

XXX 公司 Deep Security 测试报告



目录

| 1. | 文档说明 | 3 |
|----|-----------|----|
| 2. | | 4 |
| 3. | 测试环境说明 | 6 |
| 4. | 防病毒功能测试 | 8 |
| 5. | 防火墙功能测试 | |
| 6. | 深度包检测功能测试 | 14 |
| 7. | 完整性监控 | 20 |

^{博为峰旗下} **51上ES上 □ □ □** 软件测试网

1. 文档说明

本文档用于说明趋势科技为 XXX 公司提供的虚拟层防护解决方案,经过用户环境测试 后的有效性验证。内容包括:

> 测试环境说明

说明此次测试环境相关组件以及环境搭建过程

▶ 防病毒功能测试

说明此次测试验证过程以及测试结果

▶ 防火墙功能测试

说明此次测试验证过程以及测试结果

▶ 虚拟补丁功能测试

说明此次测试验证过程以及测试结果

> 完整性监控功能测试

说明此次测试验证过程以及测试结果

本文档相关截图、日志、数据皆来源于此次实际测试环境,所有测试项目都达到了预计 测试效果,达到测试目的。 ^{博为峰旗下} 51 **Lest □ ng** 软件测试网

www.51testing.com

2. 测试环境需求说明

DSM 控制台需求

| 程序 | 操作系统 | 功能 |
|---------|------------------|-----------------|
| DSM | Win2008 sp2 64 位 | DS 管理控制台 |
| | | *至少分配 8GB 内存 |
| | | *至少分配 2 颗志强 CPU |
| SQL2008 | Win2008 sp2 64 位 | 存储日志 |
| | | *至少分配 8GB 内存 |
| | | *至少分配 2 颗志强 CPU |

DSVA 客户端需求

DS 客户端安装是在每台物理机上以 DSVA 方式存在,安装方式与物理机增加无关,单台物理机上虚拟机数增加,相对应分配给 DSVA 的资源要增加,安装过程中,物理主机会重启,如下图所示

DSVA 资源分配建议

- 1GB of memory is assigned to the DSVA by default.
- Increase the memory to 4GB for a DSVA protecting 30-80 Virtual Machines.
- Increase the memory to 8GB for a DSVA protecting 80+ Virtual Machines.





通讯需求

IP 地址需求:

- 1、DSM(SQL Server2008)、vShield Manager(VSM)各需要一个 IP 地址
- 2、每个 DSVA 需要一个 IP 地址

各组件访问规则需求:

| 序 | 源机器描述 | 目的机器描述 | 访问端口 | 备注 | | |
|-------|-------|--------|----------|----|--|--|
| 1 | DCM | VC | Tcp4119 | 코戸 | | |
| I D2M | ٧C | Tcp443 | 双回 | | | |
| 2 | VSM | VC | Tcp443 | 双向 | | |
| | | | Tcp 4118 | | | |
| 3 | DSM | DSVA | Tcp 4120 | 双向 | | |
| | | | Tcp 4122 | | | |
| 4 | DSM | VSM | Tcp 443 | 双向 | | |
| 5 | VSM | DSVA | Tcp 443 | 双向 | | |
| 6 | DSM | For | Tcp 443 | 코白 | | |
| 0 | MSM | ESX | Tcp 4119 | 双円 | | |
| 7 | VSM | Esx | Tcp443 | 双向 | | |



3. 测试环境说明

| 角色 | IP 地址 | web 控制台登录地址 | 系统类型 | web 控制台用 户名/密码 | 系统登录名和密码 |
|--|---------------|---------------------------------------|--------------|---|-----------------|
| DSM (Deep Secrutiy 控制端) | 10.100.60.121 | <u>https://</u> 10.100.60.121:4119 | windows 2008 | <u>masteradmin/</u> <u>masteradmin</u> | administrator/- |
| ESX1 | 10.100.61.111 | n/a | linux x64 | n/a | n/a |
| ESX2 | 10.100.61.113 | n/a | linux x64 | n/a | n/a |
| ESX3 | 10.100.61.114 | n/a | linux x64 | n/a | n/a |
| ESX4 | 10.100.61.115 | n/a | linux x64 | n/a | n/a |
| vCenter | 10.100.60.110 | 使用 vSphere Client 登录 | windows 2008 | administrator/- | administrator/- |
| vShield Manager (vmware 组件,用于完成 底层防病毒) | 10.100.60.122 | https://10.100.60.122 | linux x64 | admin/default | admin/default |
| DSVA for ESX1 (Deep Security 组件之一) | 10.100.60.123 | n/a | linux x64 | n/a | dsva/dsva |
| DSVA for ESX2 (Deep Security 组件之一) | 10.100.60.124 | n/a | linux x64 | n/a | dsva/dsva |
| DSVA for ESX3 (Deep Security 组件之一) | 10.100.60.125 | n/a | linux x64 | n/a | dsva/dsva |
| Test-Machine-1 (Transfer Server) | 10.100.61.167 | n/a | windows 2008 | n/a | administrator/- |
| 注:其中为趋势 Deep Security 相关服务器 | | | | | |

