



网络安全

常见攻击原理与防御方法

-东南大学网络安全协会 **medition, bright**

第一部分

网络软件安全



1

软件漏洞

2

软件安全防护

3

Web应用系统安全

特点

- 危害性大
- 影响广泛
- 长久存在
- 隐蔽性

分类

- 输入验证错误
- 缓冲区溢出
- 设计错误
- 意外情况处置错误
- 访问验证错误
- 配置错误
- 竞争条件错误
- 环境错误
- 外部数据被异常执行

漏洞库

- CVE (<http://www.cve.mitre.org>)
- BugTraq
(<http://www.securityfocus.com>)
- NVD (<http://nvd.nist.gov>)
- EDB (<http://exploit-db.com>)

漏洞库- CVE -Heartbleed

CVE-ID	
CVE-2014-0160	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
<p>The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.</p>	
References	
<p>Note: <u>References</u> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p>	
<ul style="list-style-type: none">• EXPLOIT-DB:32745• URL:http://www.exploit-db.com/exploits/32745• EXPLOIT-DB:32764• URL:http://www.exploit-db.com/exploits/32764• FULLDISC:20140408 Re: heartbleed OpenSSL bug CVE-2014-0160• URL:http://seclists.org/fulldisclosure/2014/Apr/91• FULLDISC:20140408 heartbleed OpenSSL bug CVE-2014-0160• URL:http://seclists.org/fulldisclosure/2014/Apr/90• FULLDISC:20140409 Re: heartbleed OpenSSL bug CVE-2014-0160• URL:http://seclists.org/fulldisclosure/2014/Apr/109• FULLDISC:20140412 Re: heartbleed OpenSSL bug CVE-2014-0160• URL:http://seclists.org/fulldisclosure/2014/Apr/190• FULLDISC:20140411 MRI Rubies may contain statically linked, vulnerable OpenSSL• URL:http://seclists.org/fulldisclosure/2014/Apr/173• MLIST:[syslog-ng-announce] 20140411 syslog-ng Premium Edition 5 LTS (5.0.4a) has been released• URL:https://lists.balabit.hu/pipermail/syslog-ng-announce/2014-April/000184.html• MISC:http://heartbleed.com/• MISC:http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/	

漏洞库

- CVE (<http://www.cve.mitre.org>)
- BugTraq
(<http://www.securityfocus.com>)
- NVD (<http://nvd.nist.gov>)
- EDB (<http://exploit-db.com>)

漏洞库-BugTraq-index



The screenshot shows the SecurityFocus website interface. At the top, there's a blue header with the SecurityFocus logo and navigation links for 'About' and 'Contact'. Below the header is a yellow banner for 'Symantec Connect' with the text 'A technical community for Symantec customers, end-users, developers, and partners.' and a link to 'Join the conversation'. The main content area is titled 'Vulnerabilities' and lists several security issues in two columns. Each entry includes the vulnerability title, the date (2014-05-21), and a URL to the full report on the SecurityFocus website.

SecurityFocus™ [About](#) [Contact](#)

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
[Join the conversation](#)

Vulnerabilities

Birebin.com for Android CVE-2014-2993 X.509 Certificate Validation Security Bypass Vulnerability 2014-05-23 http://www.securityfocus.com/bid/67524	Cisco WebEx Business Suite 'meetinginfo.do' Information Disclosure Vulnerability 2014-05-21 http://www.securityfocus.com/bid/67424
Apache Struts ClassLoader Manipulation CVE-2014-0114 Security Bypass Vulnerability 2014-05-21 http://www.securityfocus.com/bid/67121	Cisco Unified Web and E-Mail Interaction Manager Session Identifiers Security Bypass Vulnerability 2014-05-21 http://www.securityfocus.com/bid/67495
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability 2014-05-21 http://www.securityfocus.com/bid/51706	Cisco IOS XR Software DHCPv6 Packet Handling CVE-2014-3271 Denial of Service Vulnerability 2014-05-21 http://www.securityfocus.com/bid/67488
OpenSSL TLS 'heartbeat' Extension Multiple Information Disclosure Vulnerabilities 2014-05-21 http://www.securityfocus.com/bid/66690	Cisco IOS Software LLDP Request Processing Denial of Service Vulnerability 2014-05-21 http://www.securityfocus.com/bid/67489
Apple Mac OS X CVE-2014-1322 Local Security Bypass Vulnerability 2014-05-21 http://www.securityfocus.com/bid/67023	Cisco Email Security Appliance Remote Security Bypass Vulnerability 2014-05-21 http://www.securityfocus.com/bid/67494

» [Search all vulnerabilities](#)

漏洞库

- CVE (<http://www.cve.mitre.org>)
- BugTraq
(<http://www.securityfocus.com>)
- NVD (<http://nvd.nist.gov>)
CNNVD(<http://www.cnnvd.org.cn>)
- EDB (<http://exploit-db.com>)

漏洞库

- CVE (<http://www.cve.mitre.org>)
- BugTraq
(<http://www.securityfocus.com>)
- NVD (<http://nvd.nist.gov>)
- EDB (<http://exploit-db.com>)

漏洞库-火狐浏览器空指针引用

Mozilla Firefox 29.0 - Null Pointer Dereference Vulnerability

EDB-ID: [33386](#)

CVE: N/A

OSVDB-ID: [107044](#)

Author: Mr.XHat

Published: 2014-05-16

Verified:

Rating

Overall: (0.0)

Firefox 29 全新发布

下载最新版 Firefox 火狐浏览器，拥有最快、最安全的上网体验



Firefox

免费下载

29.0.1 中文(简体)
Windows

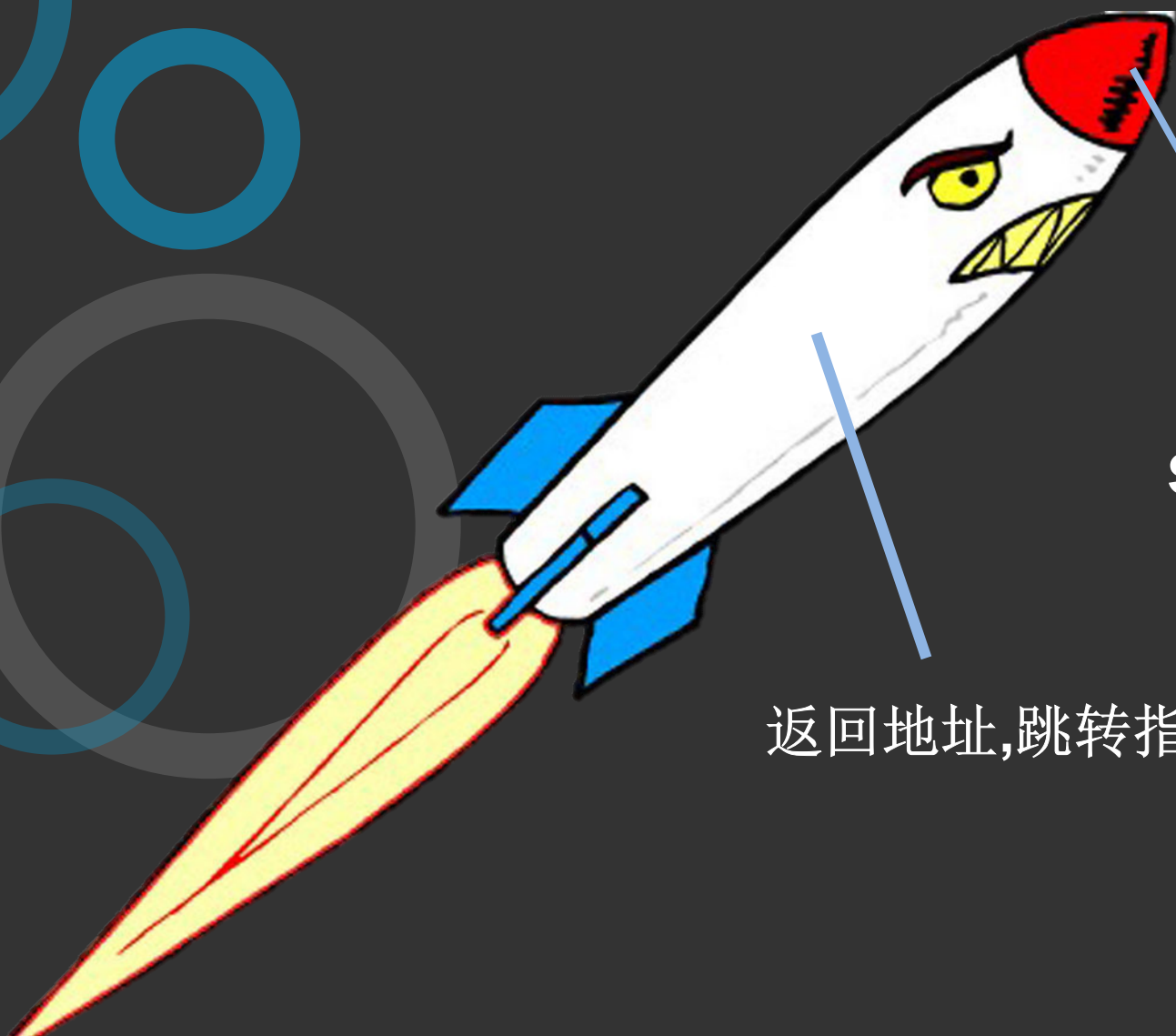
```

9      Date: 4/30/2014
10     Discovered By: Mr.XHat
11     E-Mail: Mr.XHat {AT} GMail.com
12     Tested On: Windows 7 x64 EN
13     #####
14     Disassembly:
15         01694240 8bc2          mov     eax,edx
16         01694242 d9e0          fchs
17         01694244 8b550c        mov     edx,dword ptr [ebp+0Ch]
18         01694247 d95c2418      fstp    dword ptr [esp+18h]
19         0169424b 8b1a          mov     ebx,dword ptr [edx]    ds:0023:00000000=????????
20         0169424d d9442418      fld     dword ptr [esp+18h]
21         01694251 8d4c2420      lea     ecx,[esp+20h]
22         01694255 d9c0          fld     st(0)
  
```

1

软件漏洞

漏洞利用



shellcode

返回地址,跳转指令等

弹头-Shellcode

通过溢出使控制权落在Shellcode手中,进而控制程序运行

Shellcode本身就是一段机器码,可以使用PC02编写再提取,或者直接使用现成的模版.

