S3GUR4NC4 D3 D4D05

cONC31705

J1y4n y4R1

PREMISSA:

O MUNDO VIVE A INTERNET ...

VERDADE:

A INTERNET QUE O MUNDO VIVE É INSEGURA ...

S3GUR4NC4 D3 D4D05

Segundo dados divulgados pelo FBI (Federal Beareau of Investigation – Beareau Federal de Investigação – Policia Federal Americana), aproximadamente 90% dos casos de invasão bem sucedidas a servidores corporativos os usuários de rede (usuários autorizados) tiveram algum nível de parcela de culpa.

Entre os quais estão:

- senhas mal escolhidas;
- empregados descontentes (salário, posição, etc.);
- espionagem industrial;
- pirataria;
- e-mails infectados (vírus, spy-wears, trojans, etc.).

0000 0100

S3GUR4NC4 D3 D4D05

MOTIVAÇÃO:

- HACKER: " ... HOJE VOU INVADIR AQUELE SERVIDOR DE QUALQUER JEITO ..."

- CRACKER: " ... VAMOS VER QUANTOS "TROUXAS" RESPONDERAM ÀQUELE SCAM QUE DISSEMINEI VIA E-MAIL ONTEM. SERÁ QUE O "LARANJA" MANDOU ALGUM DINHEIRO? QUERO FAZER COMPRAS HOJE ... "

- SCRIPT-KIDDIE (LAMMER): " ... SERÁ QUE VOU CONSEGUIR INVADIR A MÁQUINA DE ALGUÉM HOJE COM AQUELE PROGRAMINHA QUE BAIXEI ONTEM DE MADRUGADA?"

S3GUR4NC4 D3 D4D05

Motivação:

- Usuário final da sua empresa (ao acordar): " ... Hoje vou ferrar a vida daquele administrador de rede "mala" que não me deixa fazer nada ... Mas como vou fazer isso?"

S3GUR4NC4 D3 D4D05

Motivação:

- Administrador da Rede (com olheiras): “ Nossa já é de manhã? Vou ver o que detectou o meu servidor ... Deve ter tido pelo menos uma 10 tentativas de invasão na rede ... fora os “bios” da empresa que vão arrumar para a minha cabeça ... “