vmware 相关服务器

测试用虚拟机





| 项目 | 测试环境搭建 | | | | | |
|-----------------------------|-----------------------|-----------------|----|--|--|--|
| 时间 | 2014/3/27 | | | | | |
| 步骤 | 描述 | 结果 | 备注 | | | |
| | 该步骤用户完成 vShield API 安 | | | | | |
| 1.部署 vShield Manager | 装,以便完成稍后的底层无代理 | □成功 | | | | |
| | 防病毒功能 | | | | | |
| 2.部署 Deep Security | 该步骤用于完成 Deep | | | | | |
| Manager | Security Manager | ⊔ ⊓∿≁∕ J | | | | |
| | 该步骤用于完成 vShield API 与 | | | | | |
| 3. 命者 Deep Security Virtual | 趋势科技 Deep Security | □成功 | | | | |
| Арриансе | Virtual Appliance 联动 | | | | | |

4. 防病毒功能测试

趋势科技通过 Vmware 提供的 vShield API,无需在 Guest Server 安装客户端程序,即可 实现免客户端的底层防护功能,实现基于实时/手动的病毒查杀功能。

1. 底层防病毒功能激活

选取一台虚拟机,激活底层防病毒功能

| 计算机: WIN-AUDGI29LOQG (windows2008 test1) | | | | | | | | | |
|--|---|--|--|--|--|--|--|--|--|
| ♀ 概述 | 常规 云安全智能防护 高级 隔离的文件 事件 | | | | | | | | |
| 😨 防恶意软件 | 防恶意软件 | 防恶意软件 | | | | | | | |
| ── Web 信誉 | ▶ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 的恶息软件状态: 打井 | | | | | | | |
| 🛞 防火墙 | 实时扫描 | | | | | | | | |
| 🧐 入侵防御 | | | | | | | | | |
| () 完整性监控 | | ¥ 鋼幅 √ 编辑 | | | | | | | |
| ③ 日志审查 | | | | | | | | | |
| 🥮 接口 | | | | | | | | | |
| 🛞 设置 | □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ | ▼ 编辑 | | | | | | | |
| ■ 更新 | - 2220.474 | | | | | | | | |
| ∯ 覆盖 | | | | | | | | | |
| | 配置: 缺省的预设扫描配置 | ★ 编辑 | | | | | | | |

2. 实时扫描功能测试

通过该虚拟机的解压下载的 eicar.zip 测试文件,实时扫描功能检测并处理位于读写状态中的 EICAR 测试病毒,该测试文件的解压缩过程被实时阻止并生成相关日志。



■ 更新
 ●●● 覆盖

www.51testing.com

| 十算机: | WIN-AUDGI29LOQG | (windows2008 | test1) |) |
|------|-----------------|--------------|--------|---|
|------|-----------------|--------------|--------|---|

| | | • • | | | |
|---------|---------|---------|--------------------|----------------|--|
| Ŷ | 概述 | 常规 | 安全智能防护 高级 | 隔离的文件事 | 件 |
| | 防恶意软件 | 防恶意软 | 件事件 所有 ▼ 无分 | 3组 👻 | ♀ 搜索 |
| | ₩eb 信誉 | 期间: | 最近1小时内 | • |] |
| | 防火墙 | 计算机: | 计算机: | | WIN-AUDGI29L0QG (windows2008 test1) |
| ۲ | 入侵防御 | 111 查看 | 🚯 导出 🔹 省 自动 | 标记 🛛 🏭 列 | |
| | 完整性监控 | 时间 🔻 | | 计算机 | 受感染的文件 |
| 9 | 日志审查 | 2014-03 | -27 14:33:54 | WIN-AUDGI29L0. | C:\Users\Administrator\Desktop\eicar\eicar.com |
| • | 接口。 | ~ | | | |
| - - | · 设置 | - | | | |