Shellcode

```
"\xFC\x68\x6A\x0A\x38\x1E\x68\x63\x89\xD1\x4F\x68\x32\x74  
\x91\x0C\x8B\xF4\x8D\x7E\xF4\x33\xDB\xB7\x04\x2B\xE3\x66  
\x03\x33\x32\x53\x68\x75\x73\x65\x72\x54\x33\xD2\x64\x8B\x  
5A\x30\x8B\x4B\x0C\x8B\x49\x1C\x8B\x09\x8B\x69\x08\xAD\x  
3D\x6A\x0A\x38\x1E\x75\x05\x95\xFF\x57\xF8\x95\x60\x8B\x  
45\x3C\x8B\x4C\x05\x78\x03\xCD\x8B\x59\x20\x03\xDD\x33\x  
FF\x47\x8B\x34\x03\x03\xF5\x99\x0F\xBE\x06\x3A\xC4\x74\x  
08\xC1\xCA\x07\x03\xD0\x46\xEB\xF1\x3B\x54\x24\x1C\x75\x  
E4\x8B\x59\x24\x03\xDD\x66\x8B\x3C\x7B\x8B\x59\x1C\x03\x  
DD\x03\x2C\x03\x95\x5F\xAB\x57\x61\x3D\x6A\x0A\x38\x1E\x  
75\xA9\x33\xDB\x53\x68\x31\x32\x33\x34\x68\x31\x32\x33\x3  
4\x8B\xC4\x53\x50\x50\x53\xFF\x57\xFC\x53\xFF\x57\xF8";
```

瞄准系统-返回地址

通过淹没返回地址或者其它手段将进程的控制权送入Shellcode手中

JMP ESP

一个古老而通用的地址: 0x7ff4512

一些基础知识

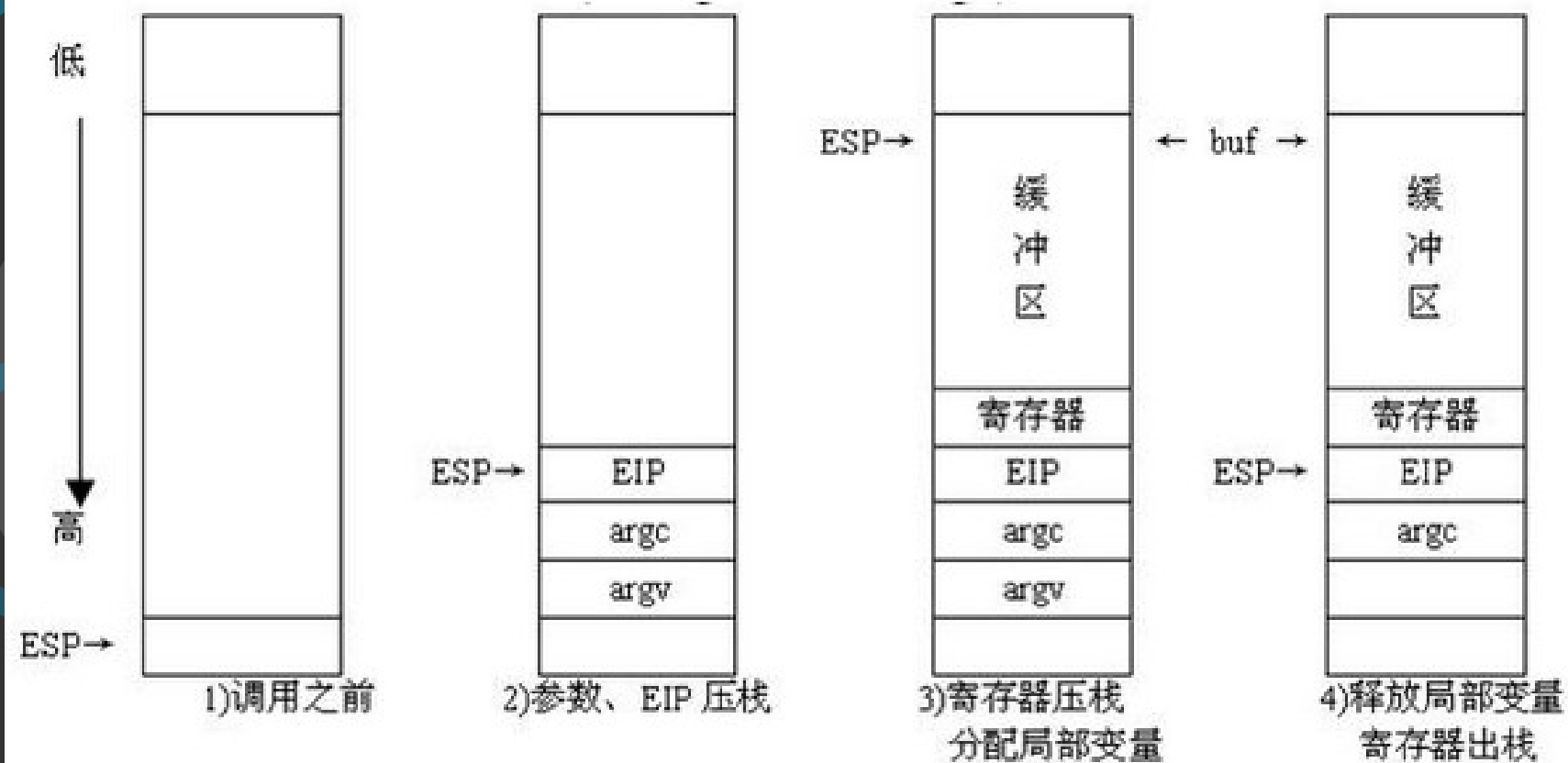
寄存器:

EIP 指令寄存器,指向下一条要执行的指令

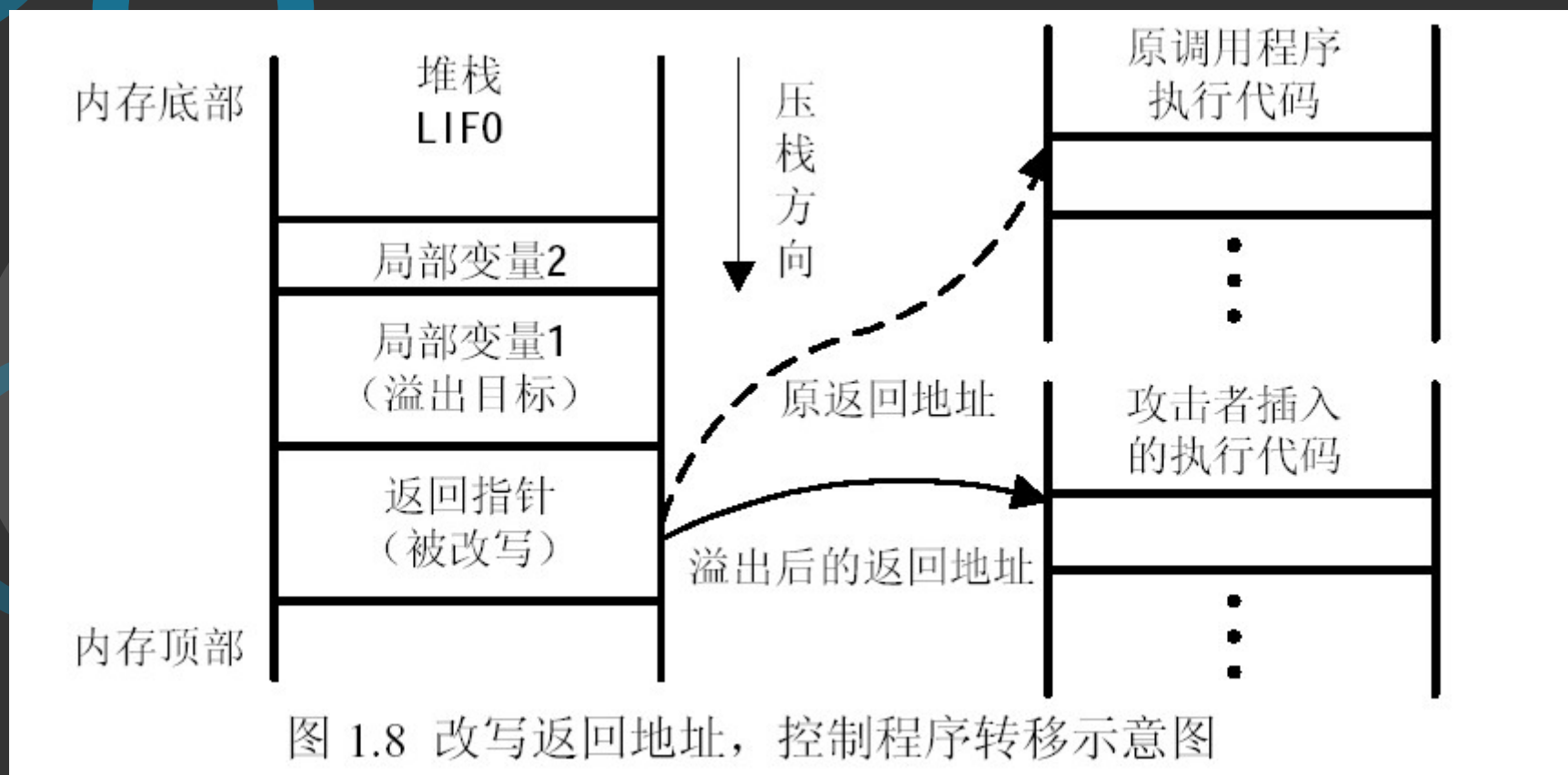
EBP 始终指向当前函数的栈底

ESP 指向当前函数栈帧的栈顶

常见漏洞-缓冲区溢出

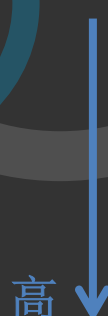


常见漏洞-缓冲区溢出



常见漏洞-缓冲区溢出

```
Void stack_overflow(char *argument){  
    char local[4];  
    for(int i=0;argument[i];i++)  
        local[i]=argument[i];  
}  
stack_overflow("010103030202DDDD");
```



Local	0101
上一个栈帧指针	0303
返回地址	0202
argument	DDDD

常见漏洞-格式化字符串

```
Void formatstring_fun1(char *buf){  
    Char mark[] = "0101"  
    Printf(buf);  
}
```

Formatstring_fun1("%x")

>>231201

常见漏洞-格式化字符串

```
Void formatstring_fun2(char *buf){  
    Char mark[100] ;  
    sprintf(mark,buf);  
}
```

Formatstring_fun2("0101030302%n")

“0x????????”指令引用的
“0x61616161”内存，该内存不能为
write，要终止程序，请单击“确定”

常见漏洞-整数溢出

```
Char *integer_overflow(char *data,size_t len)
{
    size_t size= 0xffffffff+1 = 0x00000000
    char *buffer=(char*)malloc(size);
    if(!buffer) Buffer指向了分配的0大小的内存区域
        return NULL;
    memcpy(buffer,data,len);
    buffer[len]=0;
    return buffer;
}
```

溢出!

常见漏洞-Use-After-Free

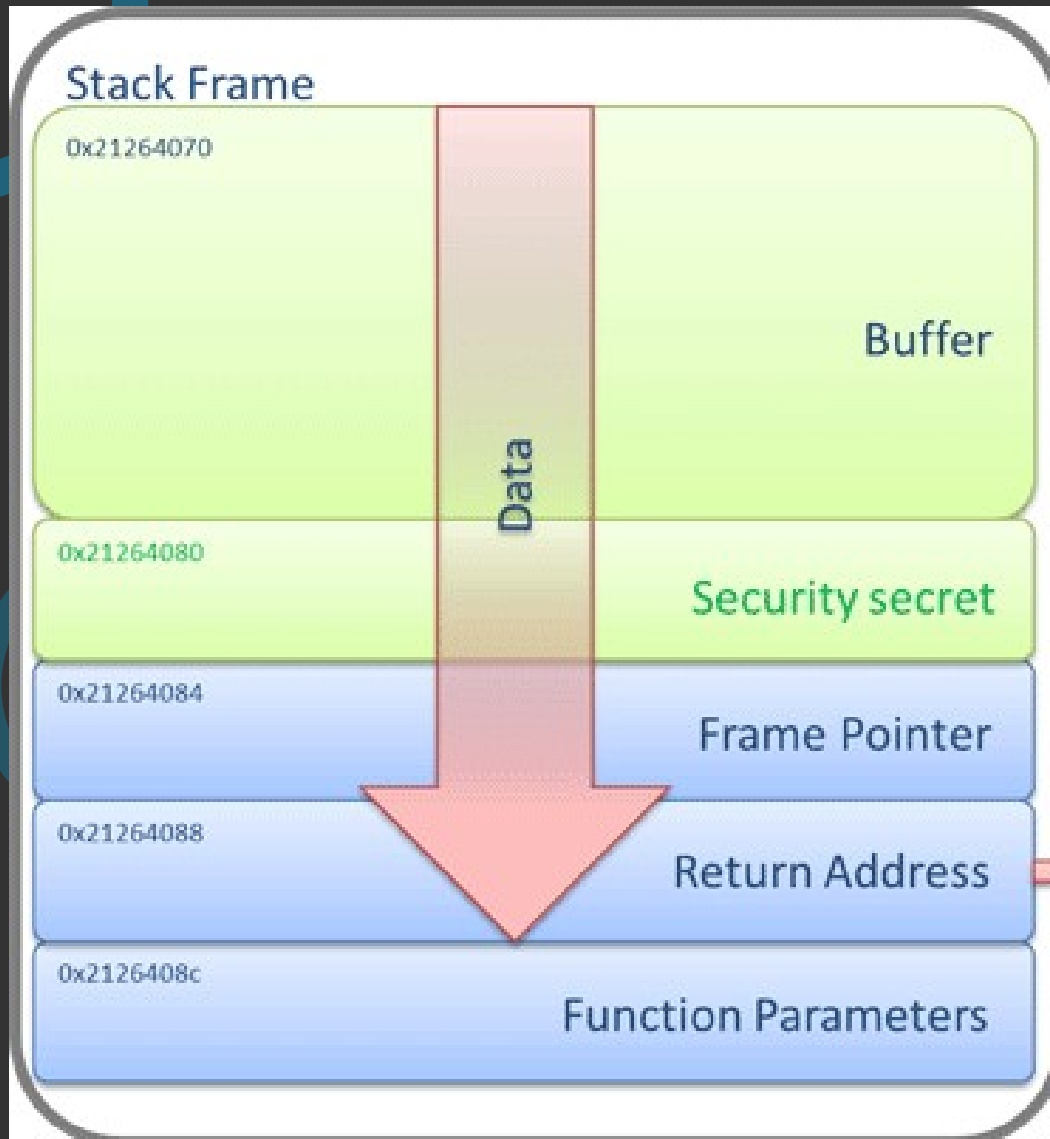
原理:

- 调用Func1(),创建对象Obj1,其内存地址为Addr1,并将Addr1保存在Var1中
- 非正常调用破坏性函数Func3(),释放内存地址Addr1中的对象Obj1
- 调用Func2(),读取Var1中的地址,并访问Var1所指向的Obj1时,发生内存访问异常

Windows的防护技术

- GS Stack protection
- DEP(Data Execute Prevention)
- ASLR(Address Space Layout Randomization)
- SafeSEH(SEH: Structured Exception Handler)

Windows的防护技术



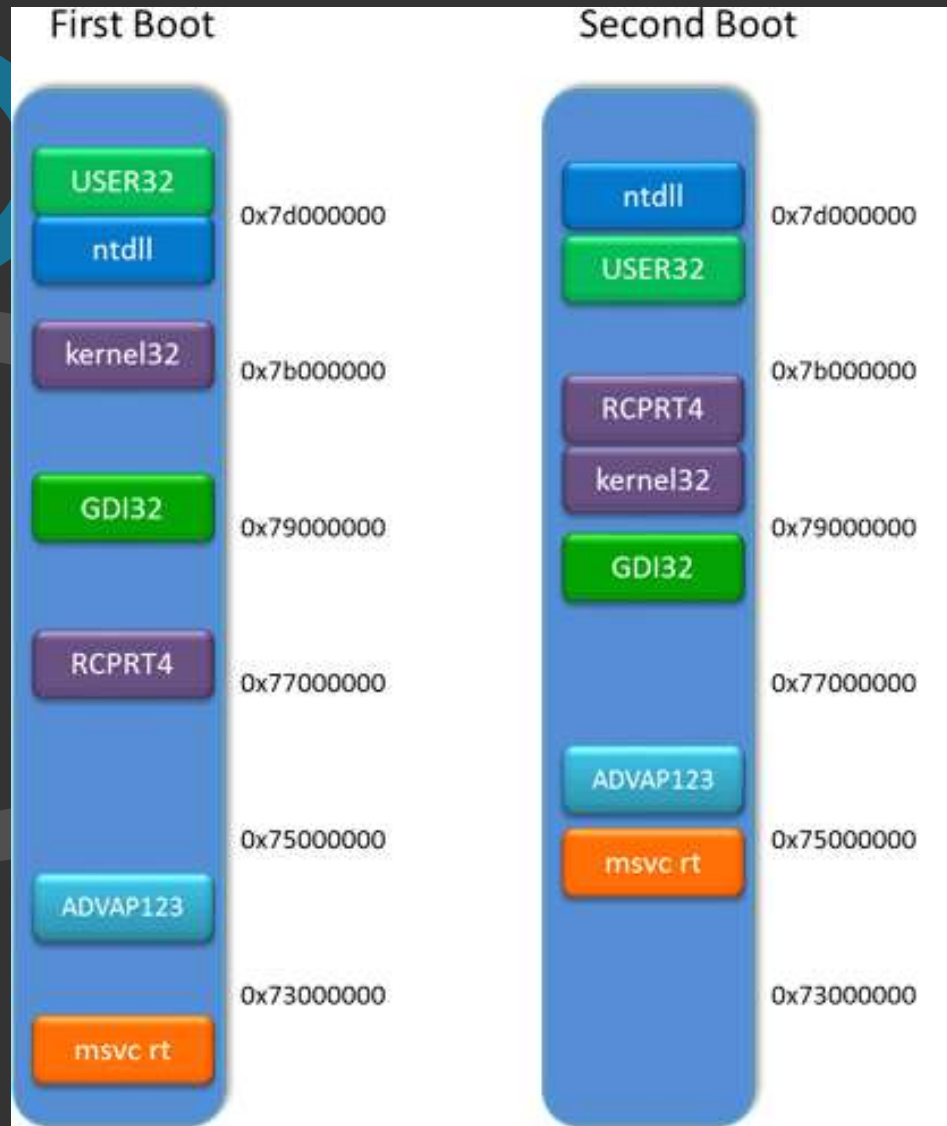
A security secret is placed between local variables and the function return address. Before the function returns the value of the secret is compared with the original. If the comparison fails an exception is raised and the process can be safely terminated



Windows的防护技术

- GS Stack protection
- DEP(Data Execute Prevention)
- ASLR(Address Space Layout Randomization)
- SafeSEH(SEH: Structured Exception Handler)

Windows的防护技术



Windows的防护技术

- GS Stack protection
- DEP(Data Execute Prevention)
- ASLR(Address Space Layout Randomization)
- SafeSEH(SEH: Structured Exception Handler)

Windows的防护技术

- GS Stack protection
- DEP(Data Execute Prevention)
- ASLR(Address Space Layout Randomization)
- SafeSEH(SEH: Structured Exception Handler)

软件保护

- 代码混淆技术
- 软件加壳技术(ASPack UPX PECompact)
- 反调试反跟踪技术

软件保护-代码混淆

加密前

此文件受保护，请不要修改任何代码以免PHP无法运行。

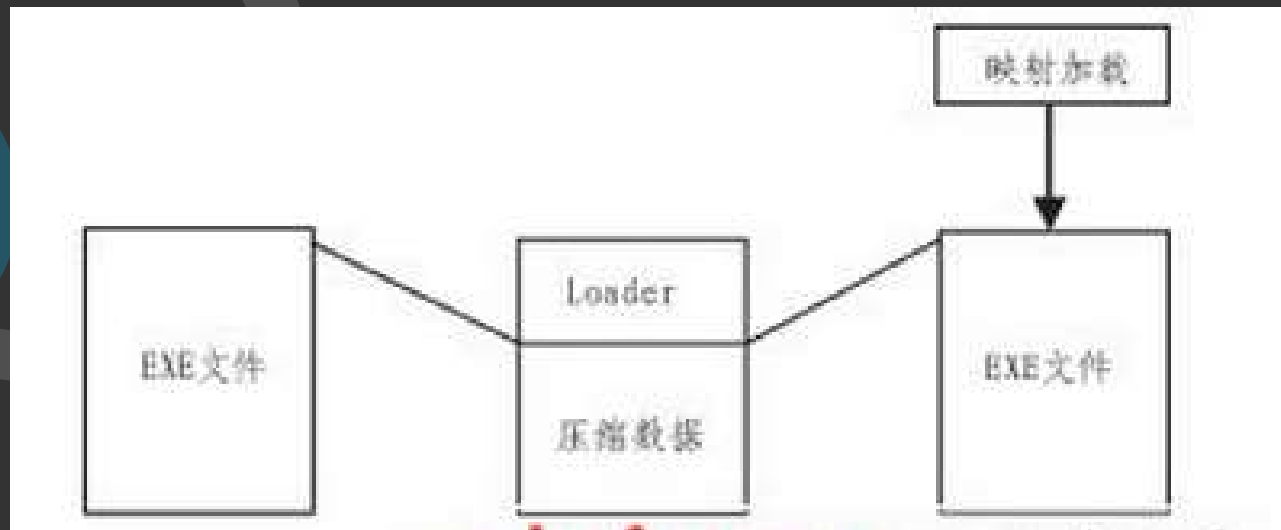
* /

加密后

软件保护

- 代码混淆技术
- 软件加壳技术(ASPack UPX PECompact ASProtect)
- 反调试反跟踪技术

软件保护-加壳

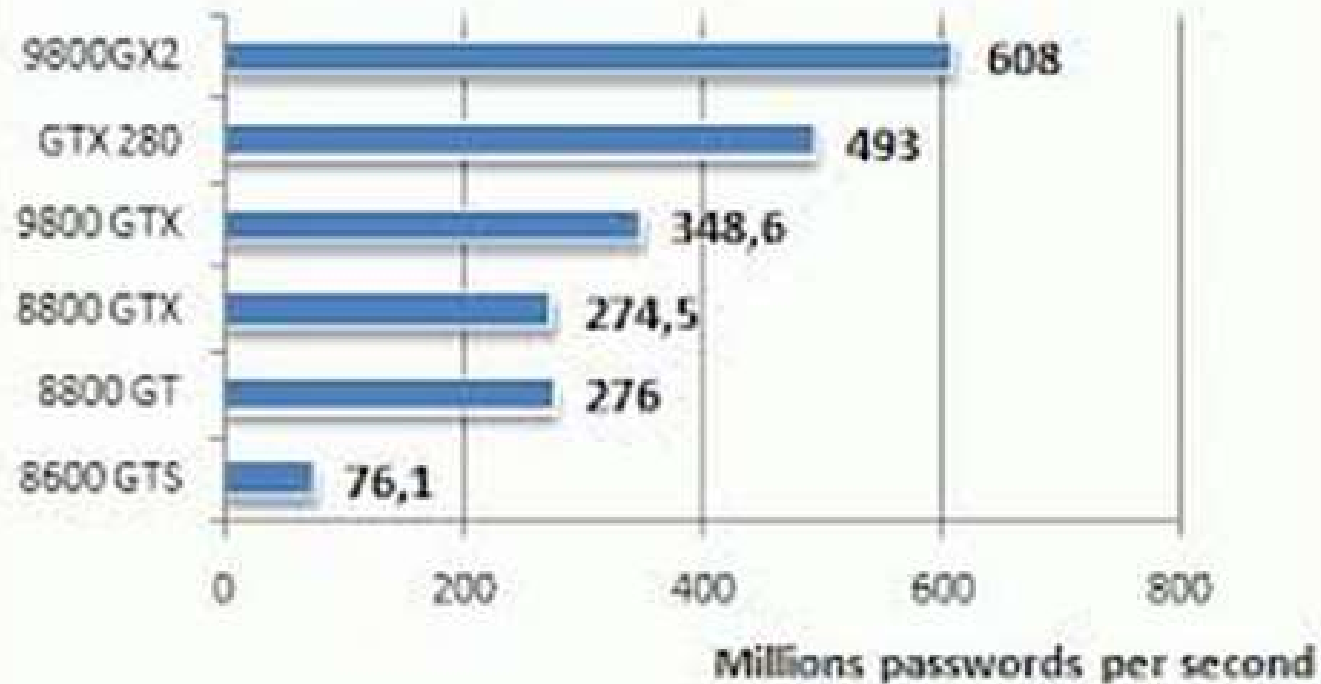


软件保护

- 代码混淆技术
- 软件加壳技术(ASPack UPX PECompact)
- 反调试反跟踪技术

遭破坏的身份认证和会话管理

Lightning Hash Cracker Benchmarks



遭破坏的身份认证和会话管理

- 用户认证需要通过加密信道进行传输

POST: http://text.com/login.php

HOST: text.com

User-Agent : Python

.....

