RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

借助 USB HID 攻击未来

Nikhil “SamratAshok” Mittal
黑客

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

会话 ID：
会话分类：

关于我本人

- SamratAshok
- Twitter - @nikhil_mitt
- 博客：http://labofapenetrationtester.blogspot.com
- Kautilya、Mareech 和 Nishang 的创造者
- 对针对 PWN 系统的攻击性信息安全、新的攻击力和方法感兴趣。
- 之前发表过的演讲
  - Clubhack'10、Hackfest'11、Clubhack'11、Black hat Abu Dhabi'11、Black Hat Europe'12、Troopers'12、PHDays'12、Black Hat USA'12
- 近期将发表的演讲
  - 在 EUSecWest'12 上发表演讲
  - 在 GrrCON'12 上教授培训

内容安排

- 人机接口设备
- 在渗透测试中使用 HID
- 选择 HID — Teensy++
- 我们将如何使用 Teensy++？
- Windows 系列
- Mac OS X 系列
- Kautilya
- 攻击演示（在 Windows 8 和 Mountain Lion 上）
- 比较
- 未来的攻击
- 限制
- 防御
- 结论

人机接口设备

- 维基百科 —“*人机接口设备或 HID 是一种计算机设备，该设备可直接与人进行交互，大多情况下，由人向计算机输入信息，而计算机也可向人提供输出。*”
- 鼠标、键盘和游戏杆设备都是常见的 HID 设备。
- 哪些方面会出现问题呢？

在渗透测试中使用 HID

- 人机接口设备受操作系统的信任。
- 诸如反病毒一类的防御措施不会关注此类设备。
- 我们使用 HID 来保证攻击安全性的方式，就像自己以用户身份坐在目标系统前操作一样。
- 攻击案例数量巨大，而且可能会产生严重影响。

选择 HID – Teensy++

- 来自 pjrc.com 的 USB 微控制器设备
- 存储容量约 130 KB。
- 我们将使用 Teensy 的更新版本 Teensy ++。
- 该设备价格实惠，仅售 24 美元。
- 该设备采用基于 Atmel 的处理器。

选择 HID – Teensy++

- 可将其用作键盘/鼠标/游戏杆设备。
- 借助 Teensyduino 插件，可使用 C 或 C 类语法在 Arduino 开发环境中对该设备轻松进行编程。
- 该设备可与许多操作系统配合使用。
- 该设备的尺寸小巧。

我们将如何使用 Teensy++？

- 可作为可编程的键盘使用。
- 我们将对该设备进行编程，以便其在连接到系统时执行一组定义好的活动。
- 我们将利用目前登录用户的权限和该用户可访问的更高权限。
- 目的是模拟该用户坐在目标系统前的情景。

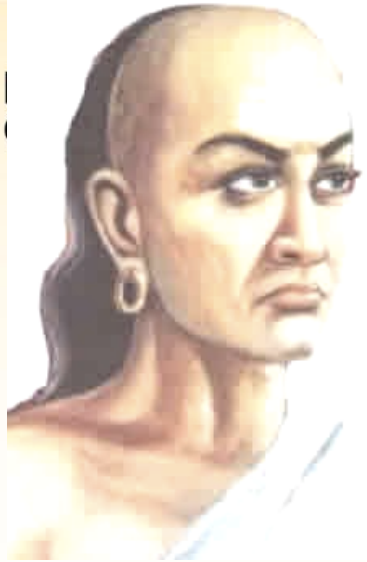
Windows 系列

- 有新设备连接时，会通知用户。
- 设备加载驱动程序需要 20 到 25 秒的时间。
- Windows 机器上的设备输入速度非常快，这得益于 Windows 上巨大的 USB 键盘缓冲器。
- 如果采用 PowerShell，功能将会更加强大。

OS X 系列

- 有 USB 设备连接时，不会通知用户。
- 检测和加载设备需要 10 到 15 秒的时间。
- 设备输入速度不是很快。
- 内置脚本语言使有效负载的能力得到增强。

Kautilya



- 这是一个工具套件，旨在使 HID 在渗透测试中更加有用。
- 以 Chanakya a.k.a. Kautilya 命名。
- 采用 Ruby 语言编写。
- 这是一个菜单驱动程序，可让用户选择以及自定义有效负载。
- 旨在使 HID 成为每位渗透测试人员工具箱的一部分。
- 包含针对 Windows、Linux 和 OS X 的有效负载。

Kautilya 中的有效负载

- 在不使用 SD 卡的情况下，测试 Teensy 上的有效负载。
- Pastebin 广泛用于上传和下载。
- 有效负载是命令、powershell 脚本或两者的组合。
- 插入设备后，有效负载依据登录用户的权限执行。

攻击演示
（在 Windows 8 和 Mountain Lion 上）

- 我们来看一看在这两种操作系统上实施的三种攻击
  - 下载并执行 shellcode。
  - 使用内置功能反向 shell。
  - 执行 DNS TXT 代码。

比较

属性	Windows 8	Mac OS X Mountain Lion
检测或阻止 USB HID	显示提示框。使用组策略可轻松防止安装可移动设备。	不对用户显示任何信息。难以阻止设备。
响应非常快速的键盘输入	发送输入的速度非常快。	在键盘输入之间必须有延迟。
信任最终用户（我们模拟的是最终用户）	对于敏感功能，会显示 UAC 提示。	敏感功能需要使用 Sudo。

Teensy 的局限性

- Teensy 中的存储空间有限。将 Teensy 与 SD 卡同时使用，即可解决这一问题。
- 无法从系统“读取”。您必须假设受害操作系统的响应，而且流量是单向的。

Kautilya 的局限性

- 许多有效负载需要管理员权限。
- 许多流量需要流入 pastebin 或从其中流出。
- 运行一次后，无法自行清除。
- 有效负载有时不稳定。
- 对于使用可执行文件的有效负载，需要手动将其转换并粘贴到 pastebin。

未来的攻击

- 目前的有效负载得到改善。
- 可将部分有效负载用作库，以便可再次使用。
- 非 Windows 平台的有效负载更多。
- 实施较新的有效负载。
- 检测可靠的用户活动。

防御

- 对于 Windows 系统，可使用组策略“防止安装可移动设备”。
- 对于 Mac OS X，可使用 udev 规则。
- 最好的防御方法是以物理方法阻挡 USB 端口或将现有设备锁定到端口。

结论

- USB HID 攻击有切实的威胁而且持续不断。
- 其原因是操作系统信任自己和自己的用户。
- 信任会带来安全隐患。

谢谢大家！

- 如果还有什么问题？
- 如果受到任何伤害？
- 如果有任何反馈？

- Kautilya 的网址为 http://code.google.com/p/kautilya/
- 关注我 @nikhil_mitt
- http://labofapenetrationtester.blogspot.com/