测试文件解压缩失败。

| - 10.100.61.167 | 远程桌面连接 | | |
|-----------------|--|------------|---------|
| | | | |
| | 🔒 eicar | | |
| | 💮 💮 📕 🕶 eicar | | |
| eicar | 组织 ▼ 包含到库中 ▼ | 共享 ▼ 新建文件夹 | |
| | □☆ 收藏夹 | 名称 🔺 | 修改日期 |
| eicar | ▶▶ 下载 ■■ 桌面 | | 该文件夹为空。 |
| | 日 📴 库 | | |
| | | | |
| | Image: BC and the second seco | | |
| | □p️➡️ 计算机 □ 叠 本地磁盘 (r·) | | |

检测日志,在防恶意软件事件中发现解压缩的文件已经被隔离。



3. 测试结果

| 项目 | 虚拟层无客户端防病毒功能测试(针对 Win2008) | | | | | |
|--|---|-------|------|--|--|--|
| 时间 | | 2014/ | 3/27 | | | |
| 步骤 | 描述 | 结果 | 备注 | | | |
| 1.激活实时扫描功能,将测试 病毒 Eicar 释放到本地硬盘; 正常情况下,该文件无法释 放,DSM 上可观察到相关文 件被隔离的日志 | 该步骤用于验证趋势科 技解决方案可以实时地 对来自外部的病毒进行 处理 | □成功 | 无 | | | |
| 2.以上步骤执行过程中 , 无兼 容性问题 | 该步骤用于验证趋势科 技解决方案在运行中不 会对用户环境产生兼容 性问题 | □成功 | | | | |
| 3.以上步骤执行过程中 , 无性 能问题 | 该步骤用于验证趋势科 技解决方案在运行中不 会对用户环境产生性能 问题 | □成功 | | | | |

5. 防火墙功能测试

趋势科技通过 Vmware 提供的 vSafe API,无需在 Guest Server 安装客户端程序,即可实 现免客户端的底层防护功能,实现基于流量内容的虚拟补丁功能,实现过滤针对利用操作系 统漏洞进行攻击的流量。

1. 搭建用于测试的环境

进入测试策略界面开启防火墙功能



www.51testing.com

| 计算 | 和: WIN-AUDGI29 |)L(| DQG (wi | indows20 | 0 8 tes | st1) | | | | |
|----------------|----------------|-----|----------------------|---|----------------|------------|--------|---------|----|-----|
| ¢ | 概述 | | 常规 | 接口隔离 | 侦察 | 高级 | 事件 | | | |
| ② | 防恶意软件 | | 「防火墙」 | 15-t- | | | | | | |
| - | Web 信誉 | | 防火垣 | 成心: 打井 | | | 💽 🧐 | 打开,1 规则 | ų | |
| | 防火墙 | | 「防火墙 | 犬态配置 ———————————————————————————————————— | | | | | | |
| 0 | 入侵防御 | | 👹 全! | 局(所有接口) - 5300年前33 |) | | | | | |
| ۲ | 完整性监控 | | | 网络道肖森 | 1 - 00:50 | 1:50:57:50 | 5:00 | | | |
| 9 | 日志审查 | | 「端口扫描 | Ħ | | | | | | |
| • | 接口 | - | 上次端 扫描的词 | 口扫描: 湍口: | | N/A N/A | | | | |
| ÷ | 设置 | | 打开的 | 端口: | | N/A | | | | |
| <u></u> | 更新 | | | 扫描打开的 | 当日 | | 取消端口 | 扫描 | | |
| - 5 | 覆盖 | | ┌已分酉砚 | 防火墙规则—— | | | | | | |
| | | | 分配 | 配/取消分配 | . 🔲 | 属性 | 🔊 寺出 🔸 | 🏭 列 | | |
| | | | 名利 | 你 🔺 | | | 操作类型 | 优先级 | 方向 | 帧类型 |
| | | | 🛞 禁」 | Ping | | | 拒绝 | 3 一 高 | 传入 | IP |

