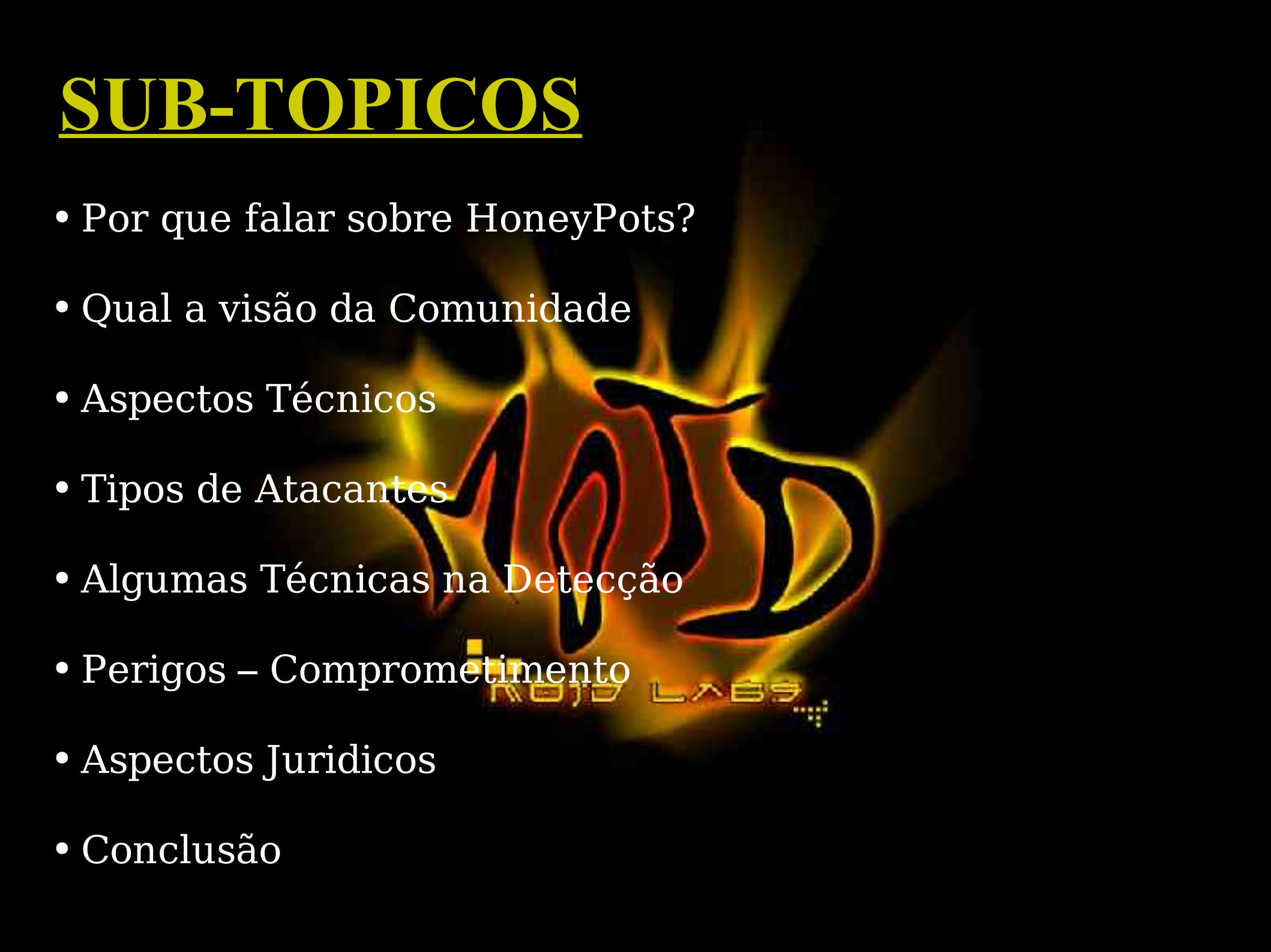
DETONANDO HONEYPOTS

FELIX COUTINHO aka SkyNet45

http://www.h2hc.com.br/

SUB-TOPICOS

- Por que falar sobre HoneyPots?
- Qual a visão da Comunidade
- Aspectos Técnicos
- Tipos de Atacantes
- Algumas Técnicas na Detecção
- Perigos – Comprometimento
- Aspectos Juridicos
- Conclusão



O QUE EH UM HONEYPOT?

