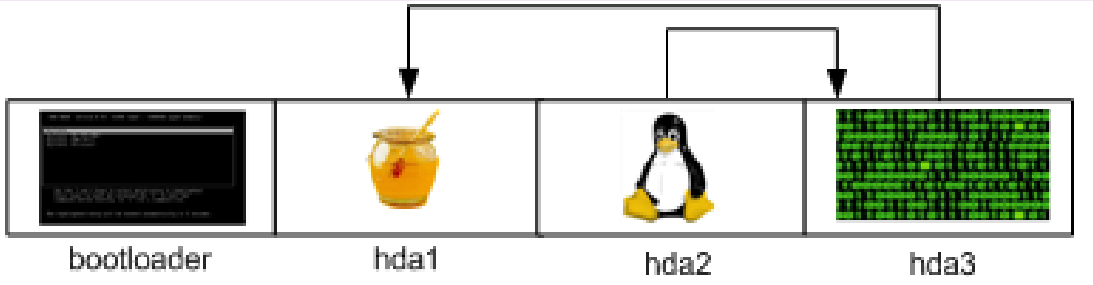
Restaurar ou Armazenar

Quando é necessário restaurar ou armazenar a imagem do *Honeypot*, o *bootloader* chama o Sistema de Restauração.



Restaurar Imagem do *Honeypot*

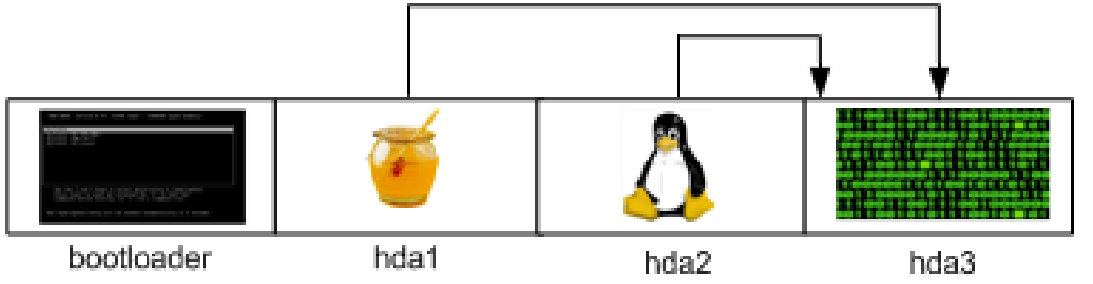
Após o sistema iniciar, scripts são responsáveis por restaurar o *Honeypot* a partir de uma imagem armazenada.



Armazenar Imagem do *Honeypot*

Quando:

- Sistema em estado original conhecido;
- Sistema comprometido.

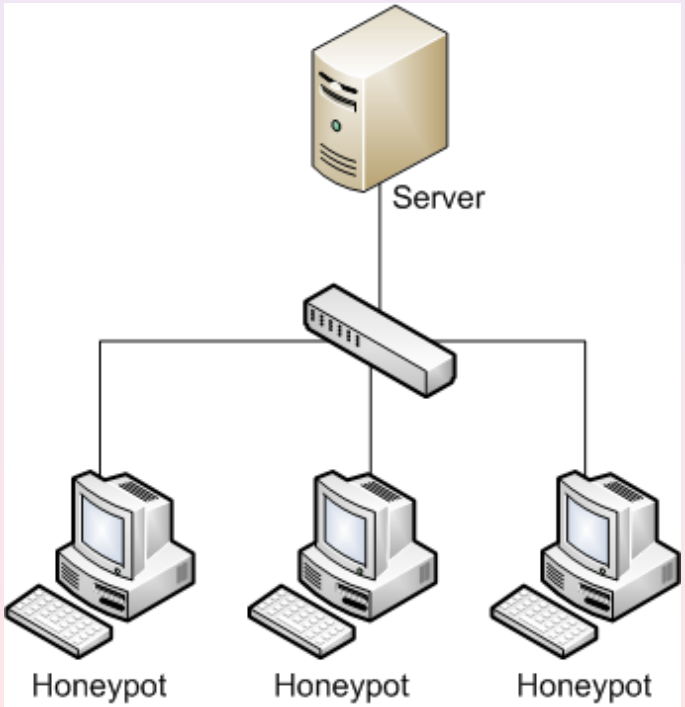


Cliente X Servidor

O Ambiente Cliente X Servidor

Arquitetura

Esta arquitetura é baseada em diversos *Honeypots* clientes e um servidor configurado como Sistema de Restauração.



Pré-Requisitos

Para que este ambiente funcione corretamente são necessários alguns requisitos.

- Clientes
  - Suporte a *boot* remoto via PXE.
- Servidor
  - Disco rígido relativamente grande.

Pré-Requisitos

Para que este ambiente funcione corretamente são necessários alguns requisitos.

- Clientes
  - Suporte a *boot* remoto via PXE.
- Servidor
  - Disco rígido relativamente grande.

Pré-Requisitos

Para que este ambiente funcione corretamente são necessários alguns requisitos.

- Clientes
  - Suporte a *boot* remoto via PXE.
- Servidor
  - Disco rígido relativamente grande.

Serviços

Além dos requisitos, são necessários serviços essenciais para o funcionamento do ambiente.

- DHCPD
- TFTPD
- PARTIMAGED
- SYSLOGD

Serviços

Além dos requisitos, são necessários serviços essenciais para o funcionamento do ambiente.

- DHCPD
- TFTPD
- PARTIMAGED
- SYSLOGD

PXE

Preboot Execution Environment (PXE) é um ambiente para inicialização de Sistemas Operacionais através da interface de rede.

Ou seja não depende do disco rígido para inicializar.