建立一条策略,禁止 icmp 包传入

| 防火墙规则 所有 ▼ 技操作类型 ▼ | | | | く装 | * | | - |
|--------------------|--------|--------|-----|---------|---------|-------|-----|
| 📑 新建 🝷 💼 刪除 🔟 團性 | 门 复制 | 🔄 导出 🔸 | 🏭 列 | | | | |
| 名称 🔺 | 优先级 | 方向 | 帧类型 | 协议 | 源 IP | 源 MAC | 源端[|
| ■ 允许 (25) | | | | | | | |
| ● 强制允许(42) | | | | | | | |
| ■ 拒绝 (5) | | | | | | | |
| 🎯 🔽 🖻 icmp_deny | 3 一 高 | 传入 | IP | 任何 | 任何 | 任何 | N/A |
| 🍘 🗖 🖻 受限接口增强 | 0 - 最低 | 传出 | 任何 | N/A | N/A | 任何 | N/A |
| 🛞 🗖 🖬 域外増强 | 0 - 最低 | 传出 | 任何 | N/A | N/A | 任何 | N/A |
| 🛞 🗆 🖻 拒绝内部 IP 范围 | 4 — 最高 | 传入 | IP | 任何 | 入口过滤器 … | 任何 | N/A |
| 🍘 🔲 🖬 远程域増强(分离隧道) | 0 - 最低 | 传出 | IP | TCP+UDP | 任何 | 任何 | 任何 |
| | | | | | | | |



启用策略



| 计算 | 计算机: WIN-AUDGI29LOQG (windows2008 test1) | | | | | | | | | | | |
|----------------|--|--|----------------|-----------------|-----------|------------|--------|-------|----|-----|--|--|
| Ø | 概述 | | 常规 | 日隔离 | 侦察 | 高级 | 事件 | | | | | |
| ② | 防恶意软件 | | | | | | | | | | | |
| | ₩eb 信誉 | | | | | | | | | | | |
| | 防火墙 | | ○防火墙状态配置 | | | | | | | | | |
| • | 入侵防御 | | | | | | | | | | | |
| | 完整性监控 | | | 治19825 I . | - 00.50.5 | 0.57.30 | | | | | | |
| 9 | 日志审查 | | | - 144 | | | | | | | | |
| • | 接口 | | 上次端口扫 扫描的端口 | 抽: : | | N/A N/A | | | | | | |
| - | 设置 | | 打开的端口 | : | | N/A | | | | | | |
| | 更新 | | ŧ | ∃描打开的端□ | _ | | 取消端□ | 1扫描 | | | | |
| 4 6 | 覆盖 | | 「已分配防火 | 墙 规则 ——— | | | | | | | | |
| | | | 分配/耳 | 观消分配 | 📰 | 性 | 🔄 导出 🔸 | 🏭 列 | | | | |
| | | | 名称 | | | | 操作类型 | 优先级 | 方向 | 帧类型 | | |
| | | | 🛞 禁止Pi | ng | | | 拒绝 | 3 一 高 | 传入 | IP | | |

使用 ping 命令测试策略是否生效,策略已经生效



同时关闭策略



检测事件记录

| Ø | 概述 | | 常規 接口 | 隔离 侦察 高级 | 事件 | | | | | |
|----------------|--------|------|------------|-------------|---------------------------------------|----|----|----|-----|------|
| 0 | 防恶意软件 | | 防火墙事件 | 所有 👻 无分组 | • | | ٩ | 招索 | | |
| 0 | Teb 信智 | | 期间: | 最近1小时内 | * | | | | | |
| ۲ | 防火墙 | | 计算机: | i+30.80: | 개대: 🐨 (mstest.hitechad.com (VDR Test) | | | v | | |
| 0 | 入部時间 | | 🔲 童香 | 🗊 导出 🔹 省 自动 | 动标记 🌉 列 | | | | | |
| 0 | 完整性监控 | | 时间 マ | | 计算机 | 原因 | 标记 | 操作 | 排序 | 方向 |
| 0 | 日志审查 | | 2014-03-24 | 14:04:48 | | | | 拒绝 | 100 | 倾入 |
| - | #D | н | 2014-03-24 | 14:04:48 | 1 | | | 拒绝 | 100 | 传入 |
| - | 16H | -00 | 2014-03-24 | 14:04:37 | 1 | | | 拒绝 | 100 | 代入 |
| 8 | 设置 | п. | 2014-03-24 | 14:04:37 | 1 | | | 拒绝 | 100 | 传入 |
| Fi. | 带领 | | 2014-03-20 | 14:04:36 | 1 | | | 拒绝 | 100 | 传入 |
| | A-41 | - 11 | 2014-03-24 | 14:04:35 | 1 | | | 拒绝 | 100 | 後入 |
| 5 6 | 覆盖 | | 2014-03-24 | 14:04:34 | | | | 拒绝 | 100 | 传入 |
| | | | 2014-03-24 | 14:04:34 | | | | 拒绝 | 100 | 传入 |
| | | | 2014-03-24 | 14:04:31 | 1 | | | 拒绝 | 100 | 传入 |
| | | | 2014-03-24 | 14:04:29 | 1 | | | 拒绝 | 100 | 传入 |
| | | | 2014-03-24 | 14:04:27 | | | | 拒绝 | 100 | 传入 |
| | | | 2014-03-24 | 14-04-26 | | | | 拒绝 | 100 | 44 X |