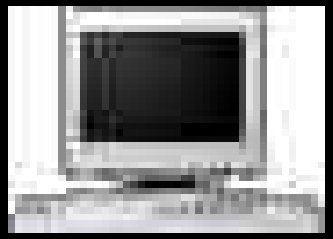
Apenas uma ou varias Ferramentas

PREPARADAS PARA:

- Atrair
- Captar
- Avisar

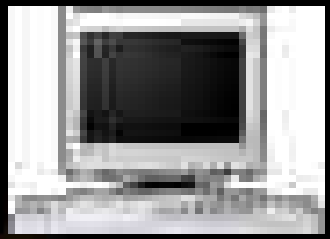
HONEYPOT

HONEYPOT



- HoneyD 0.7 -
SuSe 9
Telnet
Http

HONEYPOT



Slack 8.1
Vmware
SuSe 9
Telnet
Http
+
Sebek

Identificação do OS por scanners
atraves de OS Fingerprints

Exemplos: nmap.prints & xprobe.prints (HoneyD)

HONEYPOT

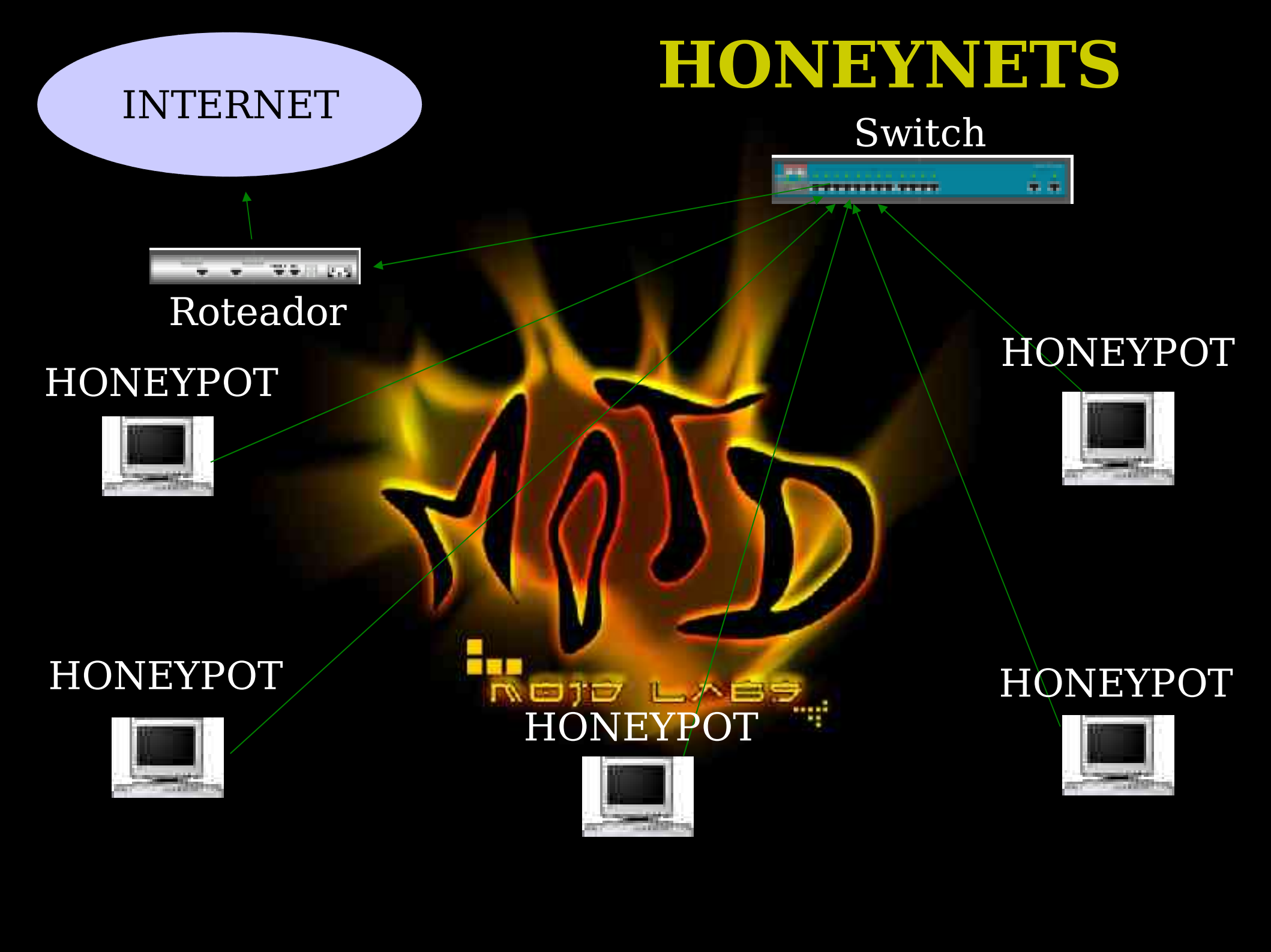
Exemplo do nmap.prints do Honeyd-0.8b

```
Fingerprint OpenBSD 3.1 on an Alpha
Class OpenBSD | OpenBSD | 3.X | general purpose
TSeq(Class=TR%gcd=<6%IPID=RD%TS=2HZ)
T1(DF=Y%W=FFFF%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(DF=Y%W=FFFF%ACK=O%Flags=R%Ops=)
T5(DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=N)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=134%RID=E%RIPCK=F%UCK=E%ULEN=134%DAT=E)
```