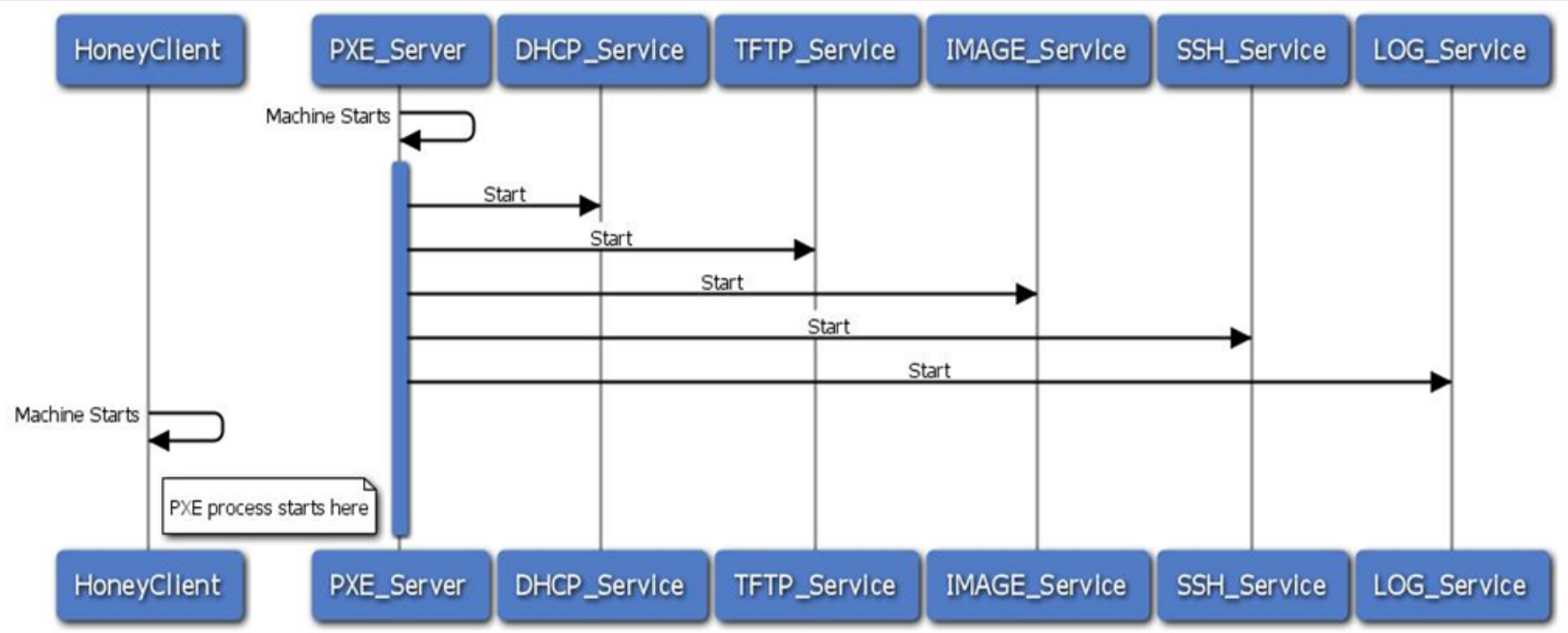
PXE

Preboot Execution Environment (PXE) é um ambiente para inicialização de Sistemas Operacionais através da interface de rede.

Ou seja não depende do disco rígido para inicializar.

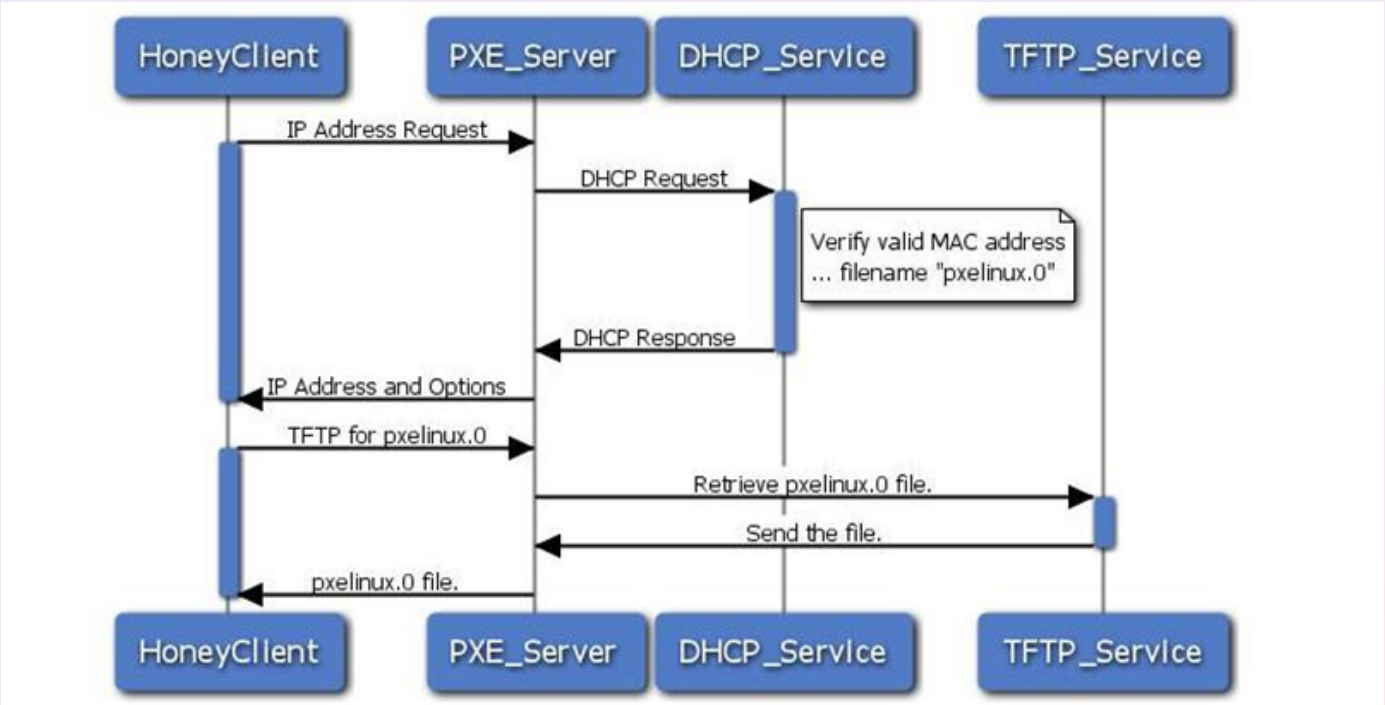
O Servidor

Na inicialização do servidor, os serviços necessários são disponibilizados para os clientes.