2. 测试结果

| 项目 | 虚拟层无客户端防火 | ,(针对 Win2008) | | | | |
|---|---|---------------|----|--|--|--|
| 时间 | 20 |)14/3/27 | | | | |
| 步骤 | 描述 | 结果 | 备注 | | | |
| 1.激活防火墙功能;可通过 虚拟机状态以及 system event 查看是否设置 | 该步骤用于启用防火墙防护功 能 , 为后续测试做准备 | | | | | |
| 2.在测试 VM 上部署 icmp 禁止传入测试 , 启用策略 | 该步骤用于测试防火墙功能针 对协议和包的有效性 | | | | | |
| 3.使用 ping 命令验证策略 部署 | 该步骤用于确认防火墙策略是 否正确生效 , 有效拒绝 icmp | | 无 | | | |
| 4.在测试 VM 上关闭部署的 icmp 拒绝策略 | 该步骤用于对策略的二次验证 | | | | | |
| 5.继续使用 ping 命令验证 策略是否生效 | 该步骤用于确实防火墙策略取 消后 icmp 包的传输是否正常 | | | | | |
| 6.以上步骤执行过程中,无 兼容性问题 | 该步骤用于验证趋势科技解决 方案在运行中不会对用户环境 产生兼容性问题 | | | | | |
| 7.以上步骤执行过程中,无 性能问题 | 该步骤用于验证趋势科技解决 方案在运行中不会对用户环境 产生性能问题 | | | | | |

6. 深度包检测功能测试

趋势科技通过 Vmware 提供的 vSafe API,无需在 Guest Server 安装客户端程序,即可实 现免客户端的底层防护功能,实现基于流量内容的虚拟补丁功能,实现过滤针对利用操作系 统漏洞进行攻击的流量。

1. 测试工具说明

A). DemoSQL 为模拟 SQL Slammer 攻击行为的演示工具(并不会对操作系统产生实际影响),利用 <u>Microsoft MS02-039</u>相关漏洞。



B). lesssecurity.py 为模拟针对远程桌面协定重大漏洞攻击行为的演示(会对操作系统产生实际影响,不建议在生产环境中测试),利用 <u>Microsoft MS12-020</u>相关漏洞。

2. 测试一:

激活虚拟补丁防护策略

启用 DPI 策略"1000617: MS-SQL Slammer Worm"

| Ø | 概述 | 1 [| 常规 高级 事件 | | | | | | | | | | | |
|----------------|--------|-----|---------------------------------|------------------------------------|----------|-------|----|----|--|--|--|--|--|--|
| © | 防恶意软件 | | | G防御 G防御状态: 打开 T G G | | | | | | | | | | |
| - | Web 信誉 | | 人侵防御状态: 打开 → 保防御行为 | | | | | | | | | | | |
| • | 防火墙 | | ◎ 阻止 | 短时间1月21 1月11日 | | | | | | | | | | |
| ۲ | 入侵防御 | | ◎ 检测 | ◎ 检测 | | | | | | | | | | |
| 0 | 完整性监控 | | 已分配的入侵防御规则 | 2分配的入侵防御规则 | | | | | | | | | | |
| 9 | 日志审查 | | 所有 👻 | | | | | | | | | | | |
| | 接口 | ~~ | 分配/取消分配 🔟 属性 | 😰 导出 🔹 💽 应用程序类型 | .] 🏭 列. | | | | | | | | | |
| : | 设置 | | 名称 🔺 | 应用程序类型 | 优先级 | 严重性 | 模式 | 类型 | | | | | | |
| | 更新 | | 🍄 1000617 - MS-SQL Slammer Worm | Database Microsoft SQL Resolut… | 3 — 高 | ••• ā | 阻止 | 入侵 | | | | | | |
| 5 5 | 覆盖 | | | | | | | | | | | | | |

使用 DemoSQL 工具进行模拟攻击

| 🏧 管理员: C:\Windows\system32\cmd.exe |
|--|
| D:\>DemoSQL.exe -a1 |
| DemoSQL 1.0 – AV Research Team.dfce4ad d |
| IP Scope: 172.27.3.242:1434 TARGET HOST: 172.27.3.242:1434 |
| 404 byte packet was sent to 172.27.3.242:1434 Alright! |
| $D: \setminus >$ |