HONEYNETS

- Caracterização
- Serviços Reais
- Serviços Falsos
- Vmware
- Exemplo

HONEYNETS


INTERNET
Switch
Roteador
HONEYPOT
HONEYPOT
HONEYPOT
HONEYPOT
HONEYPOT
HONEYPOT

TIPOS DE HONEYPOT

- ALTA INTERATIVIDADE

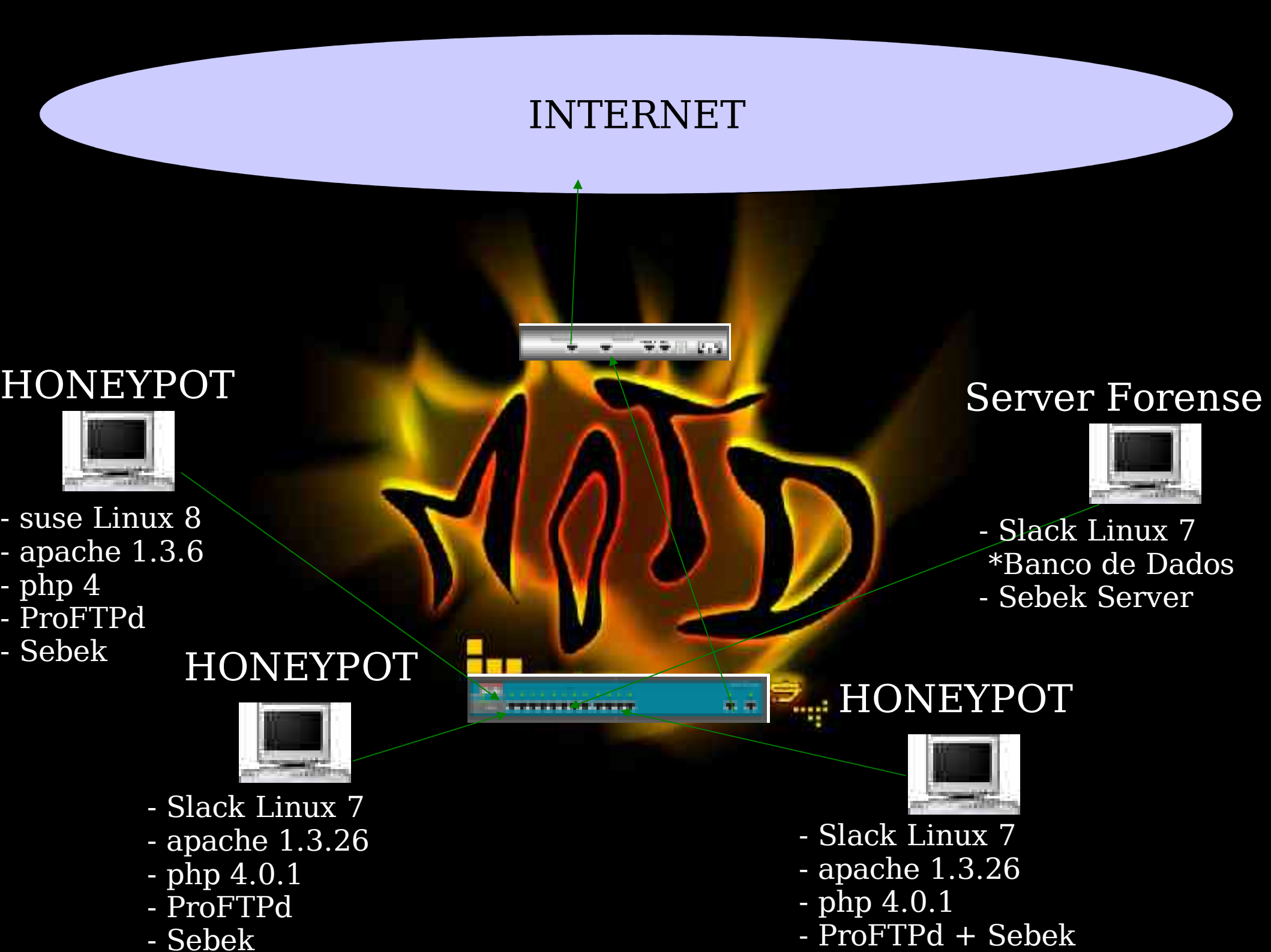
- BAIXA INTERATIVIDADE

ALTA INTERATIVIDADE

- Serviços reais.
- Geralmente rodam dentro de uma Vmware, podendo tambem existir em maquinas reais distindas.

Fazer os honeypots rodarem dentro de uma Vmware aumenta muito o numero de possibilidades de sua deteccao.

Se funcionando em maquinas reais (fisico) irah acarretar uma serie de gastos desnecessarios.


INTERNET
HONEYPOT
- suse Linux 8
- apache 1.3.6
- php 4
- ProFTPd
- Sebek
Server Forense
- Slack Linux 7
*Banco de Dados
- Sebek Server
HONEYPOT
- Slack Linux 7
- apache 1.3.26
- php 4.0.1
- ProFTPd
- Sebek
HONEYPOT
- Slack Linux 7
- apache 1.3.26
- php 4.0.1
- ProFTPd + Sebek

BAIXA INTERATIVIDADE

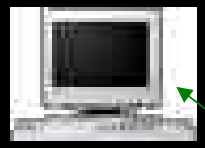
- Emulam sistemas e falhas.
- Maquina real ou Vmware
- Usam recursos da maquina hospedeira.

Exemplos: HoneyD & HoneyPerl

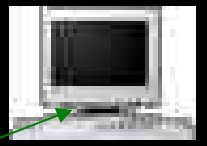
Trataremos de Ambos!!!

