TREND MICRO 趋势科技

全程护航
迈向云端

虚拟补丁防护解析

Freda Zhang
趋势科技培训部

DeepSecurity防护特点-虚拟补丁

- 漏洞被公布，但是厂商还没提供相关补丁进行修补
- 操作系统或应用软件厂商已经停止提供修复补丁
- 服务器的补丁部署，往往需要重新启动，会造成业务中断

TREND MICRO 趋势科技

DeepSecurity防护特点-虚拟补丁

F	虚拟补丁防护
A	采用防护层方式非本地修复系统及应用安全漏洞
B	采用最简便，稳定方式快速修复漏洞，保护系统及应用

- 虚拟补丁防护：
  - 操作系统，应用程序
  - 无需本地安装
  - 深度数据包过滤规则，免受未打补丁的漏洞攻击
  - 作为补丁，修补程序和更新建议扫描：
    - 推荐分配的新规则
    - 建议规则取消不再需要的系统补丁
  - 1000+预定义的DPI策略，实时更新

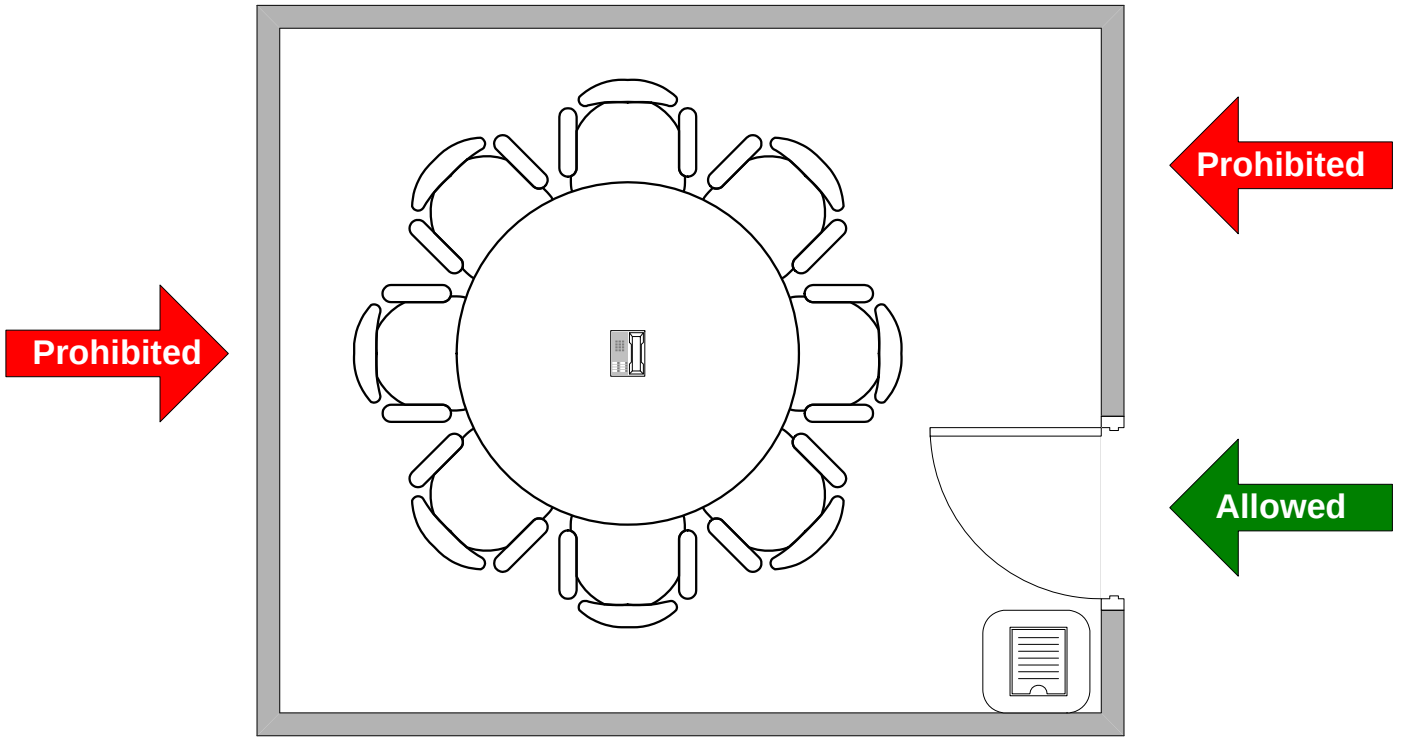
操作系统
Windows XP Desktop
Windows Vista Desktop
Windows Server 2008
Windows Server 2003
Windows Server 2000
Windows Mobile Laptop
Windows 7 Desktop
Solaris Server
Linux Server
Deep Security Virtual Appliance

应用程序
Mail Client Outlook Express (2)
Web Client Common (18)
Web Client Internet Explorer (21)
Web Client SSL (1)
Web Server Common (4)
Web Server IIS (2)
Windows Services RPC Client (2)
Windows Services RPC Server (2)

