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

Wendel Guglielmetti Henrique

Rob Havelt

Trustwave - SpiderLabs

Session ID: HT1-202

Session Classification: Intermediate

RSA CONFERENCE 2012

First things, first!

- Thanks to Steve Ocepek (@SpiderLabs) for co-author the “Oracle injection” project (thicknet).
- Thank YOU guys for your attention.
- Thanks RSACONFERENCE staff – you are awesome!

What is This All About?

What is This All About?

- More than 2300 penetration tests were delivered last year by SpiderLabs and some of the coolest were selected to present at RSACONFERENCE.

- The unique opportunity to see real, interesting, uncommon and some attacks that can't be found by automated tools.

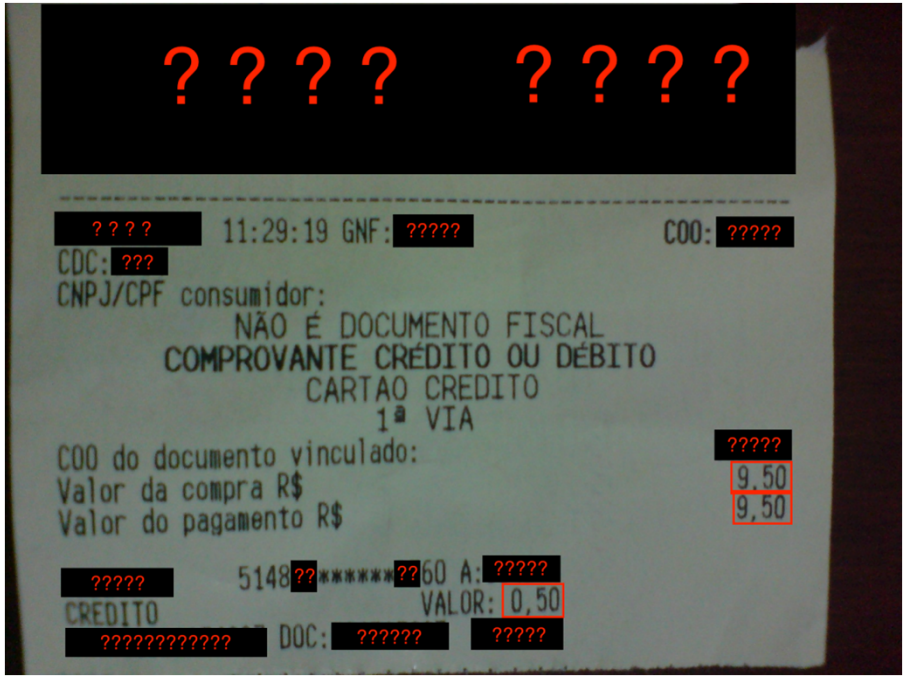
Collection of Weirdest, Freakiest, and Most Unlikely Hacks We've Found

Do you want Fries with that Hack?

- Big restaurant network that also sells food via internet.
- Web Application developed in Java and Flash - maturity of security in development.
- Redirected to a 3rd party server that holds the transaction (Credit Card).

Do you want Fries with that Hack?

- A sandwich, french fries and juice with 25 cents and the receipt at the target restaurant website printed the real value (R$9.50).



Breaking VPN from Internal to External

- Internal penetration test where the network segment was very limited (heavily filtered by firewall), systems well configured, up to date and no VLAN bypass.
- However, ARP Poisoning was possible.
- Found Web VPN SSL with self create certificate.