Content-Type: application/x-www-form-
urlencoded

Content-length: 37

User=test&password=test&Submit=submit

不安全的加密存储

例如:2012年CSDN网站600万账户密码泄露事件.该时间之所以严重因为CSDN网站采取了明文方式存储了用户名和密码.

解决方法:

密码等信息使用HASH函数加盐处理,登录时进行相同运算,比较HASH值

例如: Md5(userpassword+"salt")

未验证的重定向及转发

例如:

一个登录页面的地址为:

`http://test.com/login.php? fwd=index`

`php`

登录完成之后将被重定向到 `index.php`, 如果恶意的中间的修改了 `fwd`, 将会导致用户被重定向到恶意网页.

防范方法:

对输入的参数进行验证

Web安全防护

客户端防护

使用最新的浏览器

不轻易点击他人发送的URL

不浏览低俗网站

通信信道防护

使用HTTPS传输敏感数据

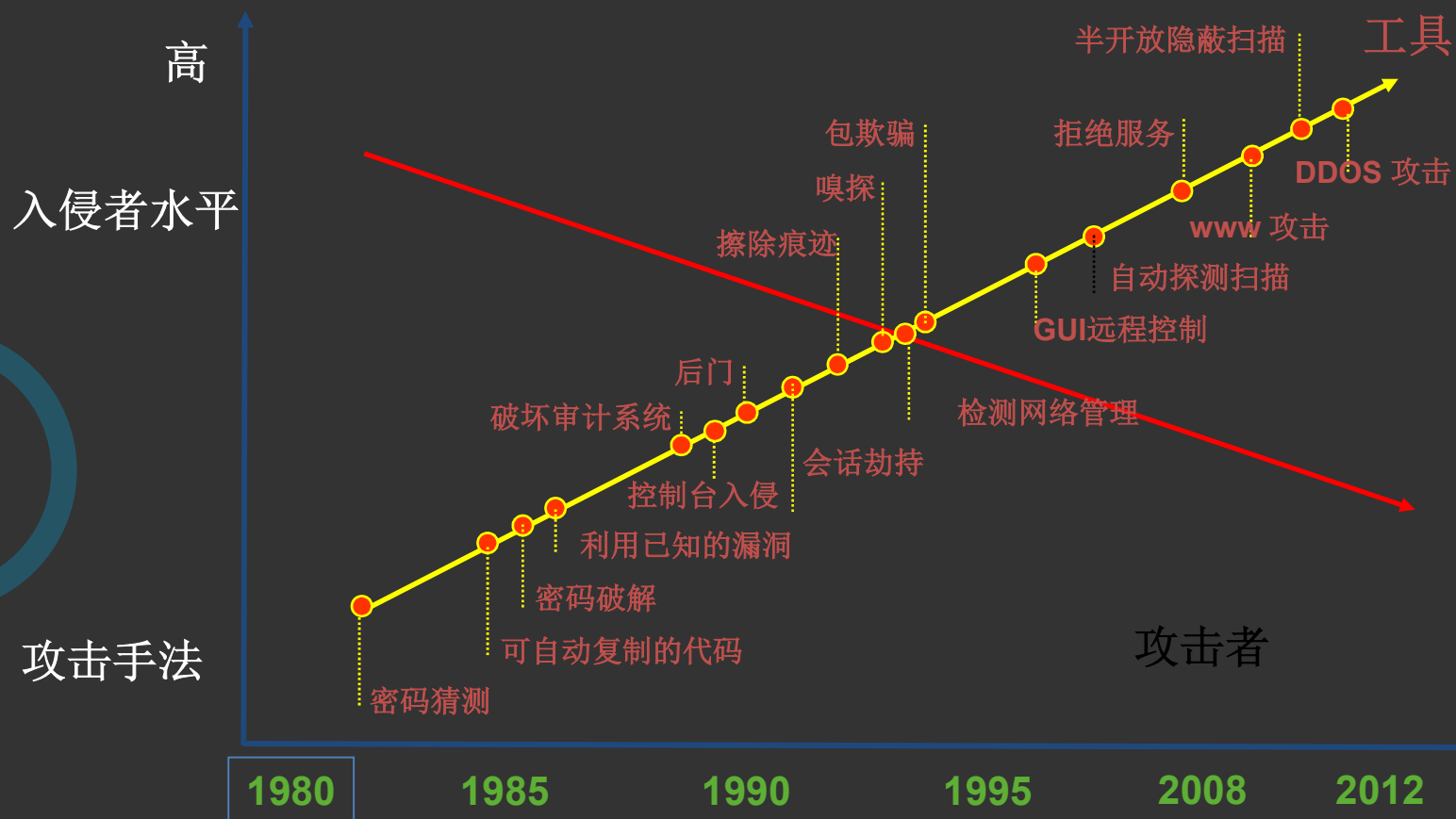
服务器防护

关闭不使用的服务及端口

及时打上最新补丁

进行必要的安全控制

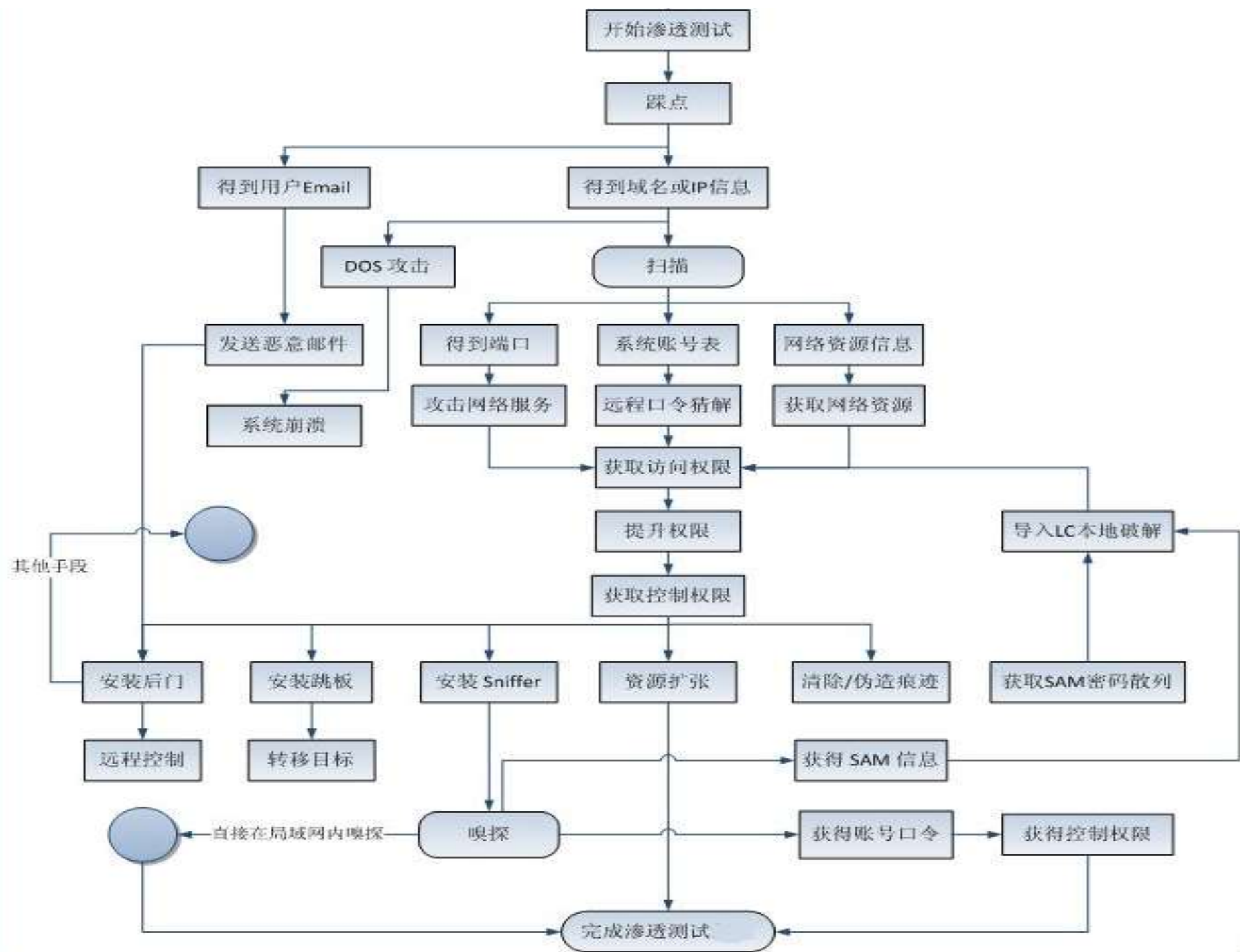
常见的Web攻击方法及入侵技术的发展





网络安全攻击技术

网络安全防护技术



网络安全攻击技术

1

扫描技术

2

网络欺骗攻击

3

拒绝服务攻击

4

web脚本攻击

扫描技术概述

网络扫描是攻击者在实施网络攻击之前必要的信息收集步骤。通过网络扫描，可以获取被攻击目标的IP、端口、操作系统版本、存在的漏洞等攻击必需信息，为实施下一步的网络攻击做好前期准备。具体的扫描技术包括：互联网信息的收集、IP地址扫描、网络端口扫描、漏洞扫描、弱口令扫描、综合漏洞扫描等