查看相关 DPI 日志



| Ø | 概述 | | 常规 高 | 级事件 | ¥ | | | | |
|---------------|--------|----|-----------|------------|-----------|-----|---------------------------------|------------|-------------------------------------|
| © | 防恶意软件 | | 入侵防御事 | 件 所有 | 頁 ▼ 无分组 ▼ | | | Q # | *索 |
| - | Web 信誉 | | 期间: | 最近1小 | 最近 1 小时内 | | | | |
| ۲ | 防火墙 | | 计算机: | 计算机: | | - | rmstest.hitechad.com (VDR Test) | | ▼ |
| ۲ | 入侵防御 | | 111 查看 | 😰 导出 | • 省 自动标记 | 👪 列 | | | |
| 0 | 完整性监控 | | 时间 🔻 | | 计算机 | | 原因 | 标记 | 应用程序类型 |
| 9 | 日志审查 | | 2014-03-2 | 4 14:09:57 | | | 1000617 - MS-SQL Slammer Worm | | Database Microsoft SQL Resolution s |
| | 接口 | ~~ | | | | | | | |
| : | 设置 | | | | | | | | |
| | 更新 | | | | | | | | |
| -1 | 覆盖 | | | | | | | | |

3. 测试二

未应用虚拟补丁防护策略测试攻击

■ 管理员: C:\Windows\system32\cmd.exe
D:\>lesssecurity.py 172.27.3.242
sending: 580 bytes
received: 19 bytes
Traceback (most recent call last):
File "D:\lesssecurity.py", line 86, in <module>
s.connect<(HOST,PORT>)
File "<string>", line 1, in connect
socket.error: [Errno 10060]
D:\>_

攻击成功, 被攻击主机蓝屏

^{博为峰旗下} 51**Lest Ing** 软件测试网

www.51testing.com



主机重启,错误信息







激活虚拟补丁防护策略

启用 DPI 策略"1004949 – Remote Desktop Protocol Vulnerability (VCE-2012-0002)"

| | | _ | | | | | | | | | | | | |
|-----------------|--------|----|-------|-----------|------------|------------|----------------|--------------------|----------|--------|----|----|--|--|
| Ø | 概述 | ſ | 常规 | 高级 | 事件 | | | | | | | | | |
| | 防恶意软件 | | 入侵防御 | 國防御状态: 打开 | | | | | | | | | | |
| | Web 信誉 | | 入侵防御 | | | | | | | | | | | |
| | 防火墙 | | ◎ 阻I | | | | | | | | | | | |
| ③ | 入侵防御 | | ◎ 检测 | ◎ 检测 | | | | | | | | | | |
| 0 | 完整性监控 | | 已分配的 | | | | | | | | | | | |
| 9 | 日志审查 | | 所有 💌 | | | | | | | | | | | |
| | 接口 | ~~ | 分酉 | ℓ/取消分 | 配 | ■ 属性 | 🚯 豊田 🔸 | ◎ 应用程序类型 | . [🏭 列. | | | | | |
| (); | 设置 | | 名移 | jī ▲ | _ | | 应用程序类型 | | 优先级 | 严重性 | 模式 | 类型 | | |
| | 更新 | | 🍄 100 | 4949 - F | Remote Des | ktop Proto | · Remote Deskt | op Protocol Server | 2 — 正常 | ••• 严重 | 阻止 | 漏洞 | | |





🚾 管理员: C:\Windows\system32\cmd.exe

D:\>lesssecurity.py 172.27.3.242
sending: 580 bytes
received: 19 bytes
Traceback (most recent call last):
 File "D:\lesssecurity.py", line 86, in <module>
 s.connect<(HOST,PORT)>
 File "<string>", line 1, in connect
socket.error: [Errno 10060]
D:\>lesssecurity.py 172.27.3.242
sending: 580 bytes
Traceback (most recent call last):
 File "D:\lesssecurity.py", line 89, in <module>
 rec = s.recv(100)
socket.error: [Errno 10054]
D:\>_

