Trustwave®
SpiderLabs®

Earth vs. The Giant Spider: Amazingly True Stories of Real Penetration Tests

Rob Havelt - Director of Penetration Testing, Trustwave SpiderLabs
Wendel G. Henrique – Security Consultant, Trustwave SpiderLabs

BIO

SpiderLabs:~ Trustwave$ whois RHavelt

- Director of Penetration Testing at Trustwave's SpiderLabs.
- Over 18 years in the security industry.
- He has worked with offensive security seemingly forever, and from running a start-up ISP, to working as a TSCM specialist, he's held just about every job possible in the realm of system administration and information security.
- Formerly a bourbon-fueled absurdist, raconteur, and man about town, currently a sardonic workaholic occasionally seeking meaning in the finer things in life — Rob is, and will always be, a career hacker.
- Given Talks at Toorcon, Black Hat, Thotcon, BSides.

BIO

SpiderLabs:~ Trustwave$ whois WendelGH

- Security consultant (Penetration Test Team) at Trustwave's SpiderLabs.
- Over 9 years in the security industry.
- Co-authored patent-pending penetration testing technology.
- Spoke in Black Hat Arsenal 2010 (USA), OWASP AppSec Research 2010 (Sweden) and Black Hat Europe 2010 (Spain). Previously, Wendel spoke in Troopers 09 (Germany), OWASP AppSecEU09 (Poland), YSTS 3.0 (Brazil), and has spoken in well known security conferences such as DEFCON 16 (USA) and H2HC (Brazil).
- Discovered vulnerabilities across a diverse set of technologies including webmail systems, wireless access points, remote access systems, web application firewalls, IP cameras, and IP telephony applications.

First Thing First

- **Up here there is a Server. Its connected to a WiFi Network. In Fact there are 2 WiFi networks in here.**
- **We will be logging into this server as root at least every 5 min during this talk. Possibly more frequently.**
- **Whomever can give us the root password for this server before the end of this talk gets one of these spiffy T-Shirts.**
- **There are two ways we know should work to accomplish this. Use one of those 2 ways, or impress us with a 3rd way we haven't though of…**
- **We will explain the point of this all later in the preso.**

Outline

1. **What is This All About?**
2. **Collection of Weirdest, Freakiest, and Most Unlikely Hacks We've Found.**
3. **Meet the Victims - These have serious implications.**
4. **DEMO – What is that thing from before all about?**
5. **Conclusions.**

Trustwave®

SpiderLabs®

What is This All About?

What is This All About?

- **The unique opportunity to see real, interesting, uncommon and some non-trivial attacks that can't be found by automated tools.**
- **More than 2300 penetration tests were delivered last year by SpiderLabs and only the coolest and freakiest were selected to present at DEFCON 19.**
- **By the end of this presentation we hope to have the you thinking about systems and applications that organizations use every day, and how they may be used against them**

Trustwave®

SpiderLabs®

Collection of Weirdest, Freakiest, and Most Unlikely Hacks We've Found

Do you want Fries with that Hack?

- Huge restaurant network that also sells food via internet.
- Web Application developed in Java and Flash - maturity of security in development.
- No severe common issues (SQL Injection, Remote Code Execution, etc).
- Manipulate prices and similar parameters gave no juice.
- When buying with Credit Card we was redirect to a 3rd party server that holds the transaction.
- The CHD was not sent to target restaurant website, instead there was a JS script calling the 3rd party server with the properly parameters.
- At the end of negotiation, the 3rd party server sends an message via a secure channel telling if the transaction was approved or not, consequently the solicitation was processed or not.
- While the target restaurant website and 3rd party server were secure, there was no proper mechanism to validate if the data sent from one to the other via the customer browser was correct.
- Consequently, was possible to buy a sandwich, french fries, juice and ice cream with 50 cents and the receipt at the target restaurant website printed the real value (9.50 USD).

One PBX Will Rule Them All Hack.

- We found a field tech account on a Siemens ROLM PBX, and we cloned the Voice Mail for the corporate Tech support.
- Some guy called in after hours with a VPN problem, it was Checkpoint, and we actually knew what the problem was and how to fix it since we was very familiar with Checkpoint.
- So we called him back, and helped him fix it – but we asked for his username, and his Secure ID Pin, and had him read the number off his token, etc.
- BINGO! We logged in myself, then told him the settings that he needed to change to get his working.