扫描技术

互联网信息收集：

whois查询、google hack搜集敏感信息

IP地址扫描：

ping 方法获取IP

网络端口扫描：

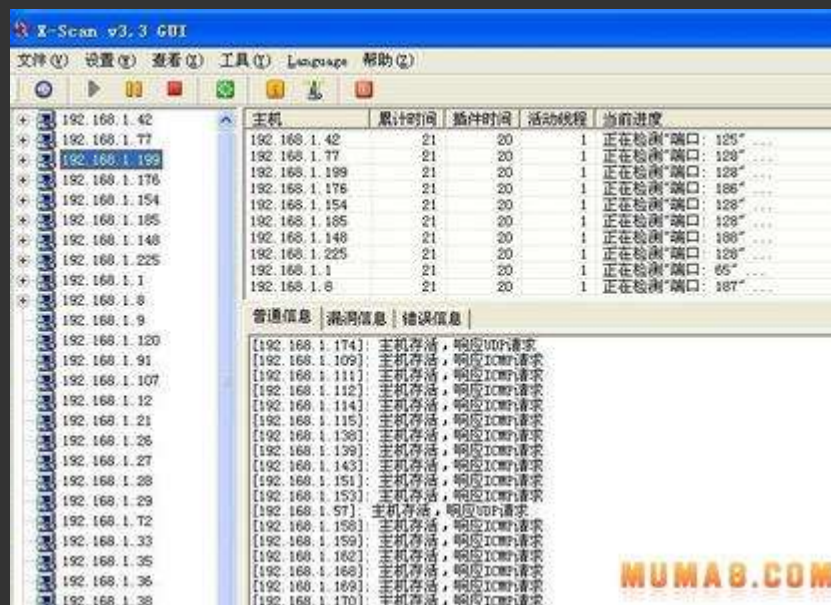
扫描目标主机开放端口（Nmap）

漏洞扫描：

网络漏洞扫描（wvs）、主机漏洞扫描（x-scan）

弱口令扫描：

探测服务器或web管理员的用户名和密码

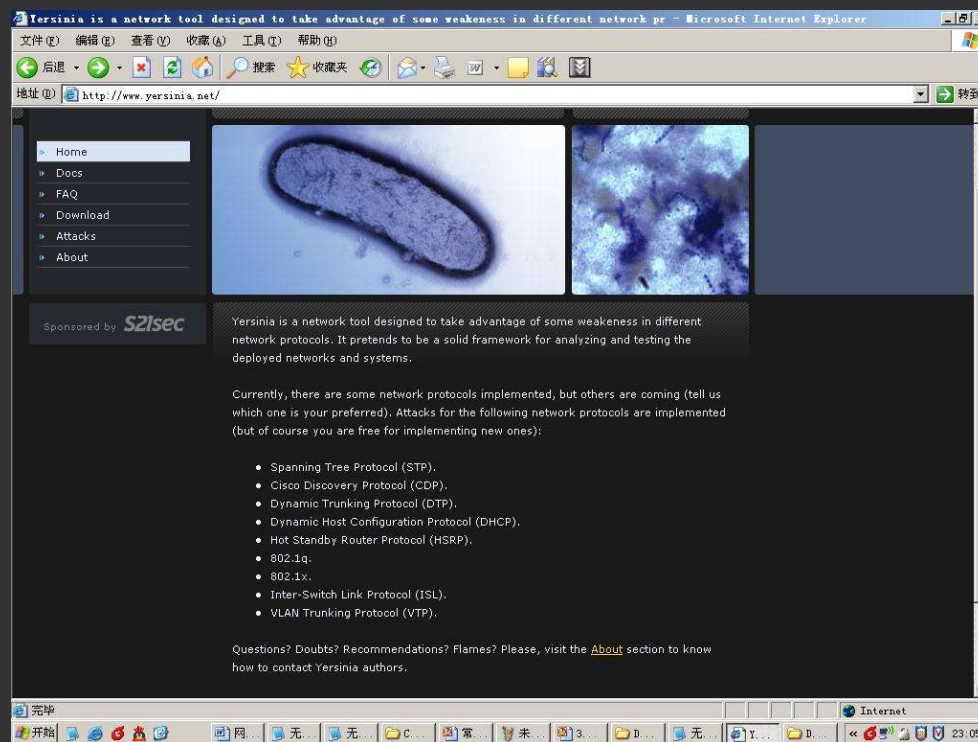


针对端口扫描的主要防御手段

- 1.关闭不必要的端口
- 2.利用数据包过滤型防火墙过滤非法数据包
- 3.利用入侵检测系统

网络欺骗

- 网络设备、网络服务的欺骗
 - Yersinia
- IP地址、MAC地址欺骗
 - IP地址冲突问题
 - ARP协议之中间人攻击
- 应用层的钓鱼攻击
 - 电子邮件欺骗
 - 虚假网站欺骗
- 社会工程学

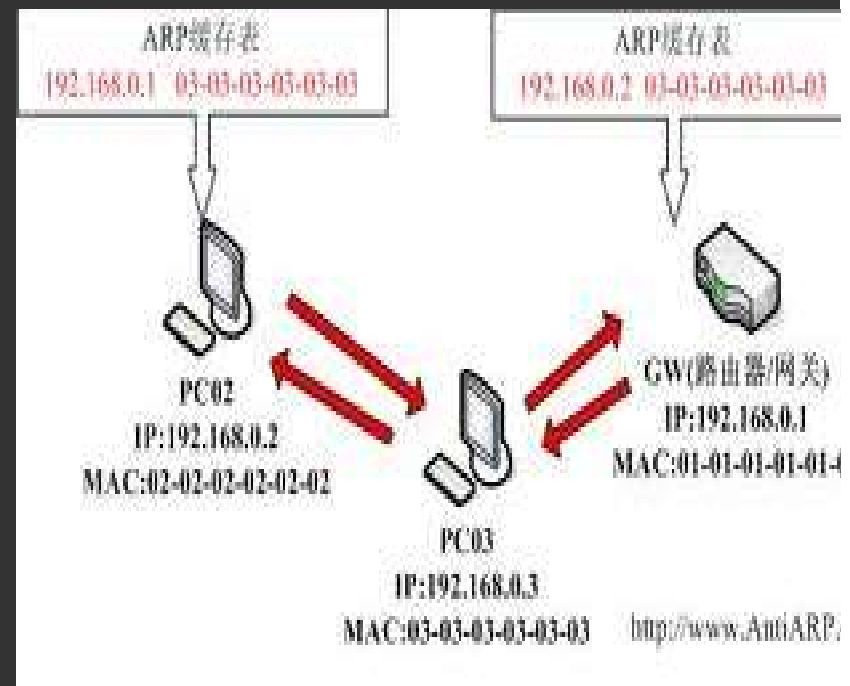


IP地址、MAC地址欺骗

- IP是网络层的一个非面向连接的协议，伪造IP地址相对容易。
 - DoS攻击为其实例
 - IP地址冲突
 - IP广播风暴
- ARP协议的安全缺陷
 - ARP风暴
 - 中间人攻击

ARP (Address Resolution Protocol)

- 正常情况下GW和PC02之间进行通讯，但是此时PC03向GW发送一个自己伪造的ARP应答，而这个应答中的数据为发送方IP地址是192.168.0.2（PC02的IP地址），MAC地址是03-03-03-03-03-03（PC02的MAC地址本来应该是02-02-02-02-02-02，这里被伪造了）。当GW接收到PC03伪造的ARP应答，就会更新本地的ARP缓存（GW被欺骗了），这时PC03就伪装成PC02了。同时，PC03同样向PC02发送一个ARP应答，应答包中发送方IP地址四192.168.0.1（GW的IP地址），MAC地址是03-03-03-03-03-03（GW的MAC地址本来应该是01-01-01-01-01-01），当PC02收到PC03伪造的ARP应答，也会更新本地ARP缓存（PC02也被欺骗了），这时PC03就伪装成了GW。这样主机GW和PC02都被主机PC03欺骗，GW和PC02之间通讯的数据都经过了PC03。主机PC03完全可以知道他们之间说的什么：）。这就是典型的ARP欺骗过程。



SMTP邮件协议

SMTP 命令

HELP

HELO

MAIL FROM

RCPT TO:

DATA

QUIT

QUIT<CRLF>

结束邮件传递，释放邮件连接

注：<CRLF>表示回车换行。

```
C:\WINDOWS\system32\cmd.exe
220 server2003.hm.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at
Mon, 30 Mar 2009 21:48:38 +0800
helo
250 server2003.hm.com Hello [192.168.0.20]
mail from:hanmei@hm.com
250 2.1.0 hanmei@hm.com....Sender OK
rcpt to:xueyuhan@hm.com
250 2.1.5 xueyuhan@hm.com
data
354 Start mail input; end with <CRLF>.<CRLF>
from:hanmei@hm.com
to:xueyuhan@hm.com
subject:test
test ok?
250 2.6.0 <SERVER2003cd9gKY1Na000000002@server2003.hm.com> Queued mail for delivery
quit
221 2.0.0 server2003.hm.com Service closing transmission channel

失去了跟主机的连接。

G:\Documents and Settings\hanmei>
```

邮件正文

from: 发件人, to: 收件人, subject: 主题, 后接正文, . 作为结束符

from 和 to 可省略不写

出有关帮助信息

己的 Email 域名

mail 地址传送到;

mail 地址传递到;

本命令

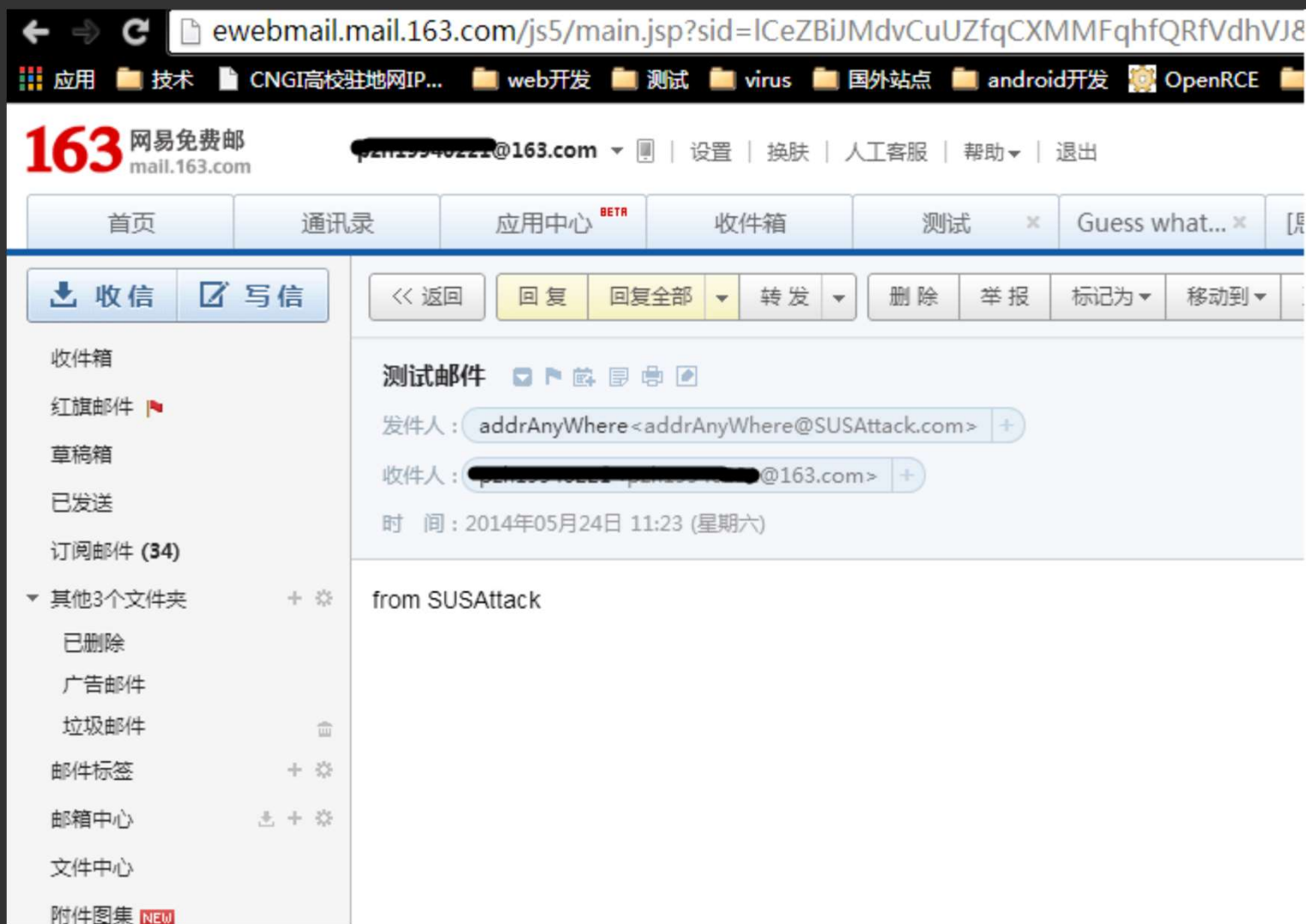
数据, 用第一列;