查看相关 DPI 日志

| | | · · · | | | | | - · |
|----------------|--------------|-------------|--------------|--------------------------------|------------|--------------------------------|-----|
| | 常规 高级 | 级事件 | | | | | |
| 7件 | 入侵防御事 | 件 所有 ▼ | 无分组 👻 | | Q 搜 | 索 | • |
| <u><u></u></u> | 期间: | 定制范围: | • | | | | |
| | | 自: 2014-03- | 24 14:00 | ② 至: 2014-03-24 | | 14:25 ⊘ | • |
| 卸 | 计算机: | 计算机: | v 1 | mstest.hitechad.com (VDR Test) | | v | |
| 控 | □ 查看 | 🚯 导出 🔹 🍕 | 🗿 自动标记 🛛 🏭 列 | | | | |
| 5 | 时间 🔻 | 计算机 | π. | 原因 | 标记 | 应用程序类型 | |
| | 1 2014-03-24 | 14:24:31 | | 1004949 - Remote Desktop Pr… | | Remote Desktop Protocol Server | |



4. 测试结果

| 项目 | 虚拟层无客户端防火墙功能测试(针对 Win2008) | | | | | |
|---|--|-----|----|--|--|--|
| 时间 | /27 | | | | | |
| 步骤 | 描述 | 结果 | 备注 | | | |
| 1.激活 DPI 功能;可通过 对应虚拟机状态以及 system event 查看是否 设置成功 2.使用 DPI 虚拟补丁策 | 该步骤用于启用 DPI 防护功能,为后续测试虚拟补丁做准备 | □成功 | 无 | | | |
| 略,屏蔽 SQL 演示攻击; 正常情况下,可以通过 DPI Event 查看是否防护 成功 | 以少乘用了 确认 DF1 显现中 丁策略正确生效 ,有效屏蔽 基于 Microsoft MS02-039 攻击 | □成功 | | | | |
| 2.使用 DPI 虚拟补丁策 略,屏蔽利用远程桌面协 定漏洞的演示攻击;正常 情况下,可以通过 DPI Event 查看是否防护成功 | 该步骤用于确认 DPI 虚拟补 丁策略正确生效 , 有效屏蔽 基于 Microsoft MS12-020 攻击 | □成功 | | | | |

7. 完整性监控

趋势科技通过 Vmware 提供的 vSafe API,无需在 Guest Server 安装客户端程序,即可实现免 客户端的底层防护功能,实现基于注册表/系统文件状态检测的完成性监控功能。

1. 搭建用于测试的环境

进入测试策略管理界面开启完整性监控功能



| 8 | 截述 | | 常規 高級 事件 | | | |
|---|--------|----|---|------|-----|------------|
| 0 | 防恶意软件 | | 完整性监控 | | | |
| 0 | Web 信誉 | | 只整性温控状态: 打开 ▼ ● 打开, 1 规则 emi20413年 | | | |
| 3 | 防火墙 | | 二 英时 | | | |
| 8 | 入强防御 | | · 二整件扫描 | | | |
| 9 | 完整性當拉 | | 外对完整性的上次完整扫描: N/A | | | |
| Ð | 日志审查 | | 扫描完整线 | | | |
| | 接口 | 40 | 「墓线 | | | |
| 8 | 设置 | | 上次创建的完整性基础: N/A | | | |
| 3 | 更新 | | 双新生成基线 臺香基线 | | | |
| ۶ | 覆盖 | | ○分配完整性监控规则 分配/取清分配 □□ 属性 □ 导出 • □ □ 易出 | | | |
| | | | 名称 ▲ | 严重性 | 类型 | 最近更新时间 |
| | | | 🌍 1002773 - Microsoft Windows - 'Bosts' file modified | en 8 | 已定义 | 2010-05-26 |

2. 开启监控 hosts 文件的策略,扫描生成基线

| | 常規 高級 事件 | | | | | | | | |
|--------------|---|-----|-----|------------|--|--|--|--|--|
| 2/# # | 完整性協技 完整性協技状态: 打开 ▼ (■ 打开, 1 規則 倉用实时扫描 ■ 实时 | | | | | | | | |
| 9 监拉 2 | 完整性扫描 针对完整性的上次完整扫描: 2014-03-24 14:29 扫描完整性 | | | | | | | | |
| | ■ 上次创建的完整性基线: 2014-03-24 14:29 重新生成基地 查看基础 | | | | | | | | |
| | ○日分配完整性监控规则 分配/取消分配 □□ 属性 □□ 局性 □□ 局性 | | | | | | | | |
| | 名称 🔺 | 严重性 | 类型 | 最近更新时间 | | | | | |
| | 😌 1002773 - Microsoft Windows - 'Hosts' file modified | - 高 | 已定义 | 2010-05-26 | | | | | |