S3GUR4NC4 D3 D4D05

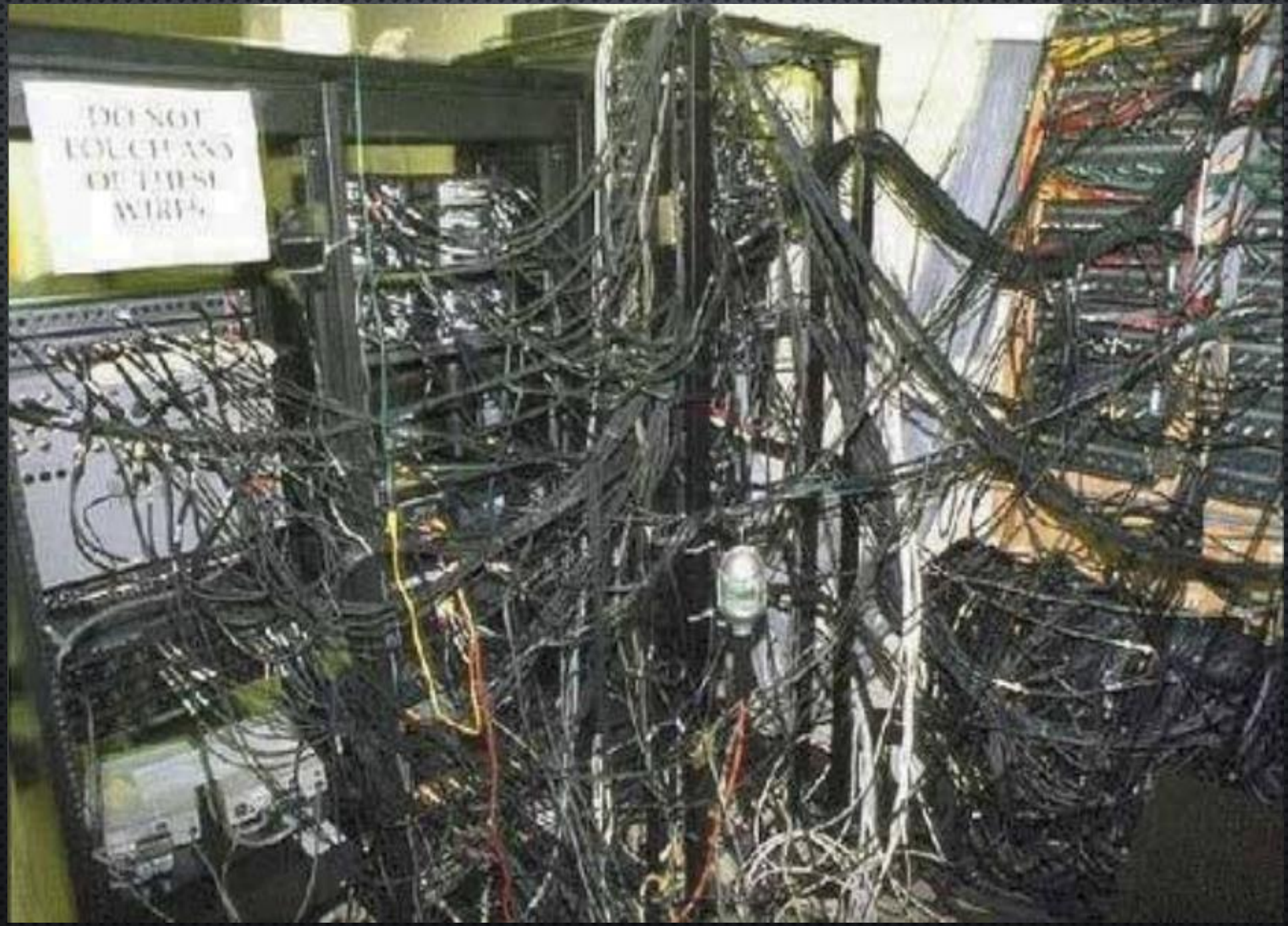
Armas dos "inimigos":

- Todo o tipo de ferramentas que existe na Internet ;

- Negligência do Administrador de Redes;

- Falta de conhecimento do Administrador de Redes; - Falta de infra-estrutura e equipamentos;

- Falta de políticas de segurança e políticas de uso.


DO NOT

S3GUR4NC4 D3 D4D05

Armas do Administrador de Redes:

- Conhecimento ;
- Comprometimento;
- Norma ABNT NBR ISO/IEC 17799:2005 (em fase final ISO/IEC 17799:2007);
- Infra-estrutura e equipamentos;
- Rígidas políticas de segurança e políticas de uso.

S3GUR4NC4 D3 D4D05

Fases da Política de Segurança:

- Projeto*;
- Implementação*;
- Implantação*.

* Norma ABNT NBR ISO/IEC 27002

S3GUR4NC4 D3 D4D05

Relatório SECUNIA (2007):

- o Red Hat Linux apresentou 633 falhas, sendo 629 relacionadas a componentes de terceiros (não incluiu a distribuição Fedora);

- o Solaris fica em segundo lugar, com 252 falhas e 80% delas relacionadas a componentes de terceiros;

- em terceiro está o Mac OS X, com 235 e 62% relacionadas a componentes de terceiros.

- o Windows, que aparece em quarto no ranking dos mais vulneráveis, apresentou 123 falhas, mas 96% delas estavam relacionadas diretamente ao sistema operacional, mas apenas 4% delas foram relacionadas a componentes de terceiros;

- O HP-UX relatou 75 falhas, sendo que 81% delas estavam relacionadas a códigos de terceiros.