TREND MICRO 趋势科技

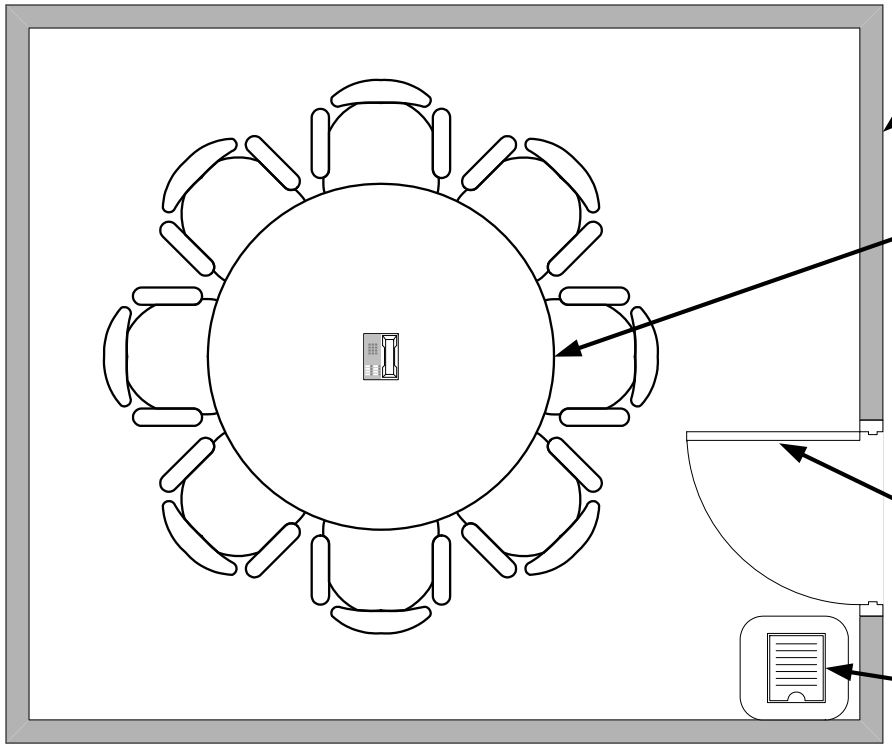
虚拟化防护DeepSecurity的功能

了解威胁入侵



TREND MICRO 趋势科技

DPI="门"



Wall
Prevent unauthorized access to the room

Firewall

Equipment inventory
Items that should be in the room

Integrity Monitoring

Door
Controls who can enter the room

Deep Packet Inspectio

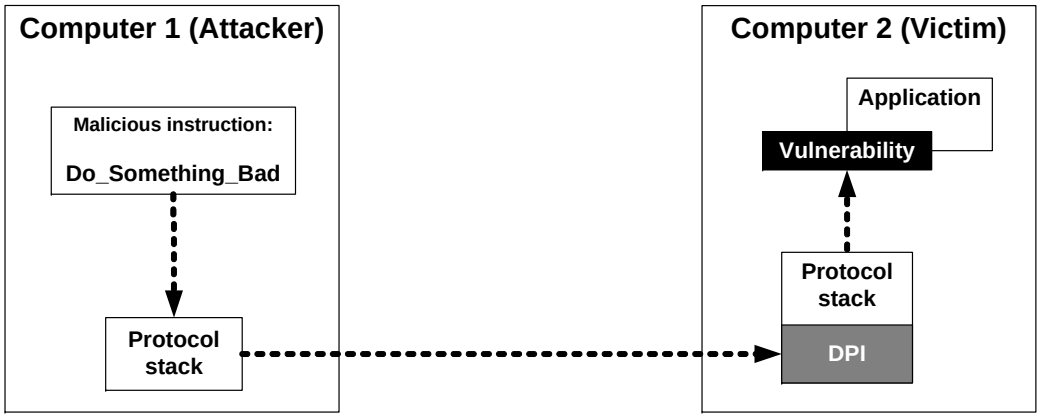
Visitor guestbook
Records visitors and their purpose