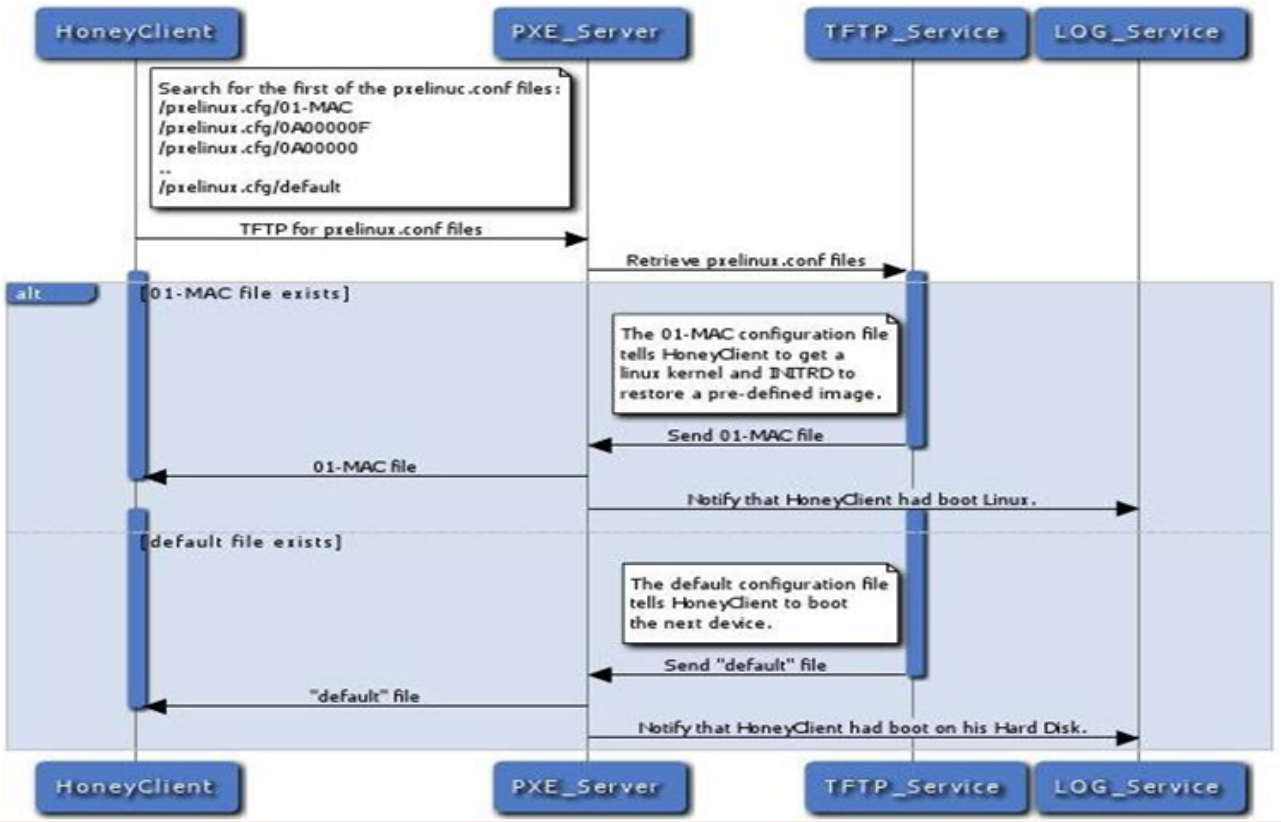
Inicializando o Honeypot

Ao inicializar o *Honeypot*, ele obtém um IP e um arquivo de configuração do PXE.



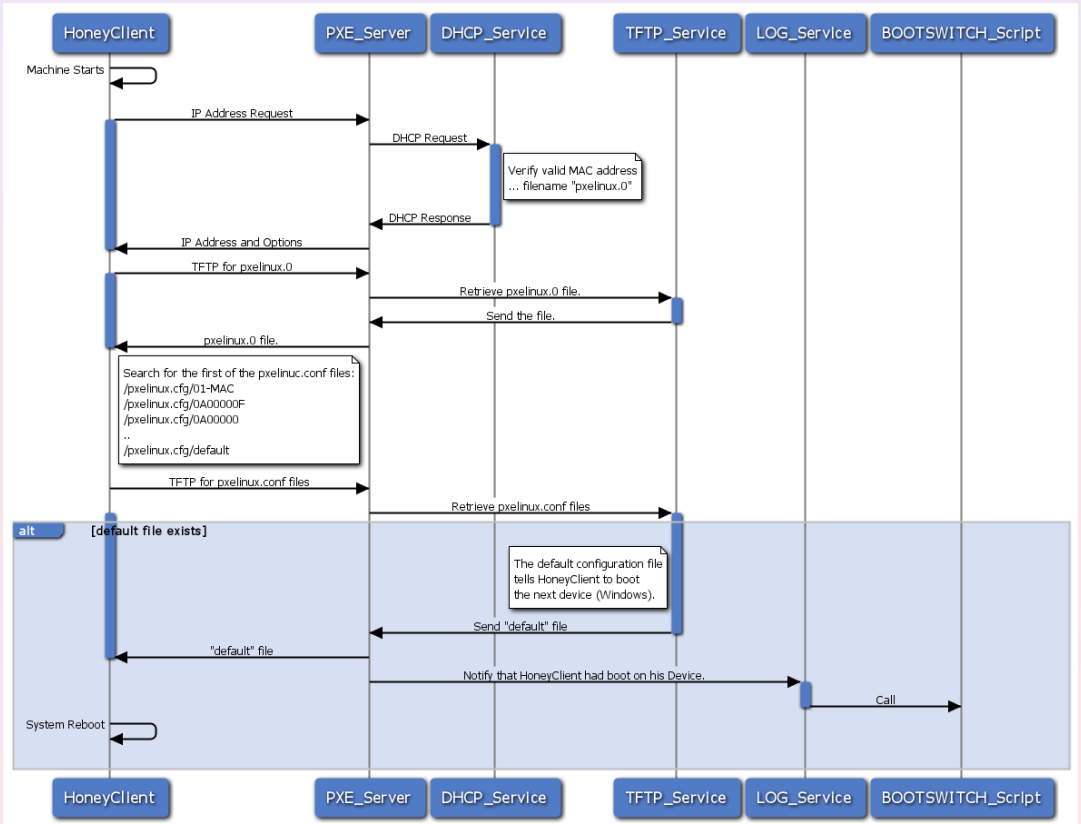
Restaurar, Armazenar ou Executar?

A partir do arquivo de configuração é definida qual ação deve ser tomada.