BAIXA INTERATIVIDADE

EXEMPLO - 1

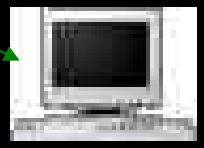


- HOST_A -
OpenBSD
HONEYD > SuSe 8
TELNET
FTP
FINGER



- HOST_B -
- VMWARE -
Slack 9.1
VM1 – Slack 8/HONEYD
HTTP
FTP
VM2 –
OpenBSD/HONEYD
HTTP
FTP

- HOST_D -
- VMWARE -
Slack 9.1
VM1 – Slack 8/HONEYD
HTTP
FTP
VM2 –
OpenBSD/HONEYD
HTTP
FTP



- HOST_C -
OpenBSD
HONEYD > SuSe 8
TELNET

DETECCAO

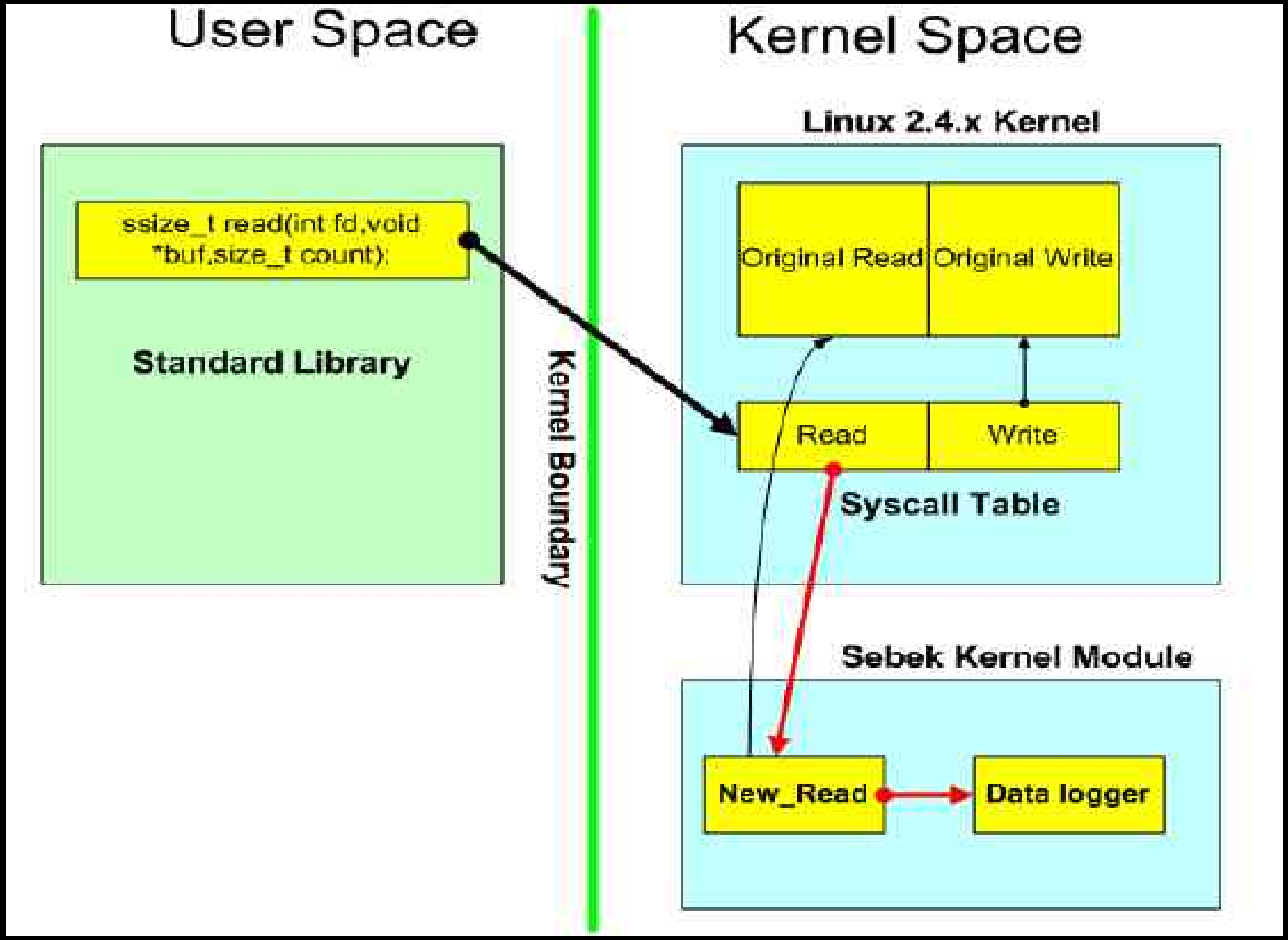
VMWARE

Como Usuario Comum
4tphi-vmchk.c (code)
Semelhanca no MAC da placa de rede

Como Root
Ksyms | grep VM

4tphi-vmchk.c--> Written by Andrew Hintz <http://guh.nu>

SEBEK



Retirado de: Sebek Know your Enemy – Lance Splinterz

SEBEK

Metodos para deteccao da ferramenta SEBEK

- Chkrootkit (*)
  Eh bem util enquanto o Sebek estiver exportando simbolos.

DETECCAO...

#./chkrootkit
...
`lkm` ... Sebek LKM Installed!
...

MAS...Em alguns casos...

#./chkrootkit
...
`lkm` ... not detected
...

SEBEK

Metodos para deteccao da ferramenta SEBEK

Surge uma ideia...

```
# grep Sebek chkrookit
    echo “Warning: Sebek LKM installed”
```

Daih...

#pico chkrootkit (Procuramos pela string “Sebek”)

Achamos as linhas:

```
### sebek LKM (Adore based)
    [ -r /proc/ksyms ] && \
    if `${egrep} -i sebek < /proc/ksyms >/dev/null 2>&1`; then
      echo "Warning: Sebek LKM installed"
    fi
```

SEBEK

Metodos para deteccao da ferramenta SEBEK

Chkrootkit baseia sua checagem apenas no nome (string) sebek.