Log inspection

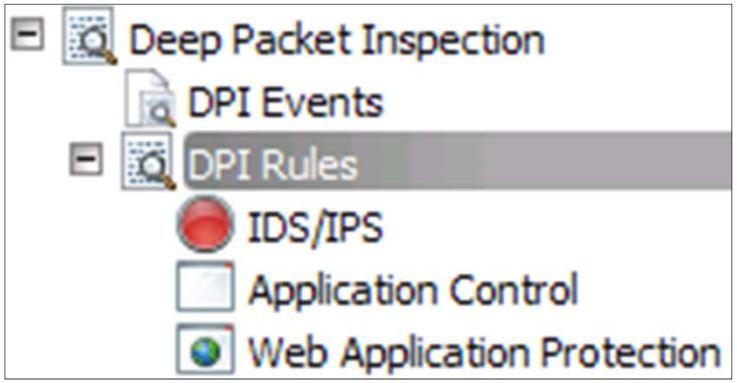
Deep Packet Inspection

使用**DPI**

- 虚拟补丁– 保护计算机在未安装补丁前阻止恶意程序的攻击

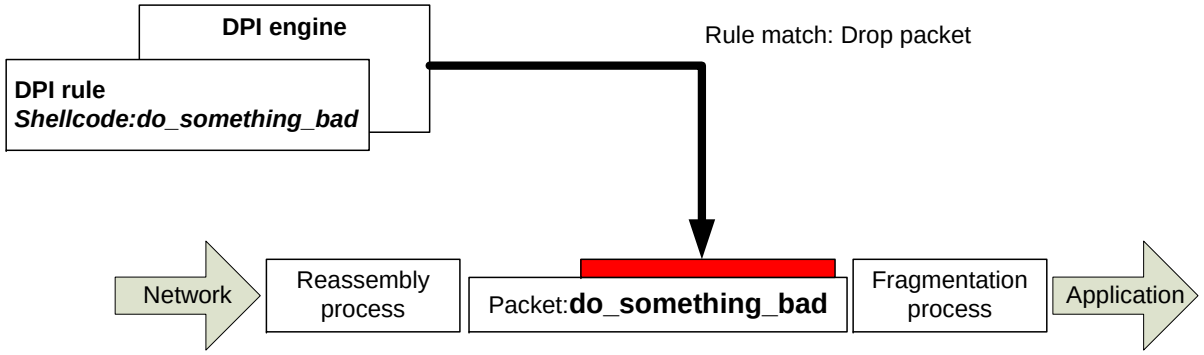


DPI > Rules



- **IDS/IPS –** 用于防御来自软件或系统的漏洞被利用。实现虚拟补丁功能

DPI > Rules

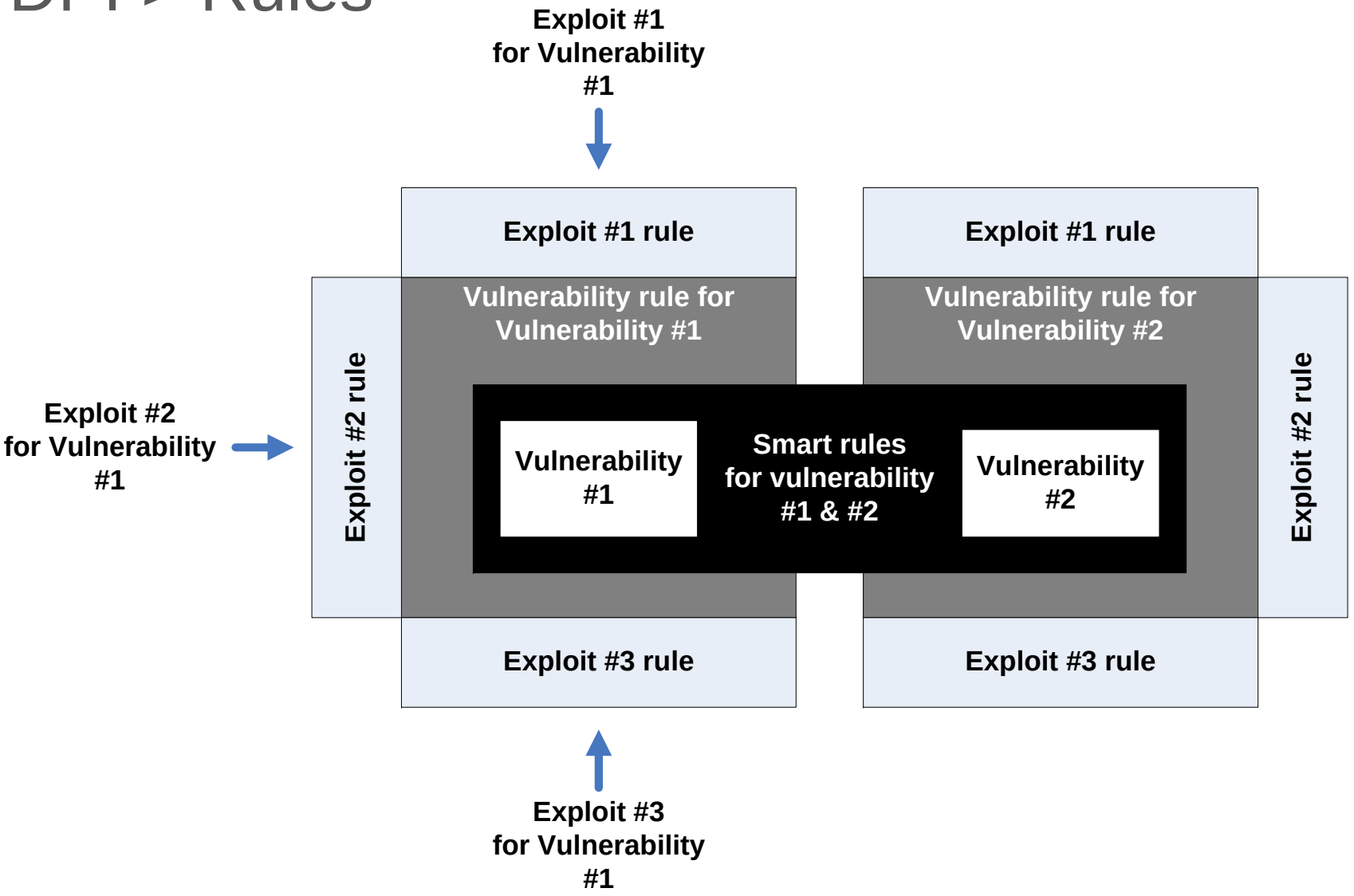


- 检查每个数据包中是否有恶意内容
- 需要重组可以被路由分割的数据包

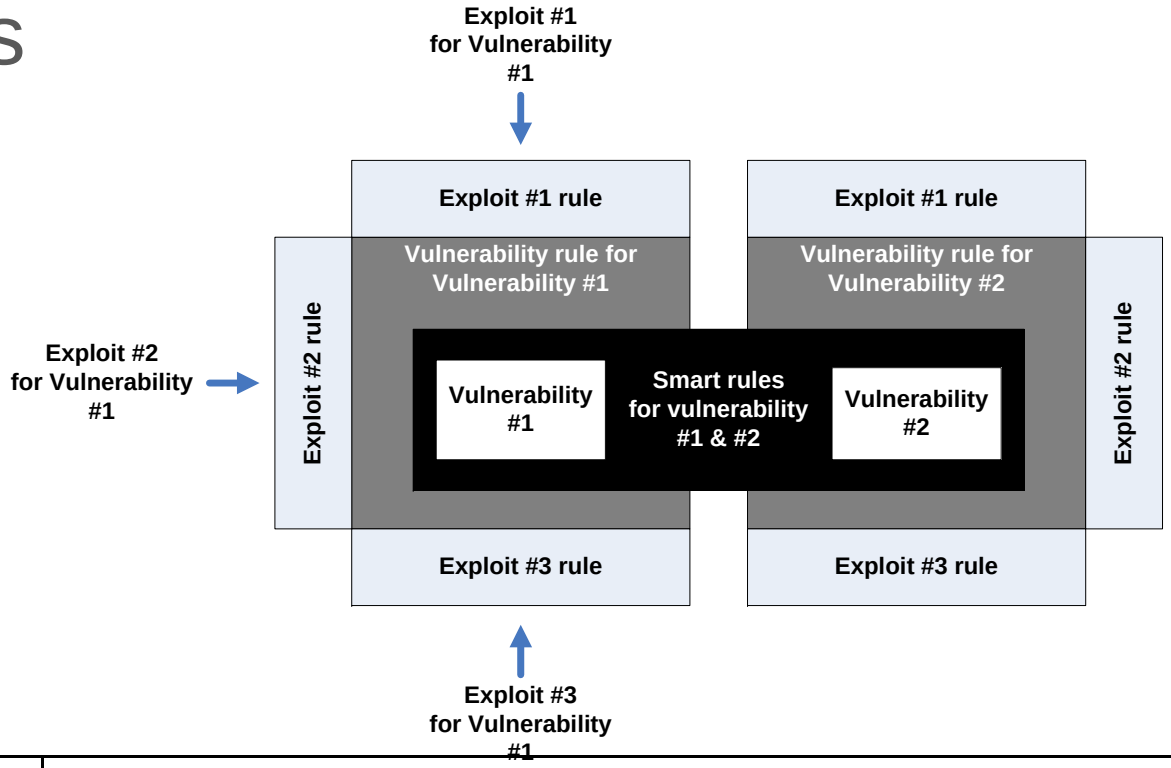
DPI > Rules

- Exploit rules
- Vulnerability rules
- Smart rules

DPI > Rules


Exploit #1
for Vulnerability
#1
Exploit #1 rule
Exploit #1 rule
Vulnerability rule for
Vulnerability #1
Vulnerability rule for
Vulnerability #2
Exploit #2
for Vulnerability
#1
Exploit #2 rule
Vulnerability
#1
Smart rules
for vulnerability
#1 & #2
Vulnerability
#2
Exploit #2 rule
Exploit #3 rule
Exploit #3 rule
Exploit #3
for Vulnerability
#1