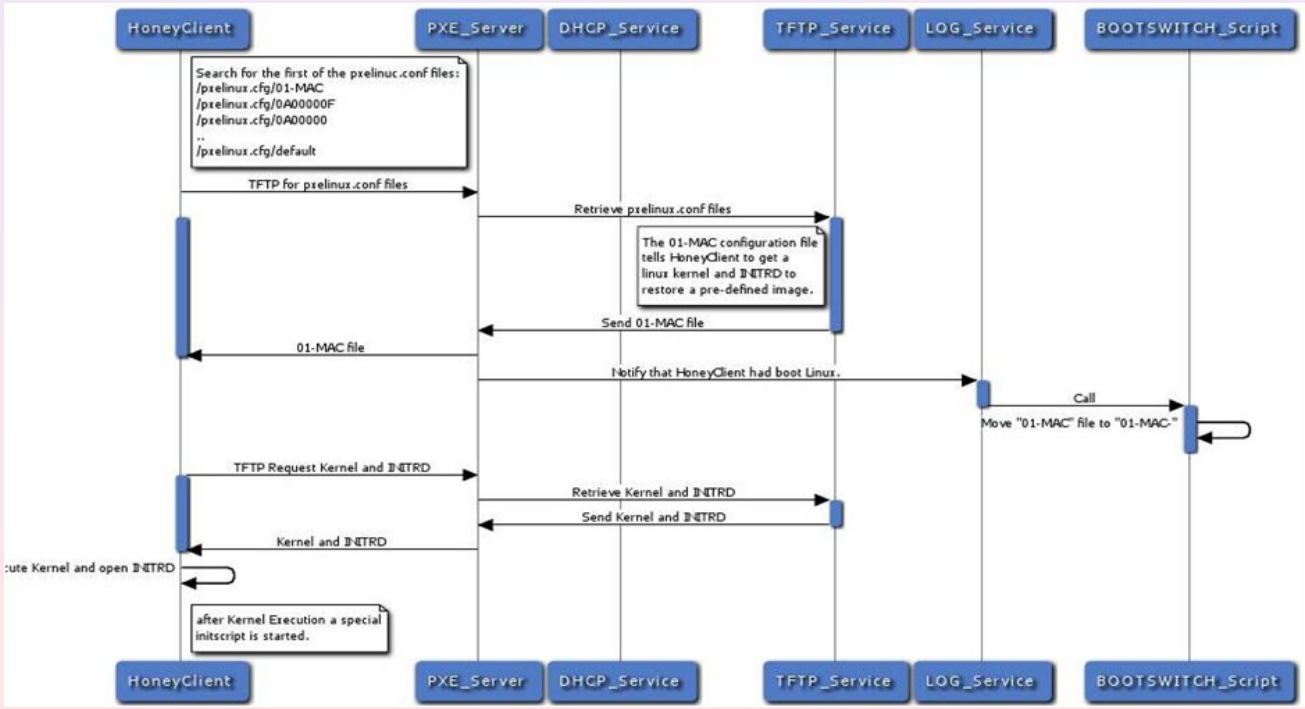
Executar o *Honeypot*

Caso o arquivo indique a executação normal do *Honeypot*, este inicializa a partir do próprio disco rígido.



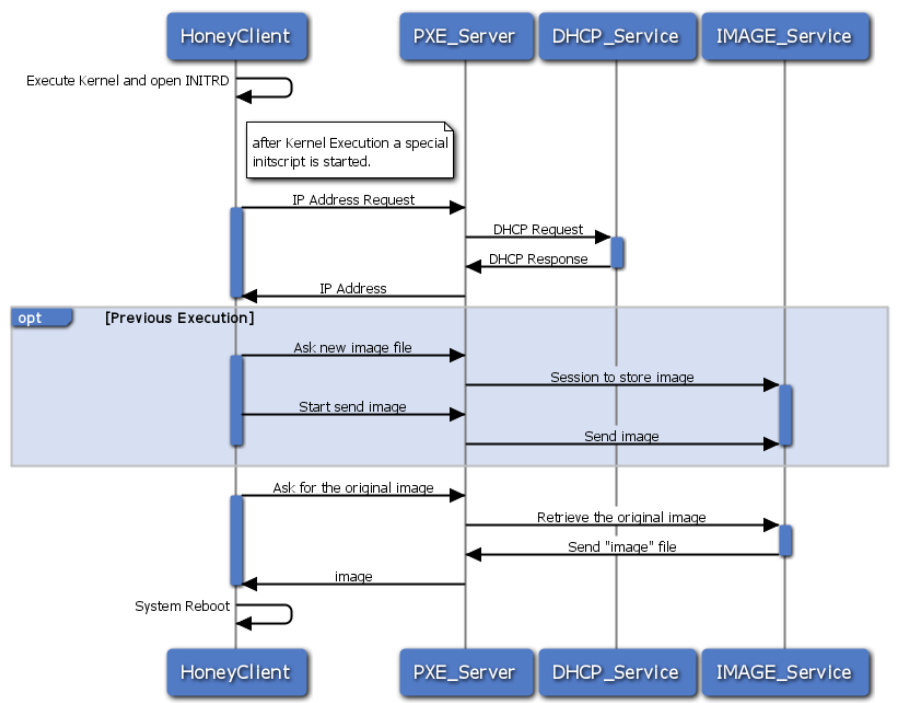
Restaurar ou Armazenar Imagem

Caso o arquivo indique a restauração ou armazenamento do *Honeypot* o cliente baixa um *Kernel* e um *initrd* para inicializar o sistema.