3. 修改测试机的 hosts 文件



| 软 件 测 试 网 | www.51testing.com | | | | |
|---|---|--|--|--|--|
| 文件(F) 视图(W) 虚拟机(V) ■ 11 | | | | | |
| Re Nots - Notepad File Edit Format View Help # Copyright (c) 1993-2006 Microsoft Corp. # This file contains the mappings of IP addresses # entry should be kept on an individual line. The # be placed in the first column followed by the co # The IP address and the host name should be separ # additionally, comments (such as these) may be in # lines or following the machine name denoted by a # # for example: # 102.54.94.97 rhino.acme.com # 127.0.0.1 localhost 12345678 | etc Search EP/IP for windows. to host names. Each IP address should prresponding host name. rated by at least one serted on individual a '#' symbol. source server x client host | | | | |

4. 扫描此时测试机的完整性,同时生成基准线

| አዙ 6 | 常規 高级 事件 完整性监控 完整性监控状态: 打开 実型性监控状态: 打开 ▼ 倉用实时扫描 实时 | | | | | | |
|--|---|--------------|-----------|----------------------|--|--|--|
| ま 出控 そ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ | 完整性扫描 针对完整性的上次完整扫描: 2014-03-24 14:29 | | | | | | |
| | 上次创建的完整性基线: 2014-03-24 14:29 東新生成基础 查看基础 已分配完整性监控规则 分配/取消分配 □□ 属性 □□ 属性 □□ 属性 | | | | | | |
| | 名称 ▲ | 严重性 ••• 高 | 東型 已定义 | 最近更新时间 2010-05-26 | | | |

5. 事件预警



| 常規 高級 | 事件 | | | | | | |
|-------------------------|--|---|---|--|---|--|--|
| 完整性监控事件 | 件 所有 👻 无分组 👻 | | Q 將當 | | | | |
| 期间: 最 | 近1小时内 | • | | | | | |
| 计算机: 计 | ¥机: | rmstest.hitechad.com (VDR Test) | Ŧ | | | | |
| 画 查看 23 导出 • 《 自动标记 摄 列 | | | | | | | |
| 时间 ▲ | 计算机 | 原因 | | 标记 | 更改 | | |
| 2014-03-24 14 | 1:32:30 | 1002773 - Microsoft Windows - 'Hosts' fi | ile modified | | 已更新 | | |
| | | | | | | | |
| | | | | | | | |
| | 常規 高級 完整性监控事 期间: 量 计算机: 计 回 查看 日 2014-03-24 14 | 常件 高级 事件 完整性监控事件 所有 ▼ 无分组 ▼ 期间: 最近 1 小时内 计算机: 计算机: 11 查看 马出 ▼ ④ 自动标记 时調 ▲ 计算机 2014-03-24 14:32:30 | 常規 高級 事件 完整性监控事件 所有 ▼ 无分组 ▼ 期间: 最近 1 小时内 ▼ 计算机: 计算机: ▼ mm 查看 □ 雪看 □ 雪子 ● 号出 ▼ ④ 自动标记 □ 列 时间 ▲ 计算机 ② 2014-03-24 14:32:30 10022773 = Microsoft Findows = "Hosts" feed | 常規 高級 事件 完整性监控事件 所有 ▼ 无分组 ▼ Q 排索 期间: 最近 1 小时内 ▼ 计算机: 计算机: ▼ mstest hitechad.com (VDR Test) ▼ 11 查看 □ 与出 ▼ ④ 自动标记 振 列 时间 ▲ 计算机 原因 2014-03-24 14:32:30 1002773 - Microsoft Findows - 'Hosts' file modified | 常規 高級 事件 完整性监控事件 所有 ▼ 无分组 ▼ 期间: 最近 1 小时内 ▼ 计算机: 计算机: ▼ 回 查看 马出 ▼ ④ 自动标记 时间 ▲ 计算机 即因 1002773 - Microsoft Tindows - 'Hosts' file modified | | |

6. 测试结果

| 项目 | 虚拟层无客户端完整性监控功能测试(针对 Win2008) | | | | |
|---|--|----|----|--|--|
| 时间 | 2014/3/27 | | | | |
| 步骤 | 描述 | 结果 | 备注 | | |
| 1.激活完整性监控功能可 以通过针对测试机生成完 整性基准线 | 该步骤用于启用 hosts 文件 监控 , 生成测试系统的完整 性基准线 | 成功 | | | |
| 2.更改测试机器的 hosts 文件 , 出发完整性监控策 略的实时性 | 该步骤用于触发部署的完整 监控策略,并且以事件的形 式发出通知 | 成功 | 无 | | |