Realizamos a mesma operacao na `mao`!

```
# grep sebek /proc/ksyms
c7a53000 __insmod_teste_O/usr/ferramentas/sebek-linux-2.1.7/teste.o_M40D837C0_V132118 [teste]
```

OPA!!!

SEBEK

Metodos para deteccao da ferramenta SEBEK

- A deteccao foi por meio do nome do diretorio (vide `sebek...`).
- Alterando o nome do diretorio e o nome do modulo...

SEBEK

Metodos para deteccao da ferramenta SEBEK
METODO II

- Drivers dos Dispositivos (Som, Pl. Rede, usb e etc)

- Procuramos qual o arquivo que carrega os modulos desses dispositivos na hora do boot.

SEBEK

Metodos para deteccao da ferramenta SEBEK

Com um simples...

#dmesg

Pudemos assim ver todos os modulos que sao carregados no boot.

#lsmod

Comparamos os modulos atuais com os que sao carregados a cada reboot.
Ao acharmos uma diferenca...

SEBEK

Metodos para deteccao da ferramenta SEBEK

Modulos do Boot

A
B
C
D
E
F
Sebek
G
H
I
J
L

#lsmod

A
B
C
D
E
F
G
H
I
J
L
M

CARACTERISTICAS DO HONEYD

- User Space
- Padronização na linha de comando
- Uma boa analise dentro do arquivo /dev/mem pode denunciar a presenca da ferramenta.

DETECCAO

- HoneyD

  Como Usuario Comum
  - Via `ps ax`

  Como Root
  - /dev/kmem

HoneyPerl
Expondo Caracteristicas

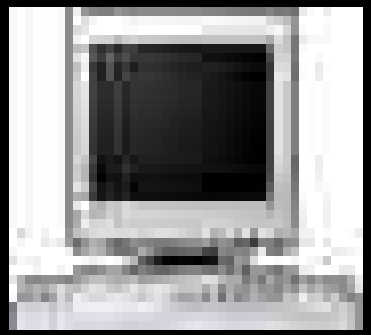
```
$welcome="220 $dominio ESMTP Sendmail 8.12.9/8.12.1;";

$error="500 5.5.1 Command unrecognized";

$datafinish="250 ok 1056985534 qp 14036";
```

Caracteristicas estáticas ao mandar fake-mails.

CAUSAS DO USO DE UM HONEYPOT

- Colocar Honeypots sozinhos na rede ira acarretar altos gastos, um custo elevado com: Link, Manutencao, Suporte e etc

HONEYPOT/NET



$$

TIPOS DE ATACANTES

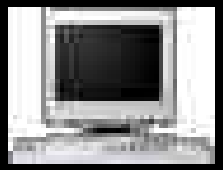
- Atacantes experientes.
- ScriptKiddies, Defacers e afins.
- Atacantes X Conceito

DIFICILMENTE ATACANTES EXPERIENTES VAO MOSTRAR O QUE SABEM PARA OS HONEYPOTS!!!

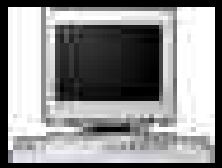
PERIGOS!!!

- Se o Honeypot for comprometido pode ser usado para futuros “crimes”, como: hospedar pornografia infatil, ataques a redes de bancos, do governo e etc.

ATACANTE



HONEYPOT



#comprometido#

REDE . GOV

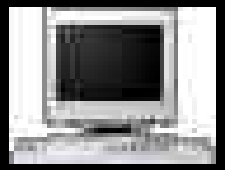
PERIGOS!!!

- Usado para servir de escravo em ataques Ddos.

PERIGOS!!!