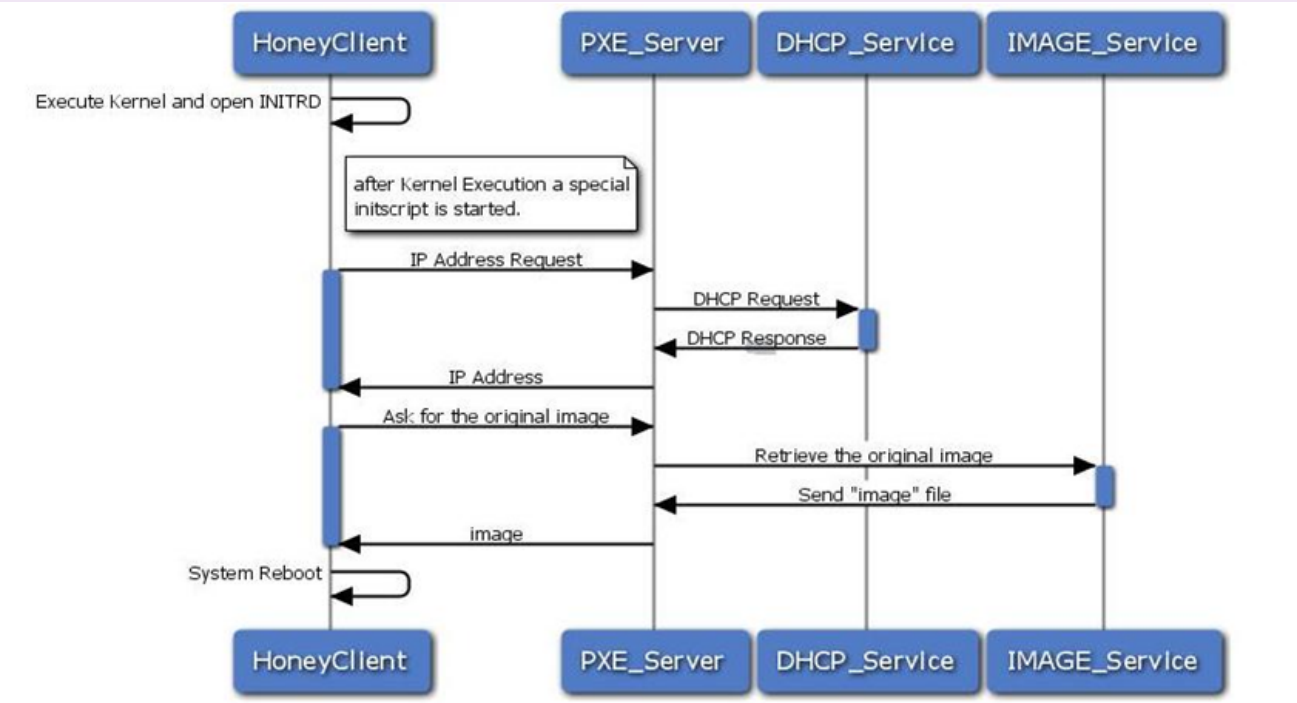
Restaurar ou Armazenar Imagem

Já com o sistema inicializado existe a possibilidade de armazenar ou restaurar a imagem do disco.



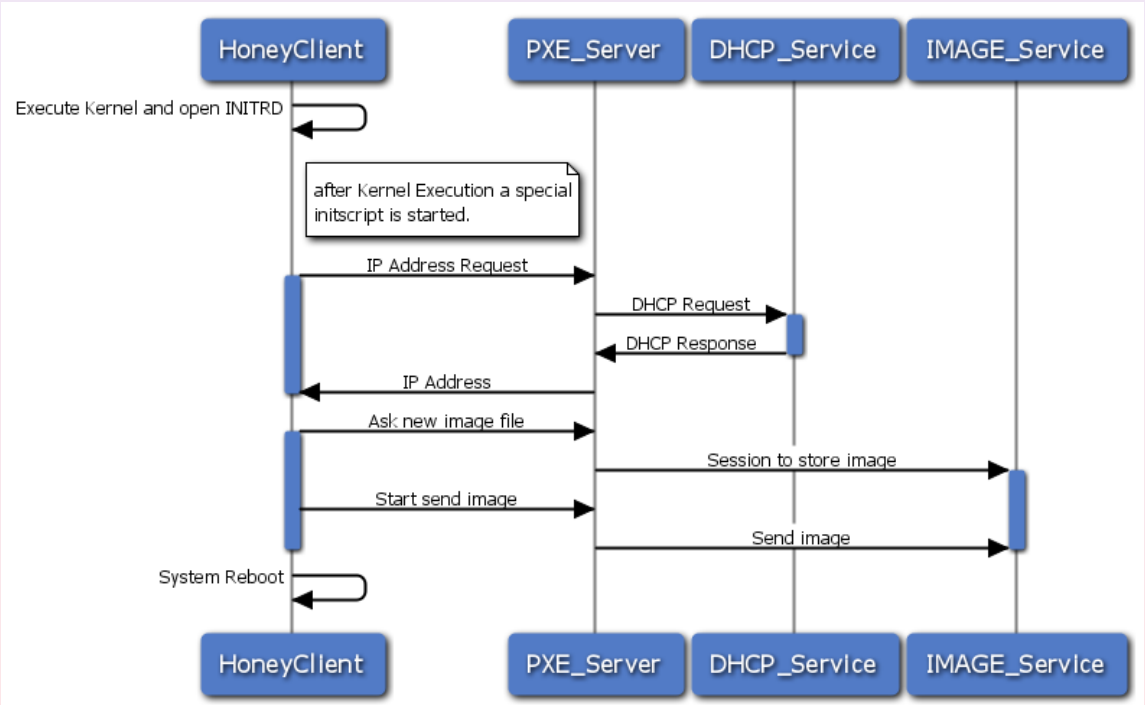
Restaurar Imagem do *Honeypot*

Na restauração do sistema são executados scripts que iniciam o processo enviando a imagem para o disco.



Armazenar Imagem do *Honeypot*

Para armazenar são executados scripts que iniciam o processo enviando a imagem do cliente para o servidor.



Setup

Com o ambiente *Standalone* em execução, foram aferidos o uso de CPU e tempo para restauração de uma imagem.

A configuração do computador é a seguinte:

- Processador AMD Sempron(tm) 2500+
- 2 GB de Memória RAM
- HD SAMSUNG SP0411N 40GB

O tamanho da imagem restaurada é de 4,67 GB armazenada em 1,42 GB.

Setup

Com o ambiente *Standalone* em execução, foram aferidos o uso de CPU e tempo para restauração de uma imagem.

A configuração do computador é a seguinte:

- Processador AMD Sempron(tm) 2500+
- 2 GB de Memória RAM
- HD SAMSUNG SP0411N 40GB

O tamanho da imagem restaurada é de 4,67 GB armazenada em 1,42 GB.

Setup

Com o ambiente *Standalone* em execução, foram aferidos o uso de CPU e tempo para restauração de uma imagem.

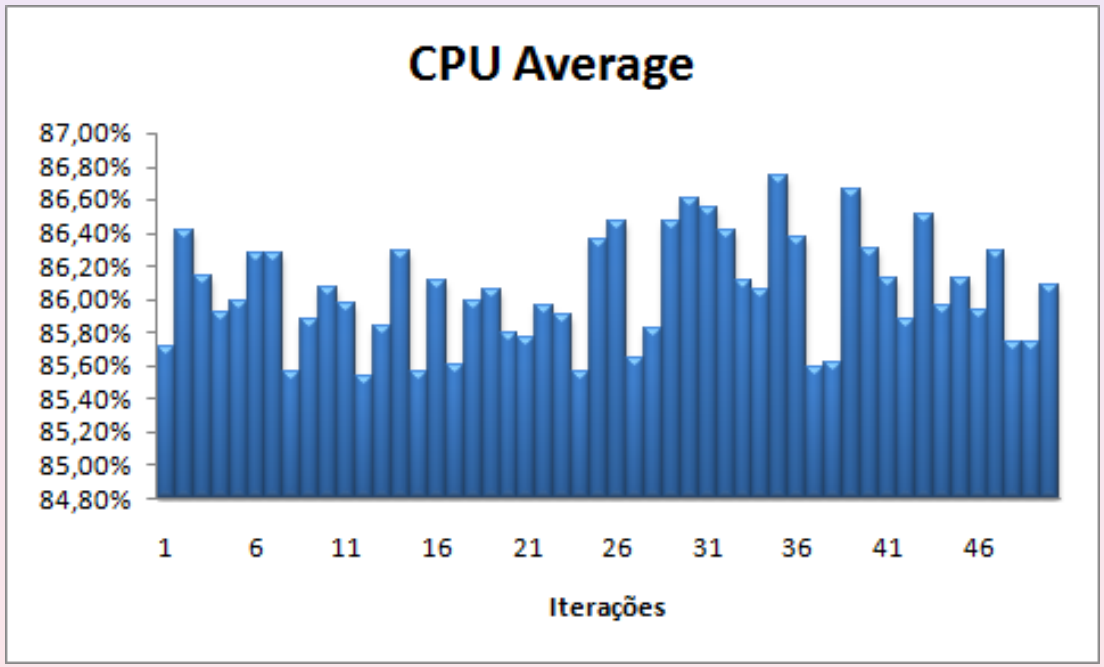
A configuração do computador é a seguinte:

- Processador AMD Sempron(tm) 2500+
- 2 GB de Memória RAM
- HD SAMSUNG SP0411N 40GB

O tamanho da imagem restaurada é de 4,67 GB armazenada em 1,42 GB.

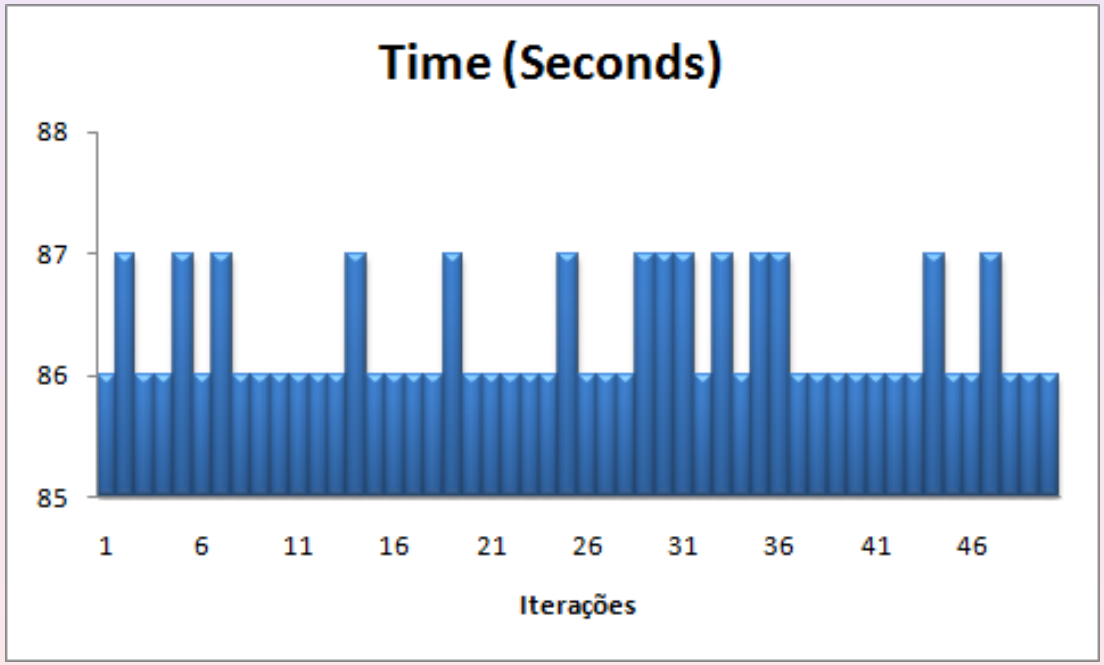
Processamento

Média de uso de CPU pelo processo (nice -19)



Tempo

Tempo de restauração da imagem.



Setup

Com o ambiente Cliente X Servidor em execução, foram aferidos o uso de CPU, Memória e Rede no servidor e tempo para restauração de uma imagem padrão.

O tamanho da imagem restaurada é de 4,67 GB armazenada em 1,42 GB.

Setup

Com o ambiente Cliente X Servidor em execução, foram aferidos o uso de CPU, Memória e Rede no servidor e tempo para restauração de uma imagem padrão.

O tamanho da imagem restaurada é de 4,67 GB armazenada em 1,42 GB.

Setup

A configuração do servidor é a seguinte:

- Processador AMD Sempron(tm) 2500+
- 2 GB de Memória RAM
- HD SAMSUNG SP0411N 40GB
- Interface de Rede VIA VT6102 [Rhine-II]

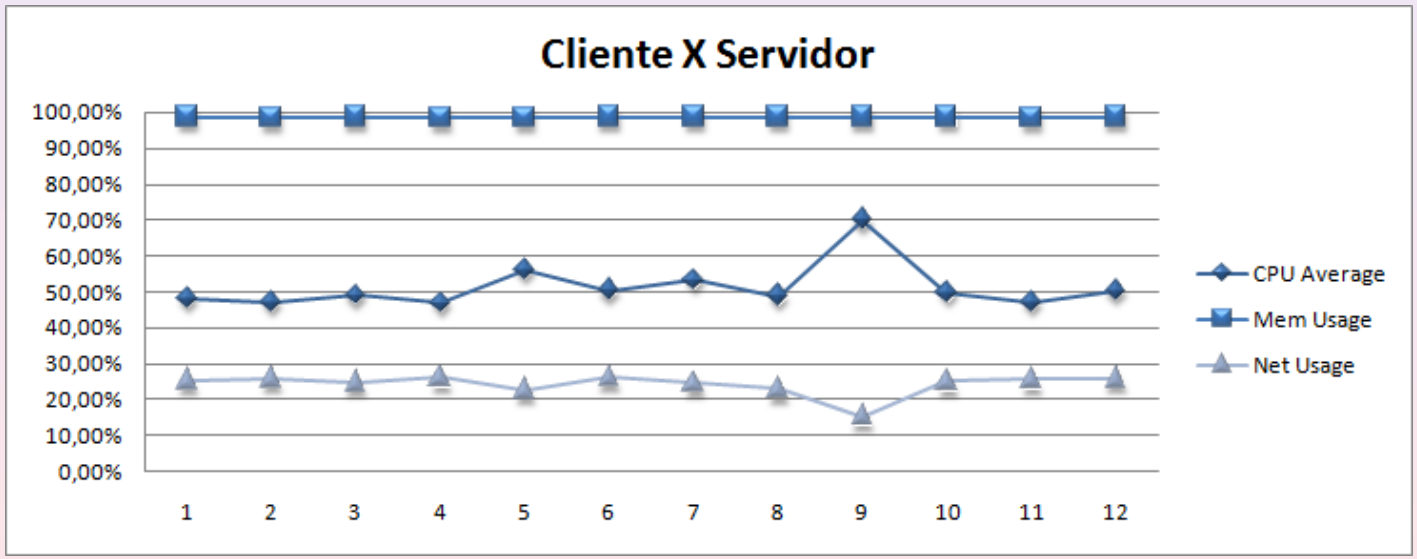
Setup

A configuração do cliente é a seguinte:

- Processador AMD Sempron(tm) 2500+
- 2 GB de Memória RAM
- HD SAMSUNG SP0411N 40GB
- Interface de Rede VIA VT6102 [Rhine-II]

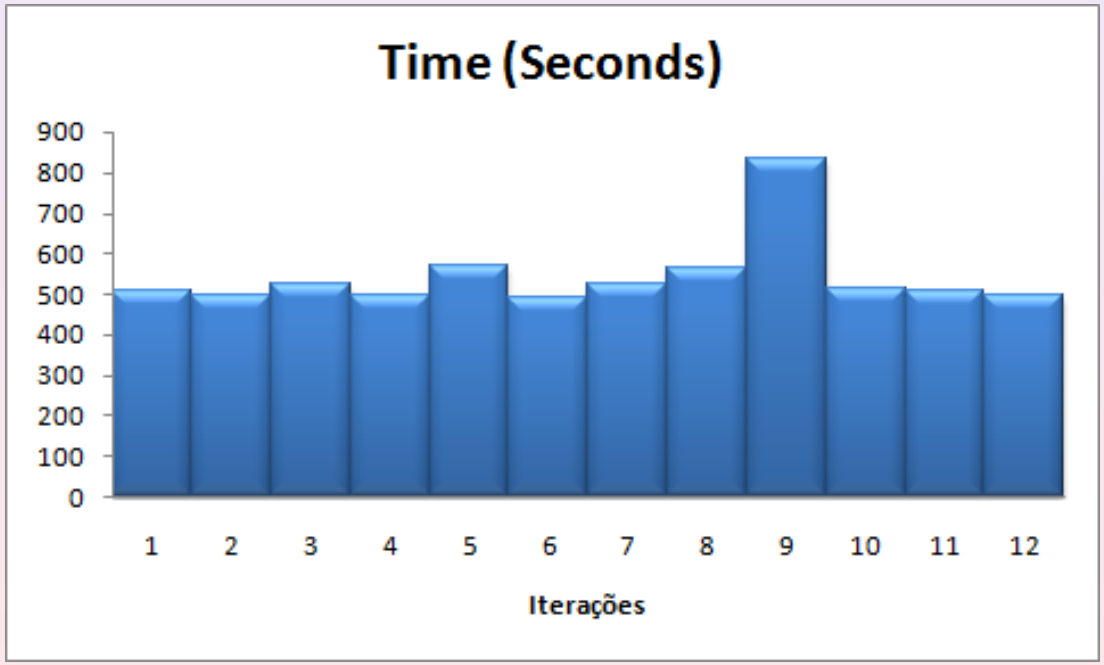
Processamento x Memória x Rede

Porcentagem de uso de processamento, memória e rede no servidor.



Tempo

Tempo de restauração da imagem.



Atualmente

Atualmente estes ambientes estão sendo utilizados em duas *Honeynets* em produção.

- CTI
  - 6 *Honeypots* Windows
  - 2 *Honeypots* GNU/Linux
- INPE
  - 2 *Honeypots* Windows
  - 2 *Honeypots* GNU/Linux

Atualmente

Atualmente estes ambientes estão sendo utilizados em duas *Honeynets* em produção.

- CTI
  - 6 *Honeypots* Windows
  - 2 *Honeypots* GNU/Linux
- INPE
  - 2 *Honeypots* Windows
  - 2 *Honeypots* GNU/Linux

Atualmente

Atualmente estes ambientes estão sendo utilizados em duas *Honeynets* em produção.

- CTI
  - 6 *Honeypots* Windows
  - 2 *Honeypots* GNU/Linux
- INPE
  - 2 *Honeypots* Windows
  - 2 *Honeypots* GNU/Linux

Outras Aplicações

Mas esta ferramenta não é restrita apenas a *Honeypots* de alta interatividade, ela também pode ser utilizada em outros ambientes:

- Sandboxes para análise de artefatos maliciosos;
- Laboratórios de Escolas;
- Quiosques em Cyber-cafés;
- Lan-Houses.

Outras Aplicações

Mas esta ferramenta não é restrita apenas a *Honeypots* de alta interatividade, ela também pode ser utilizada em outros ambientes:

- Sandboxes para análise de artefatos maliciosos;
- Laboratórios de Escolas;
- Quiosques em Cyber-cafés;
- Lan-Houses.

Conclusão

O uso desta ferramenta para *Honeynets* se mostra viável, devidos a pontos positivos como:

- Facilidade de uso;
- Baixo custo de implantação e tempo de restauração;
- Administração de *Honeypots* remotamente;
- Possibilidade de armazenamento de sistema comprometido;
- Grande independência do Sistema Operacional do cliente (GNU/Linux e Microsoft Windows).

Conclusão

O uso desta ferramenta para *Honeynets* se mostra viável, devidos a pontos positivos como:

- Facilidade de uso;
- Baixo custo de implantação e tempo de restauração;
- Administração de *Honeypots* remotamente;
- Possibilidade de armazenamento de sistema comprometido;
- Grande independência do Sistema Operacional do cliente (GNU/Linux e Microsoft Windows).

Conclusão

O uso desta ferramenta para *Honeynets* se mostra viável, devidos a pontos positivos como:

- Facilidade de uso;
- Baixo custo de implantação e tempo de restauração;
- Administração de *Honeypots* remotamente;
- Possibilidade de armazenamento de sistema comprometido;
- Grande independência do Sistema Operacional do cliente (GNU/Linux e Microsoft Windows).

Conclusão

O uso desta ferramenta para *Honeynets* se mostra viável, devidos a pontos positivos como:

- Facilidade de uso;
- Baixo custo de implantação e tempo de restauração;
- Administração de *Honeypots* remotamente;
- Possibilidade de armazenamento de sistema comprometido;
- Grande independência do Sistema Operacional do cliente (GNU/Linux e Microsoft Windows).

Conclusão

O uso desta ferramenta para *Honeynets* se mostra viável, devidos a pontos positivos como:

- Facilidade de uso;
- Baixo custo de implantação e tempo de restauração;
- Administração de *Honeypots* remotamente;
- Possibilidade de armazenamento de sistema comprometido;
- Grande independência do Sistema Operacional do cliente (GNU/Linux e Microsoft Windows).