的一行结束

51CTO.com
技术博客

应用层攻击之邮件欺骗

- 交易网站的欺骗邮件



邮件欺骗的检测防范

← → ↻ ewebmail.mail.163.com/js5/main.jsp?sid=ICeZBiJMdvCuUZfqCXMMFqhfQRfVdhVJ8

应用 技术 CNGI高校驻地网IP... web开发 测试 virus 国外站点 android开发 OpenRCE

163 网易免费邮 mail.163.com pzh19940221@163.com 设置 换肤 人工客服 帮助 退出

首页 通讯录 应用中心 ^{BETA} 收件箱 测试 × Guess what... ×

← → ↻ ewebmail.mail.163.com/js5/main.jsp?sid=ICeZBiJMdvCuUZfqCXMMFqhfQRfVdhVJ&df=mail163

应用 技术 CNGI高校驻地网IP... web开发 测试 virus 国外站点 android开发 OpenRCE 比赛 Em

163 网易免费邮 mail.163.com pzh19940221@163.com 设置 换肤 人工客服 帮助 退出

首页 通讯录 应用中心 ^{BETA} 收件箱 **测试邮件** ×

↓ 收信 写信

收件箱
红旗邮件
草稿箱
已发送
订阅邮件 (34)
其他3个文件夹 + ✖
已删除
广告邮件
垃圾邮件
邮件标签 + ✖
邮箱中心 云 + ✖

<< 返回 回复 回复全部 转发 删除 举报 标记为 移动到 更多

发件人: addrAnyWhere <addrAnyWhere@SUSAttack.com> +

收件人: [REDACTED]@163.com> +

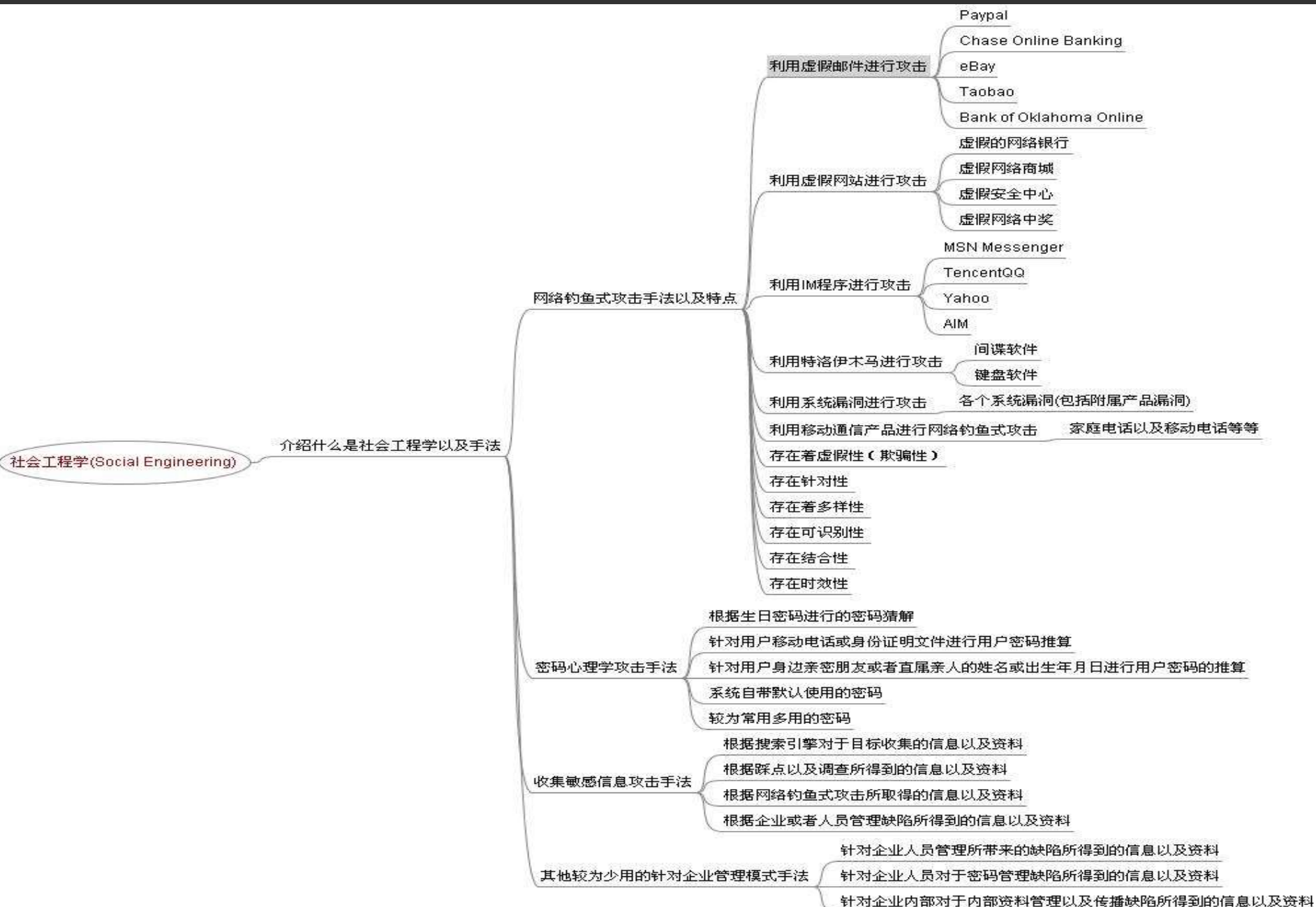
时 间: 2014年05月24日 11:23 (星期六)

Received: from SUSAttack.com (unknown [219.234.4.191])
by mx44 (Coremail) with SMTP id XsCowEDJSEPCeIBT4PHfAA--.891S2;
Sat, 24 May 2014 11:23:46 +0800 (CST)
From: addrAnyWhere@SUSAttack.com
To: pzh19940221@163.com
Subject: =?utf-8?Q?=E6=B5=8B=E8=AF=95=E9=82=AE=E4=BB=B6?=
Message-Id: <4076ec32c8a4fa79753c93a954ae8b74e2666ab7@www.chacuo.net>
Date: Sat, 24 May 2014 11:23:45 +0800
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline
MIME-Version: 1.0

应用层攻击之虚假网站



社会工程学



■ 常用手段

- 伪装
- 引诱
- 恐吓
- 说服
- 恭维
- 渗透

■ 另类方式

- 翻垃圾
- 背后偷窥
- 反向社会工程

■ 防御手段

- 从技术上避免网站被仿冒
- 严格的内部安全控制
- 进行员工安全意识训练

拒绝服务攻击类型的划分

攻击类型划分I

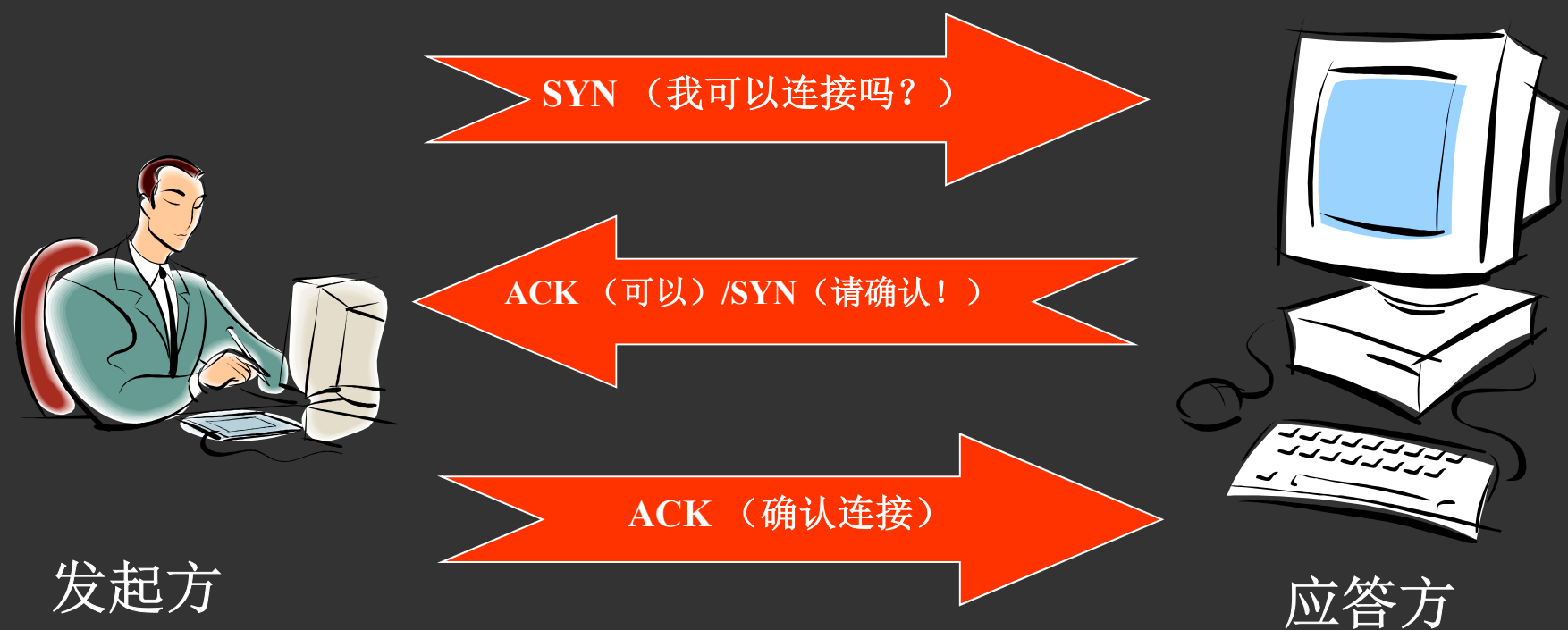
- 堆栈突破型（利用主机/设备漏洞）
 - 远程溢出拒绝服务攻击
- 网络流量型（利用网络通讯协议）
 - SYN Flood
 - ACK Flood
 - ICMP Flood
 - UDP Flood
 - Connection Flood
 - HTTP Get Flood

攻击类型划分II

- 应用层
 - 垃圾邮件、病毒邮件
 - DNS Flood
- 网络层
 - SYN Flood、ICMP Flood
 - 伪造IP包
- 链路层
 - ARP 伪造报文
- 物理层
 - 直接线路破坏
 - 电磁干扰