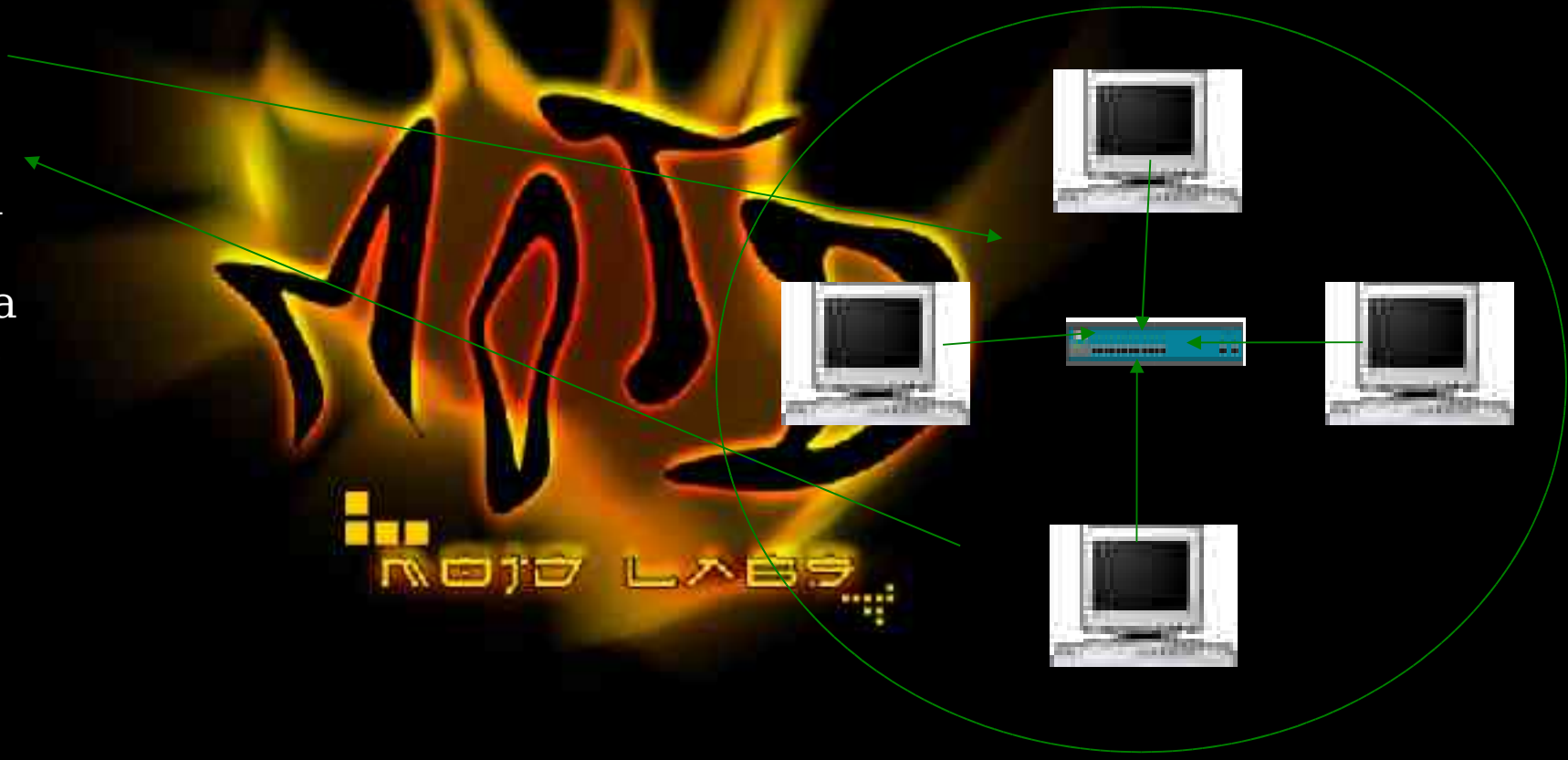
- Auxiliar na `quebra` de chaves, possiveis senhas.

ATACANTE



Tentando quebrar um chave criptografica por metodo distribuido.

HONEYNET COMPROMETIDA



ASPECTOS JURIDICOS

- Constituições

  - Canada
  - Europa
  - Reino Unido
  - EUA

ASPECTOS JURIDICOS

- Logs do ponto de Vista Judicial

- Indução Legal

ASPECTOS JURIDICOS

- Ações Judiciais = Responsabilidade do Administrador

Procederes Maliciosos Serão Respondidos pelos Administradores

PERGUNTAS???

Ultimas Palavras

AGRADECIMENTOS

MATERIAL

skynet45@motdlabs.org
http://skynet45.motdlabs.org/
http://www.motdlabs.org/
http://www.phrack.com/
http://www.insecure.com/

Leituras Recomendadas

Todos os Documentos de Lance Spitzner
(http://www.honeynet.org)
Todos do Niels Provos (http://www.monkey.org/~provos)

Phrack 62 Unofficial
Phrack 63 Unofficial