DPI > Rules

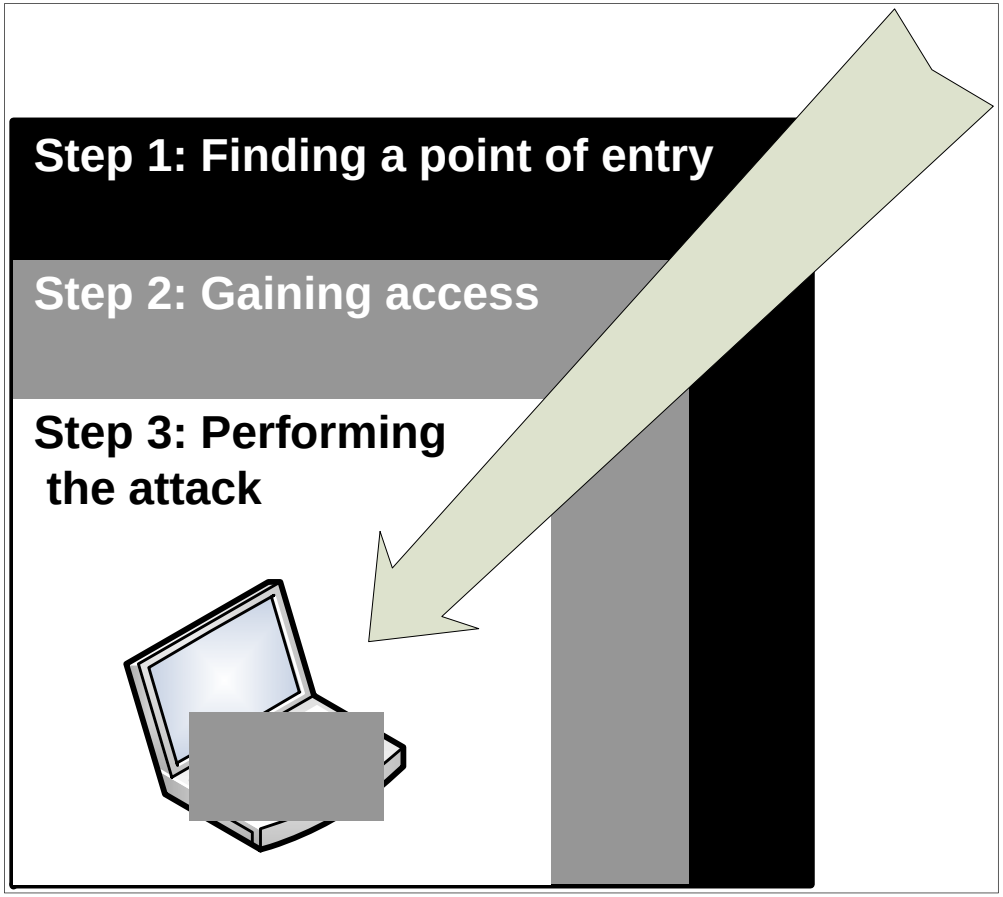


Rule No.	Type	Action
1	Smart	块的密码条目超过100个字符
2	Vulnerability	评估软件漏洞#1. 易受攻击的：进入超过512多个字符的密码字段
3	Vulnerability	评估软件漏洞#2. 易受攻击的：进入超过700多个字符的密码字段
4	Exploit	利用评估软件漏洞#1.当一个特定的字符序列占512个字符缓冲区溢出可导致软件执行恶意操作