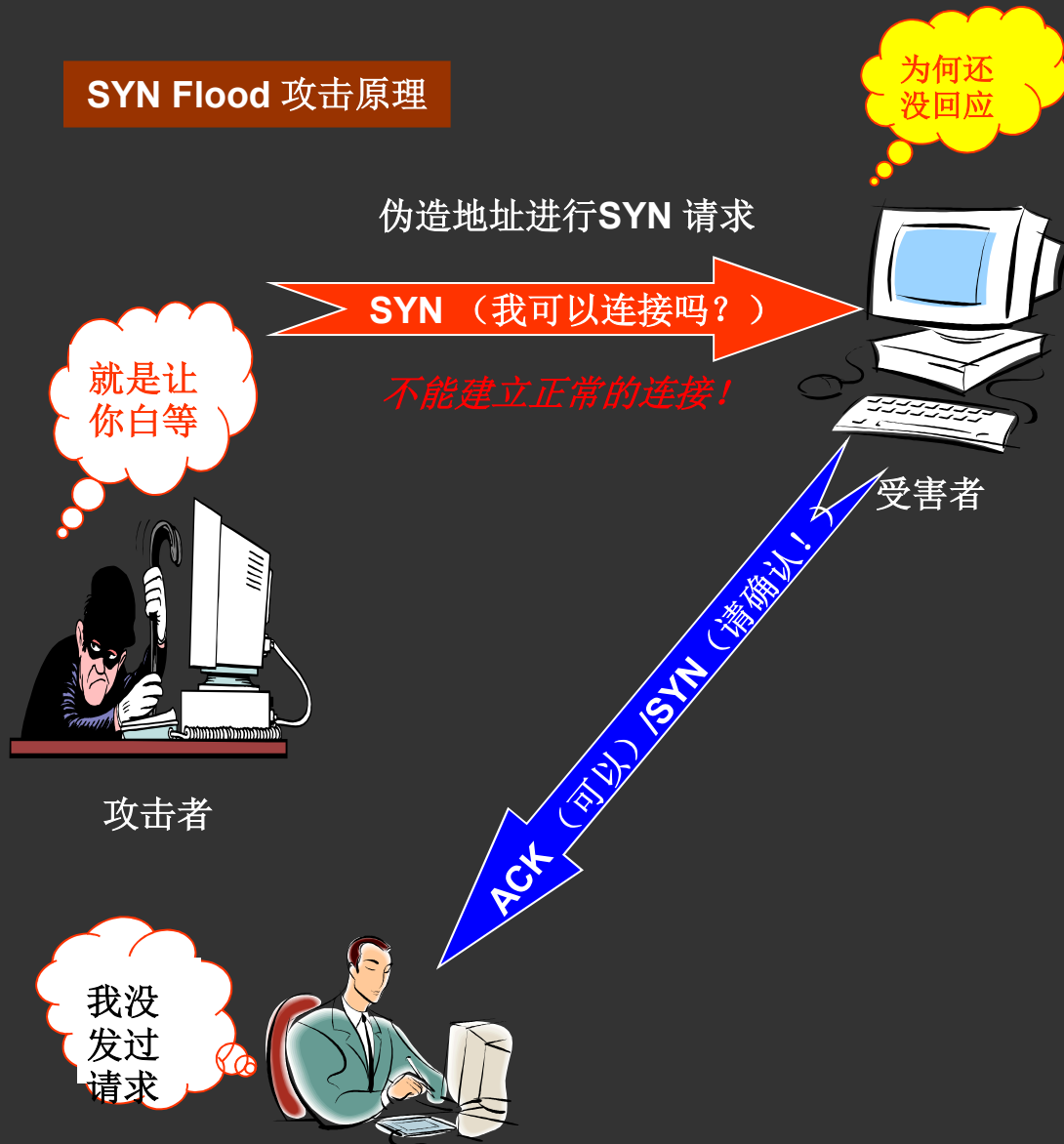
TCP三次握手原理

- 正常的三次握手建立通讯的过程



SYN Flood 攻击原理

SYN Flood 攻击原理

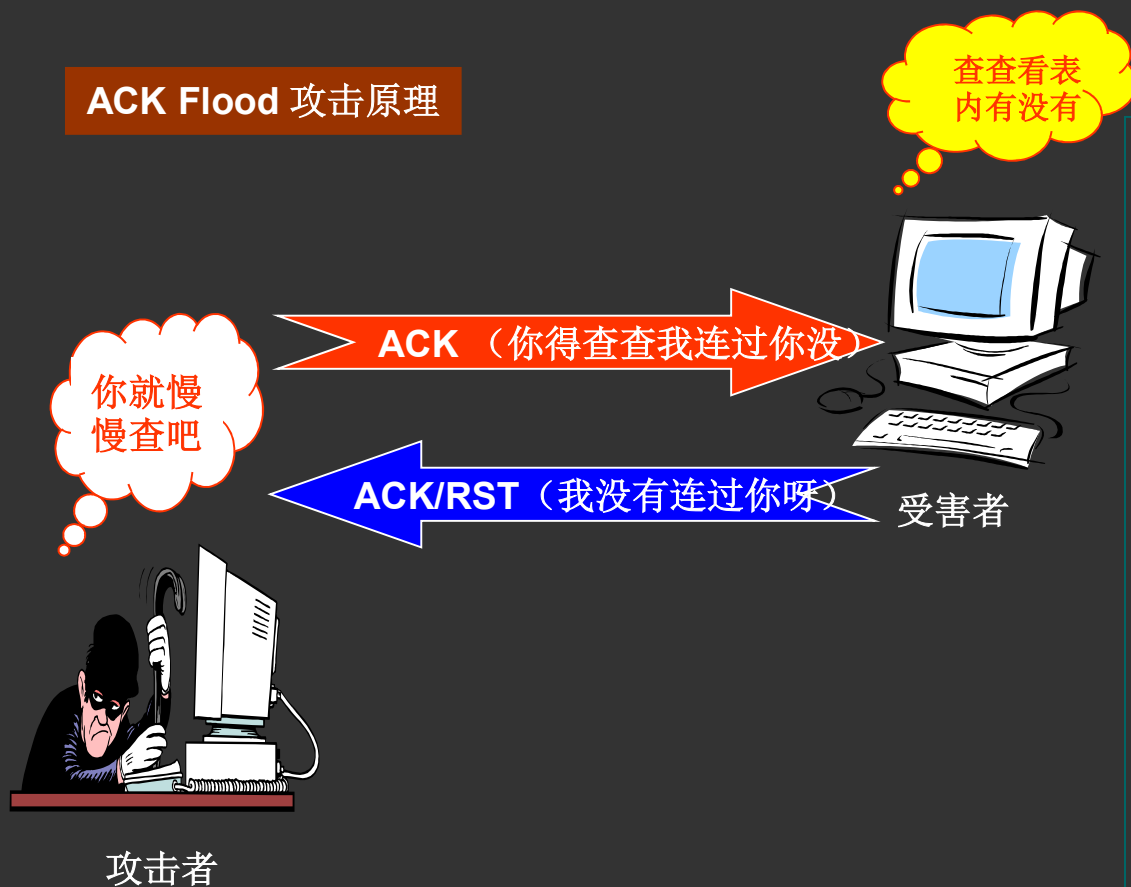


攻击表现

- SYN_RECV状态
- 半开连接队列
 - 遍历, 消耗CPU和内存
 - SYN|ACK 重试
 - SYN Timeout: 30秒~2分钟
- 无暇理睬正常的连接请求—拒绝服务

ACK Flood攻击原理

ACK Flood 攻击原理

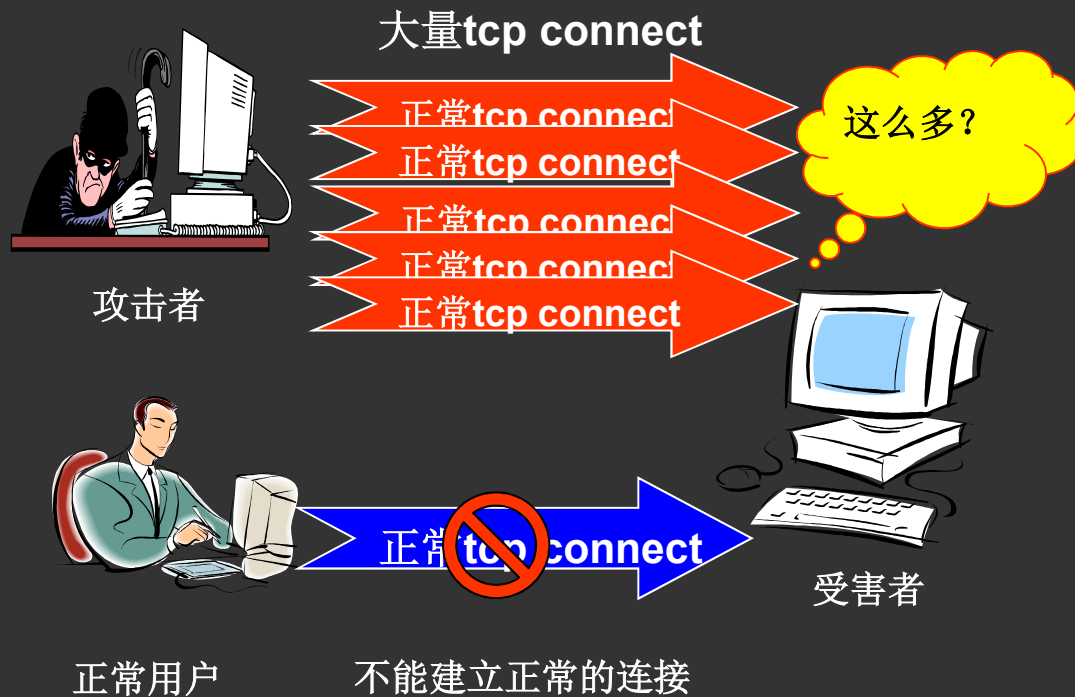


攻击表现

- 大量ACK冲击服务器
- 受害者资源消耗
 - 查表
 - 回应ACK/RST
- ACK Flood流量要很大才会对服务器造成影响

Connection Flood攻击原理

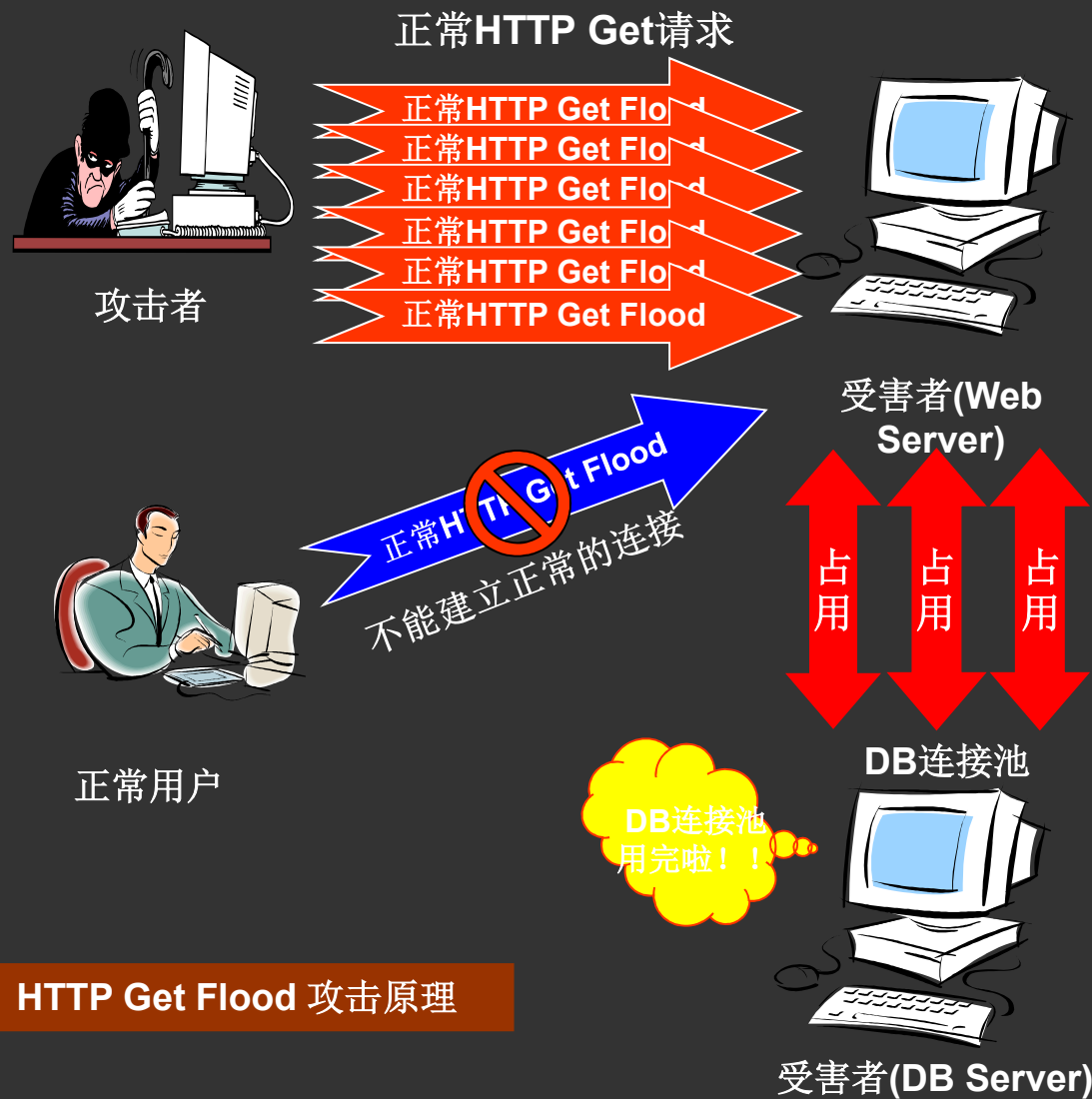
Connection Flood 攻击原理



攻击表现

- 利用真实 IP 地址（代理服务器、广告页面）在服务器上建立大量连接
- 服务器上残余连接 (WAIT状态) 过多，效率降低，甚至资源耗尽，无法响应
- 消耗骨干设备的资源，如防火墙的连接数