Conclusão

O uso desta ferramenta para *Honeynets* se mostra viável, devidos a pontos positivos como:

- Facilidade de uso;
- Baixo custo de implantação e tempo de restauração;
- Administração de *Honeypots* remotamente;
- Possibilidade de armazenamento de sistema comprometido;
- Grande independência do Sistema Operacional do cliente (GNU/Linux e Microsoft Windows).

Conclusão

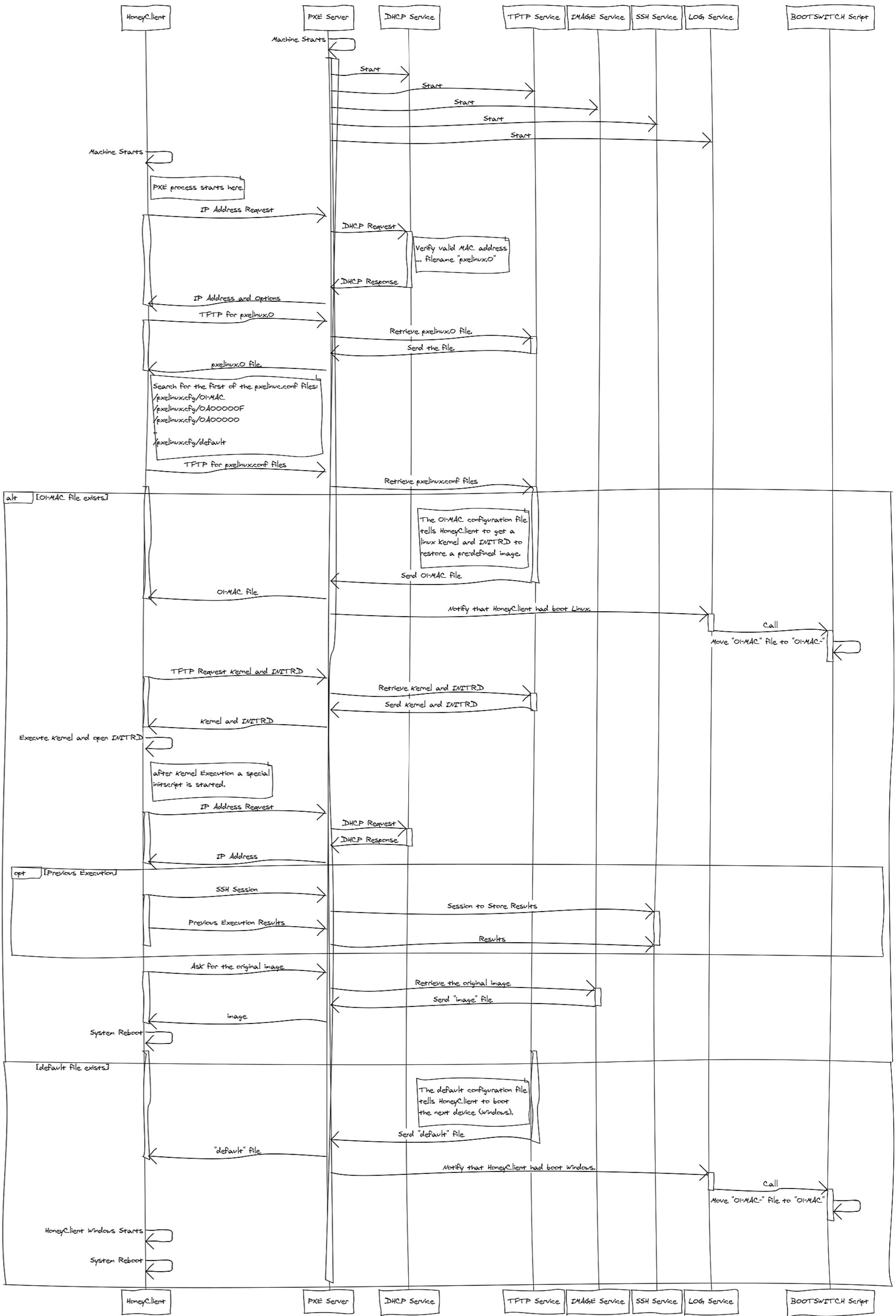
Obrigado!

Contatos

Ricardo Makino
ricardo.makino@dssi.cti.gov.br
ricardo.nobu@gmail.com

Luiz Otávio Duarte
lod@dssi.cti.gov.br
loduarte@gmail.com

Renato Yuzo
renato.madokoro@dssi.cti.gov.br
renatoyuzo@gmail.com


HoneyClient
PXE Server
DHCP Service
TFTP Service
IMAGE Service
SSH Service
LOG Service
BOOTSWITCH Script
Machine Starts
Start
Start
Start
Start
Start
Machine Starts
PXE process starts here.
IP Address Request
DHCP Request
Verify valid MAC address
... filename "pxelinux.0"
DHCP Response
IP Address and Options
TFTP for pxelinux.0
Retrieve pxelinux.0 file.
Send the file.
pxelinux.0 file.
Search for the first of the pxelinux.conf files:
/pxelinux.cfg/01-MAC
/pxelinux.cfg/0A00000F
/pxelinux.cfg/0A000000
...
/pxelinux.cfg/default
TFTP for pxelinux.conf files
Retrieve pxelinux.conf files
alt
[01-MAC file exists]
The 01-MAC configuration file
tells HoneyClient to get a
linux kernel and INITRD to
restore a predefined image.
Send 01-MAC file
01-MAC file
Notify that HoneyClient had boot Linux.
Call
Move "01-MAC" file to "01-MAC-"
TFTP Request Kernel and INITRD
Retrieve Kernel and INITRD
Send Kernel and INITRD
Kernel and INITRD
Execute Kernel and open INITRD
after Kernel Execution a special
initscript is started.
IP Address Request
DHCP Request
DHCP Response
IP Address
opt
[Previous Execution]
SSH Session
Session to Store Results
Previous Execution Results
Results
Ask for the original image
Retrieve the original image
Send "image" file
image
System Reboot
[default file exists]
The default configuration file
tells HoneyClient to boot
the next device (Windows).
Send "default" file
"default" file
Notify that HoneyClient had boot Windows.
Call
Move "01-MAC-" file to "01-MAC"
HoneyClient Windows Starts
System Reboot
HoneyClient
PXE Server
DHCP Service
TFTP Service
IMAGE Service
SSH Service
LOG Service
BOOTSWITCH Script