The Inside-Out VPN Hack.

- Internal penetration test where the network segment was very limited (heavily filtered by firewall).
- All reachable systems had just a few services, including 2 OpenSSH servers, 1 Samba server and some Microsoft Windows answering to ICMP request (ping) but filtering almost all incoming connections.
- All services were well configured and up-to-date, also VLAN bypass was not possible.
- However, ARP Poisoning was possible.
- The bad news is that after 2 hours looking for traffic there was nothing useful.
- We decided to do an HTTPS MITM (Man In The Middle) with an self create certificate.
- User accepted it and we dumped the plain-text content of requests and responses.
- We found an session from an internal system to a external Web VPN SSL.
- From home, we started a session with this external server and cloned the cookies and we got access to several applications and file servers.

The Island Nation and Port 0 Hack.

- Very restrictive firewall in-place.
- However, when sending packets sourced from Port 0 it would go right through the firewall.
- Allowed to compromise all credit card processing for the whole country.

The Caucasian-Asian Love Hack.

- External Penetration Test with very few services.
- However there was an administrative web interface.
- Looking at comments and meta-data we found the e-mail of the Web Application developer.
- Researching at Internet we found that he had some code he posted in a newsgroup, but sadly that was not very helpful.
- But looking up the guy name, we found his Facebook page, and found a nickname that his friends called him.
- It turns out that he used that nickname on a site called "Caucasian-Asian Love" so we built a wordlist from his dating profile and it worked, he used a word from there as his password.

In Soviet Russia Hackers Monitor You Hack.

- External Penetration Test in a multi-national company.
- The main network in LAC was huge, but up-to-date.
- There was several uncommon services and applications.
- We found almost 20 IP HD Cameras accessible from Internet.
- No default password or well known vulnerabilities.
- We found a bypass on the authentication system and we discovered two Operating System undocumented accounts.
- Allowed us to monitor several places inside the company and even zoom up to 10x.
- We owned the Operating System that was connected to the internal network.
- Ref.: https://www.trustwave.com/spiderlabs/advisories/TWSL2010-006.txt).

Oracle and The New Tool Hack

- Internal Penetration Test where just Oracle databases were accessible.
- Oracle databases well hardened, not success on direct compromise.
- ARP Poisoning was possible, looking for almost 2 hours the traffic there was just Oracle.
- However no new sessions was established since we were looking.
- We used thicknet to hijack an pre-existent Oracle session and take-over the database.
- Ref.: https://www.trustwave.com/downloads/spiderlabs/Trustwave-SpiderLabs-Oracle-Interrupted-Henrique-and-Ocepek.pdf

Trustwave®

SpiderLabs®

Meet the Victims - These have serious implications

Meet the Victims - These have serious implications.

None of these attacks lead to anything trivial. Nor were these trivial organizations. Most of them had a lot to loose and some major juice.

- Types of Organizations We are Talking About Here:
  - A Few Multi-National Banks
  - A Global Restaurant Franchise
  - A Credit Card Processor for an Entire LAC Nation
  - A Major Retail Chain

- Types of Data Stolen / Accessed
  - Every Visa and Mastercard transaction processed in an entire country.
  - Hundreds of Millions of Credit Card PAN and Track Data
  - HR Data for global organizations
  - The DHS Terrorist Watch List for Financial Institutions
  - Billions of Dollars

Trustwave®

SpiderLabs®

DEMO: Who won a T-Shirt?

Trustwave®
SpiderLabs®

Conclusion

Conclusion

- This talk was focused on those complex or uncommon hacks found in real environments.
- Some in very high end and important systems, that are unlikely but true.
- This is indeed a bizarre world where odd business logic flaws get you almost free food [including home shipping], sourcing traffic from port 0 allows ownership of the finances a nation, and security systems are used to hack organizations.
- We are happy to be here [again] and hope you have enjoyed.
- Contact us:

Rhavelt <arroba> trustwave <ponto> com
Whenrique <arroba> trustwave <ponto> com