HTTP Get Flood 攻击原理



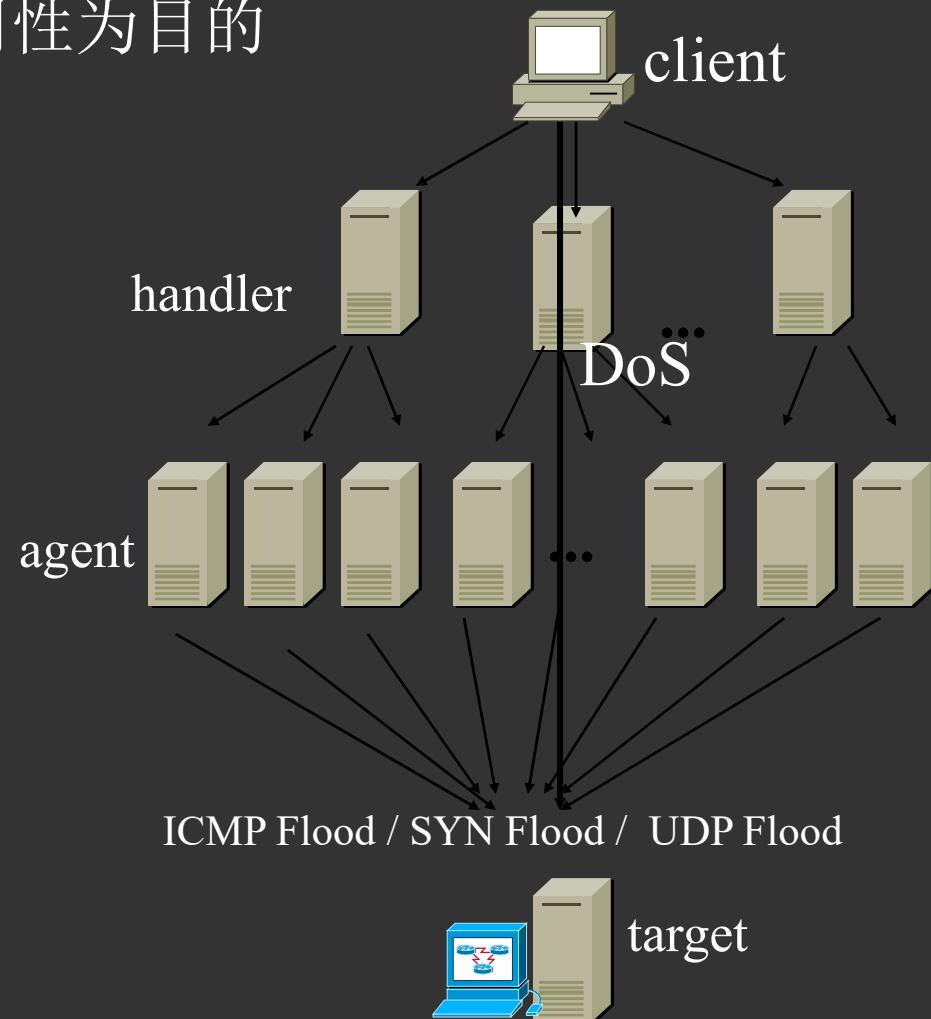
HTTP Get Flood 攻击原理

攻击表象

- 利用代理服务器向受害者发起大量HTTP Get请求
- 主要请求动态页面，涉及到数据库访问操作
- 数据库负载以及数据库连接池负载极高，无法响应正常请求

分布式拒绝服务（DDoS）

- 以破坏系统或网络的可用性为目的
- 常用的工具：
 - Trin00
 - TFN/TFN2K
 - Stacheldraht
- 很难于防范
- 伪造源地址，流量加密
因此很难跟踪

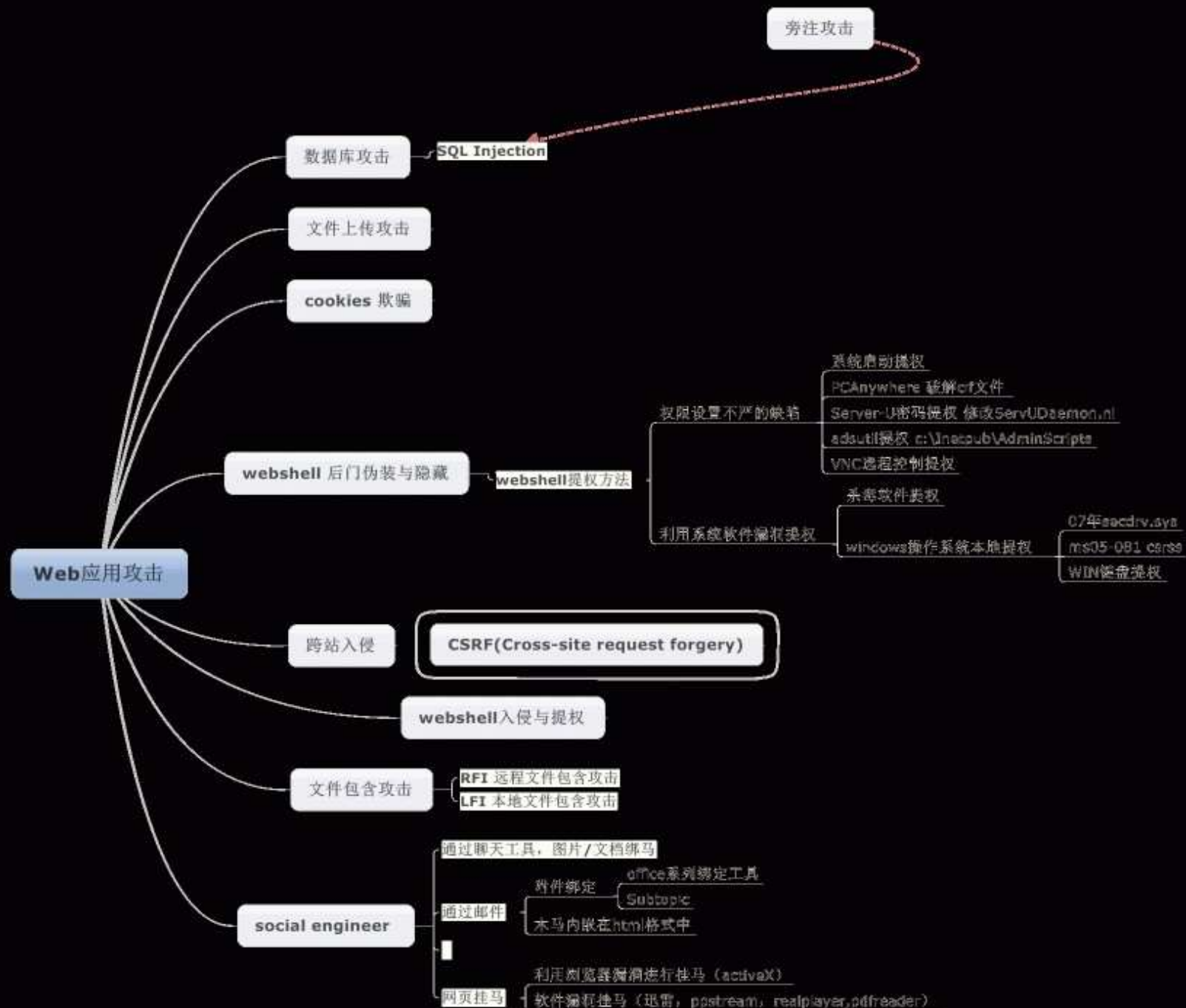


DoS攻击的检测

- 根据异常情况分析
 - 访问量突然剧增，经过sniffer分析，有大量的非正常的包，如没有正常的tcp三次握手，或者是三次握手后没有正常的关闭连接，或者大量的广播包，或者大量的icmp包，这说明极有可能是遭受DoS攻击。
 - 主机反应很迟钝, 两种可能，一种是流量确实很大，有可能是遭受DoS攻击，还有就是应用程序编写有误，导致系统资源耗尽。
- 安全设备报警
 - 入侵检测、防火墙、防毒软件提示

Web应用程序安全漏洞类型列表

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6



SQL注入攻击原理

一条没有任何过滤的sql语句:

```
$sql = "SELECT * FROM a02ounts where  
      username='".$_POST['username']."' and  
      passwd='".$_POST['passwd']."'";
```

SQL注入攻击原理

正常情况

用户名: **guojing**; 口令: **123456**

正常SQL: **SELECT * from FROM a02ounts WHERE
username ='guojing' AND passwd = '123456'**

恶意代码

用户名/口令: **huangrong' OR '1'='1**

注入SQL结果: **SELECT * from FROM a02ounts
WHERE username ='huangrong' OR '1'='1'
AND passwd = 'huangrong' OR '1'='1'**

等价于: **SELECT * from FROM a02ounts**

后果: 绕过了**login.php**用户身份认证的正常逻辑, 获得访问权限

SQL注入攻击防范措施

使用类型安全(**type-safe**)的参数编码机制

凡是来自外部的用户输入，必须进行完备检查

“限制、拒绝、净化”

URLScan过滤器:丢弃不符合规则的输入

将动态**SQL**语句替换为存储过程、预编译**SQL**或**ADO**
命令对象

加强**SQL**数据库服务器的配置与连接

避免将敏感性数据(如口令)明文存放于数据库中

最小权限原则配置**Web**应用程序连接数据库的查询操作权限

实现一个不泄漏任何有价值信息的默认出错处理机制

跨站脚本攻击

(XSS: Cross-Site Scripting)

`<script>alert(document.cookie)</script>`



跨站脚本攻击

(XSS: Cross-Site Scripting)

什么是跨站脚本? (Wikipedia)

跨站脚本是一种通常存在于**Web**应用程序中的安全漏洞，使得攻击者可以将恶意的代码注入到网页中，从而危害其他**Web**访问者。

客户端脚本: **Javascript, Flash ActionScript**
等

与代码注入攻击的比较

相似的漏洞根源: **Web**应用程序没有对非预期输入做全面有效检查和净化.

不同的最终攻击目标

代码注入: **Web**站点

XSS: 访问**Web**应用程序的其他用户

XSS跨站脚本攻击防范措施

服务器端防范措施-“限制、拒绝、净化”

输入验证: 对用户提交数据进行尽可能严格的验证
与过滤

输出净化: **HTMLEncode()**方法

消除危险的输入点

客户端防范措施

提高浏览器访问非受信网站时的安全等级

安全意识和浏览习惯->非主流浏览器**Chrome,**
Safari, Opera

The background of the slide is a dark charcoal grey. On the left side, there is a cluster of overlapping circles. These circles are in three colors: a vibrant blue, a clean white, and a light grey. Some circles are solid, while others are just outlines. Some of the white circles have a small white dot on their circumference. The circles vary in size and are arranged in a way that creates a sense of depth and movement. On the right side of the slide, the words "Thank You" are written in a clean, sans-serif font. The word "Thank" is in the same vibrant blue as some of the circles, while "You" is in white. The text is positioned in the upper right quadrant of the slide.

Thank You