攻击类型

- 被动攻击（Passive attack）
- 主动攻击（Active attack）

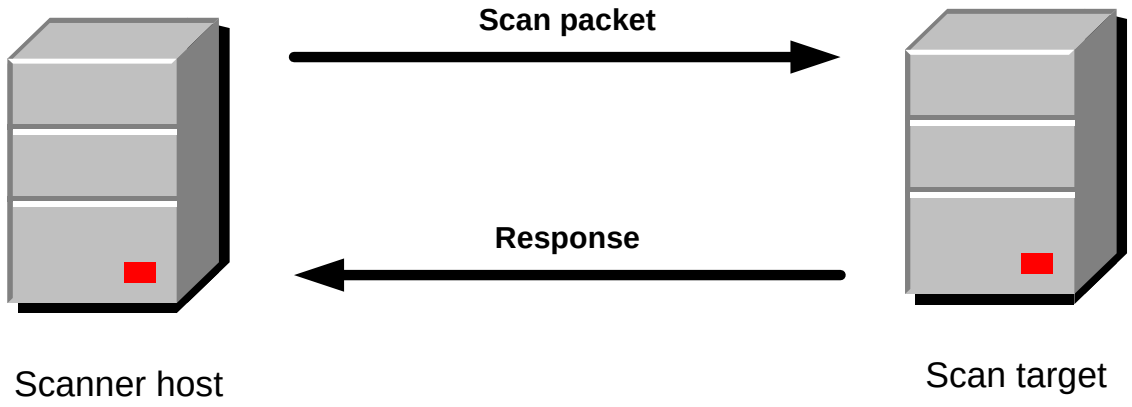
“解剖”攻击



“解剖”攻击> 进入点

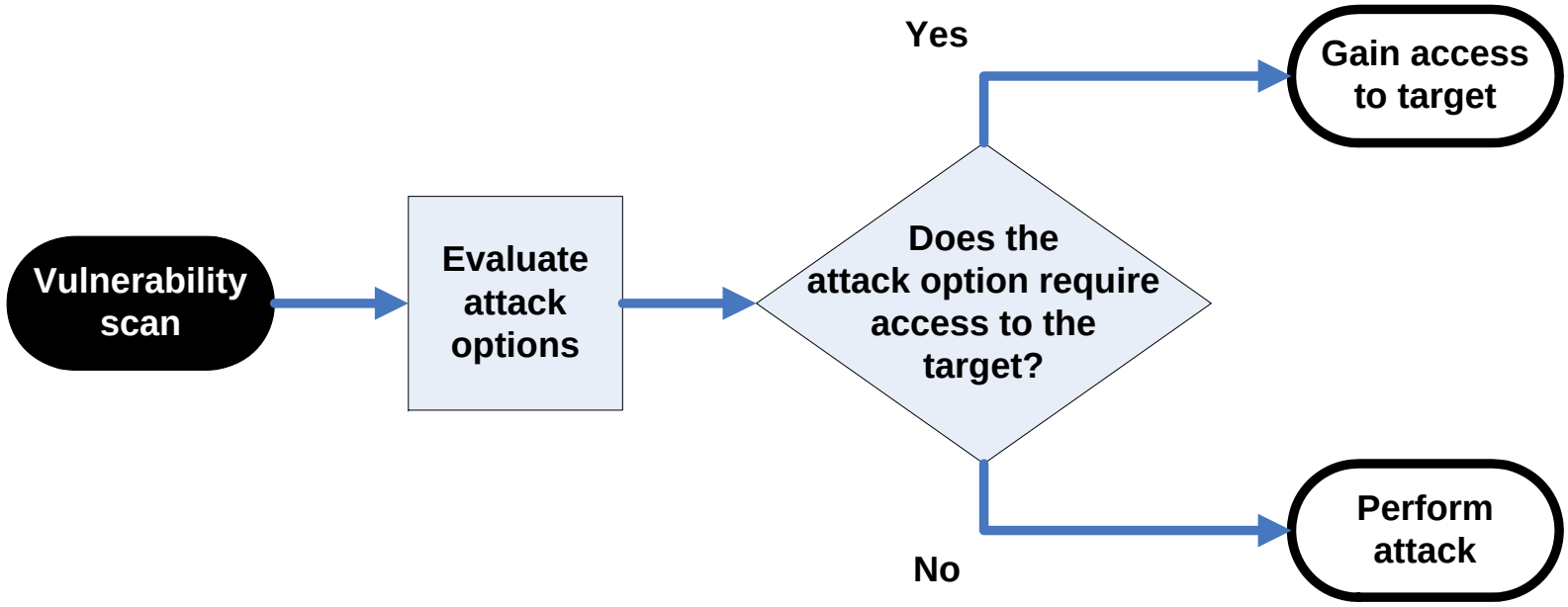
- 目标是什么?
- 目标环境是如何的?
- 哪个漏洞符合目标环境?

“解剖”攻击> 进入点



- 网络映射/ 扫描
- 端口扫描
- OS fingerprinting
- 漏洞列表

“解剖”攻击> 进入点



“解剖”攻击> 获取访问权

Conficker/Worm_Downad 如何获取系统访问权

- 利用漏洞
- 暴力攻击网络共享
- 命名管道（Named-pipes）
- 恶意HTTP 服务
- Autorun.inf

攻击 > 访问 > 利用漏洞

Server Service Vulnerability (MS08-067). Affected:

- RPC support
- File & print sharing support
- Named-pipe sharing

获取攻击能力:

- 安装程序
- 查看/修改/删除文件
- 创建一个具有完全权限的新账号

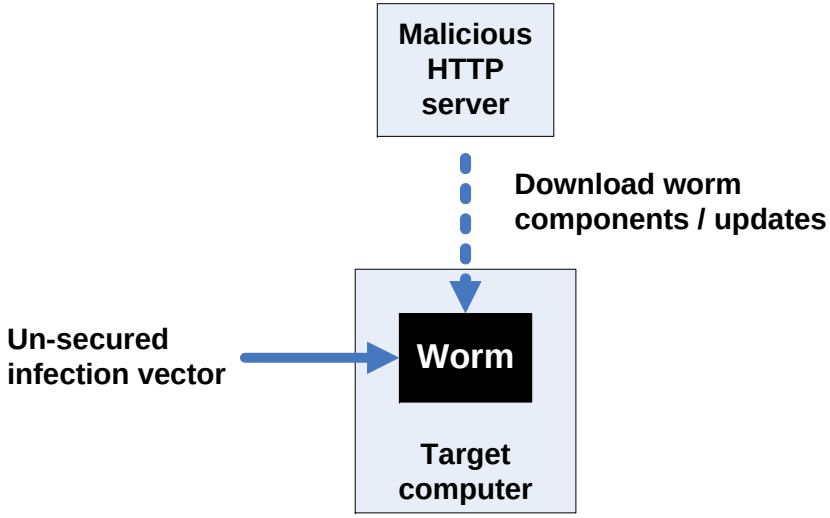
攻击 > 访问 > 网络共享

- 使用暴力破解方式攻击具有密码保护的网络共享
- 如果密码被猜测到，恶意程序即可以使用该网络共享

攻击 > 访问 > 命名管道

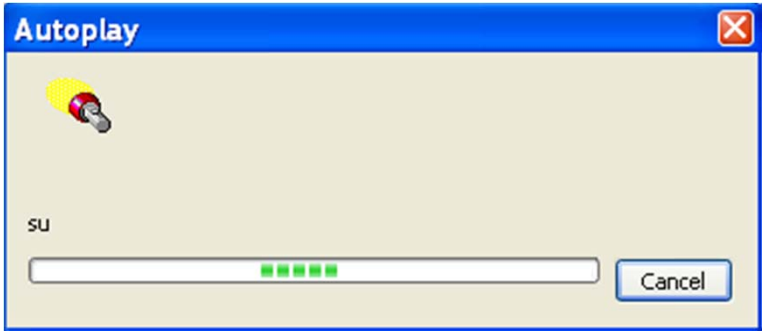
- 用作繁衍途径
- 生成新的病毒变种

攻击 > 访问 > 恶意 HTTP 服务



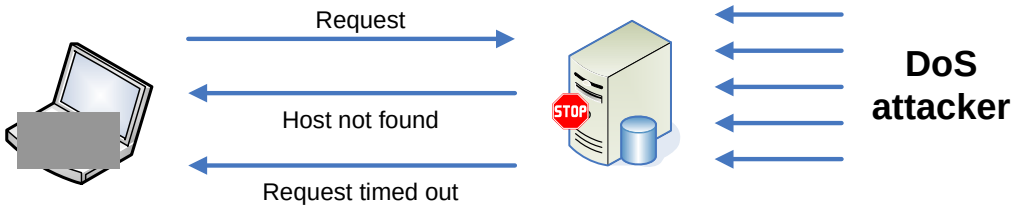
- 可作为获取访问权和攻击的一部分
- 恶意HTTP 服务使用一个随机端口

攻击 > 访问 > Autorun.inf



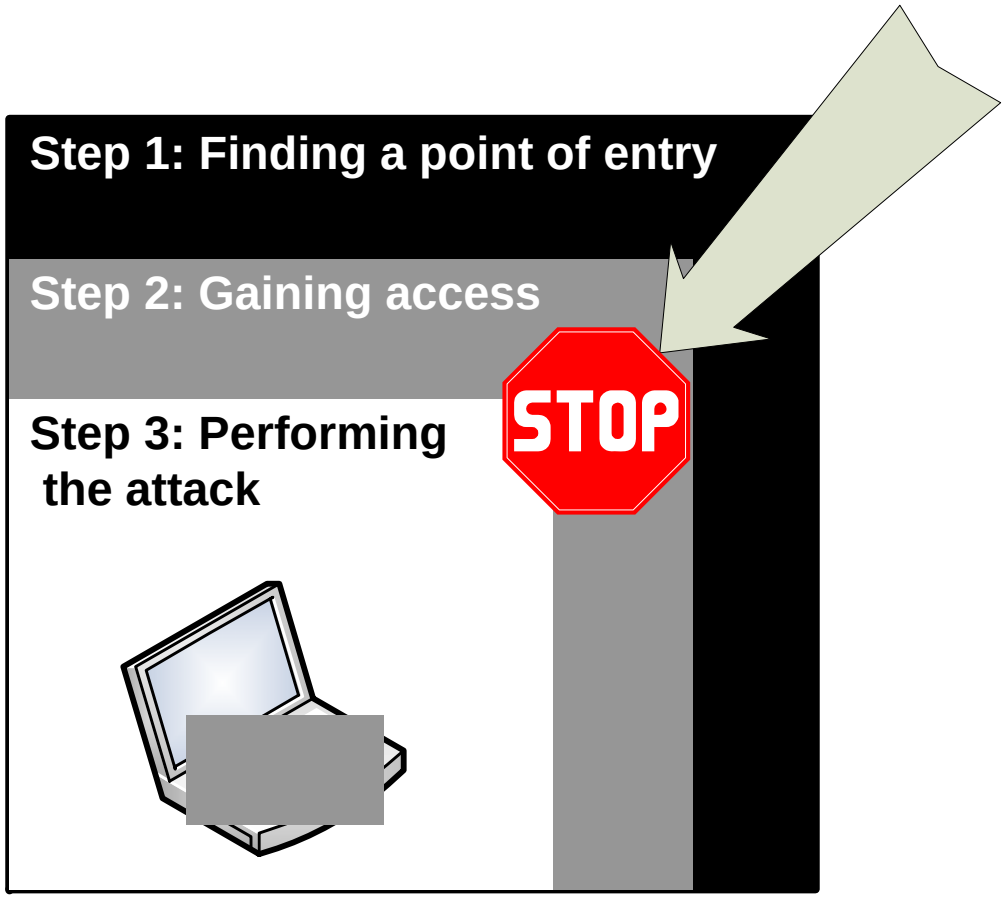
- 该病毒攻击USB drives，并使用此方式访问系统

“解剖”攻击> 执行攻击

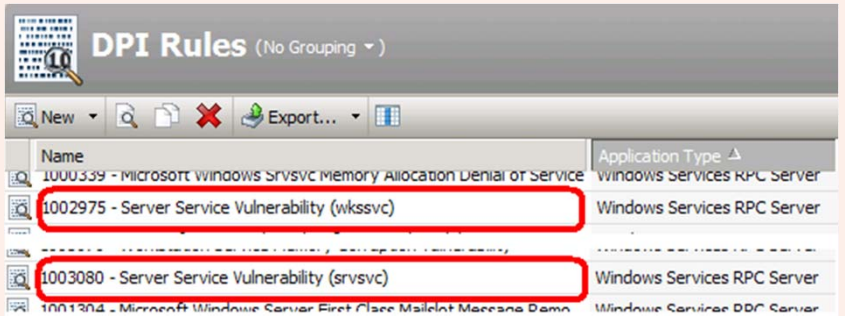


- 拒绝服务（DOS）
- 中间人
- Web应用攻击
- 在虚拟环境中攻击

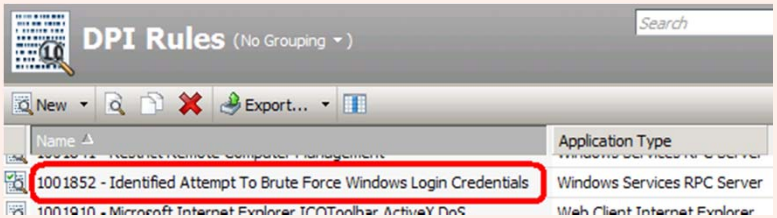
拦截威胁> 获取访问


Step 1: Finding a point of entry
Step 2: Gaining access
STOP
Step 3: Performing the attack

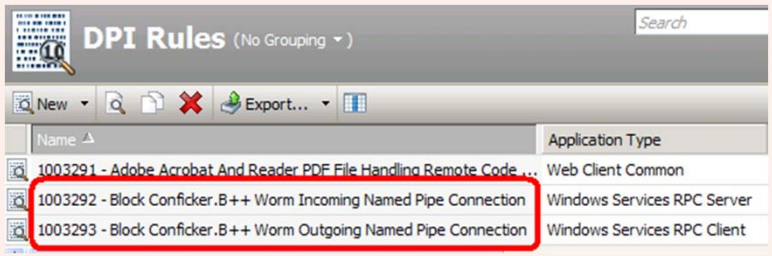
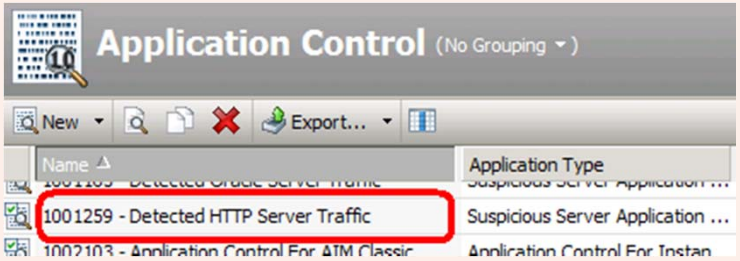
拦截威胁> 获取访问

Attack vector	Deep Security solution
• 利用漏洞	Feature: Deep Packet Inspection > DPI Rules Action: Prevent 该DPI规则指定Conficker/WORM_DOWNAD利用的the Server Service vulnerability 

拦截威胁> 获取访问

Attack vector	Deep Security solution
• 暴力攻击网络共享	Feature: Deep Packet Inspection > DPI rules Action: Prevent 该过滤器标识尝试暴力破解Windows 密码。 默认情况下， 这一规则被触发条件为，在180秒进行50次密码登录尝试。这个值是可配置。这种防恶意软件，使用字母组合或字典”猜“密码。 

拦截威胁> 获取访问

Attack vector	Deep Security solution
命名管道	Feature: Deep Packet Inspection > DPI rules Action: Prevent 
恶意HTTP服务	Feature: Deep Packet Inspection > Application control Action: Prevent 这是一个启发式检测流量过滤器，检测非端口80，8080，或其他一些管理员定义的HTTP流量 

TREND MICRO 趋势科技 全程护航 迈向云端

谢谢!

爱趋势互动社区 www.iqushi.com

趋势CEO Eva微博

趋势官方微博

趋势云计算安全博客

趋势云计算安全网站