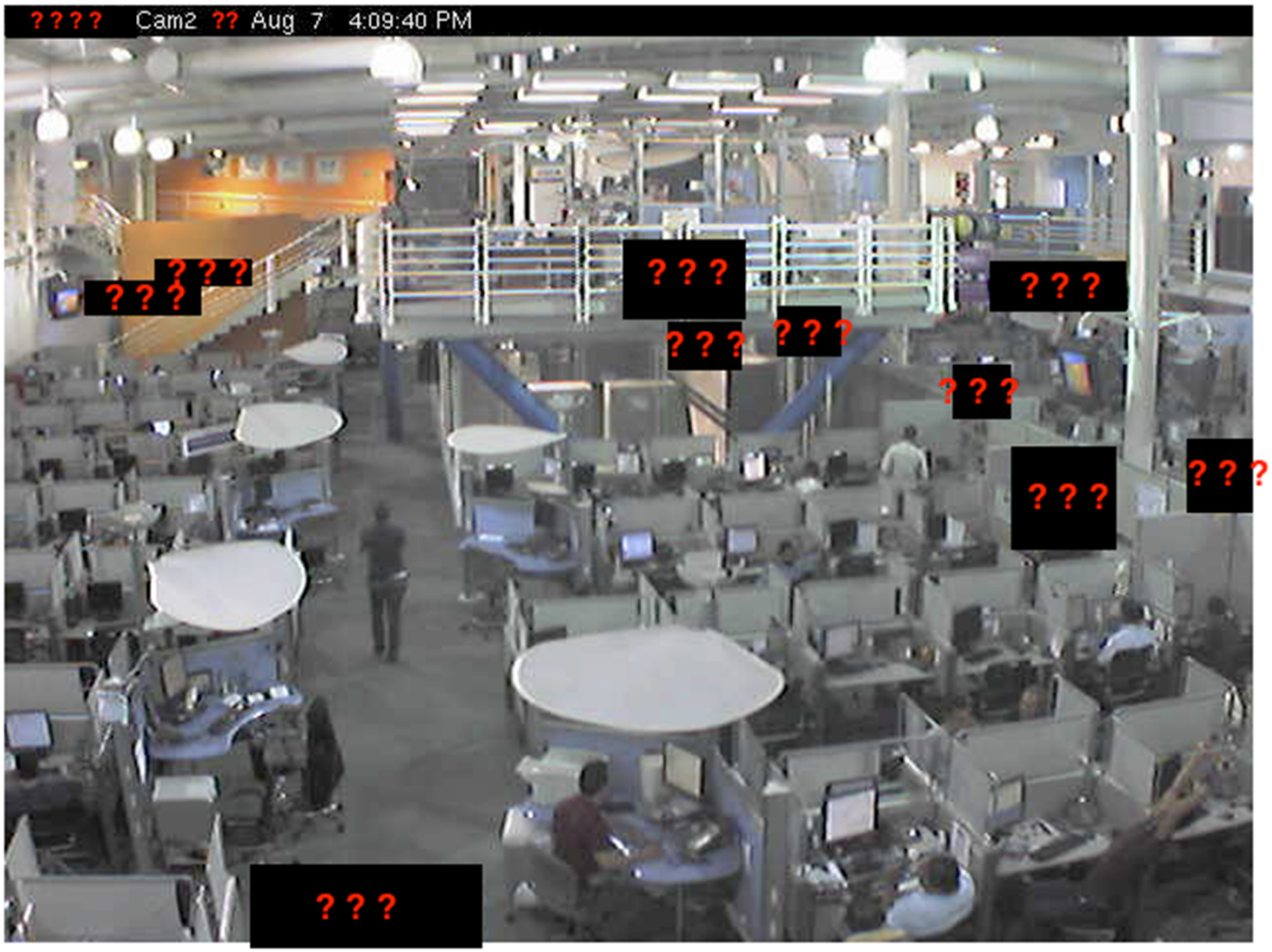
IP Camera: Hackers Monitor you.

- External Penetration Test in a multi-national company. The main network was huge, but very well up to date.
- On a small Internet accessible subnet, we found about 20 IP HD cameras.
- No default passwords or published vulnerabilities so what's the harm?

IP Camera: Hackers Monitor you.

- Found a way to bypass the authentication system, and two OS undocumented accounts.
- Able to access the camera functionality – turns out these were surveillance cameras.

IP Camera: Hackers Monitor you.



IP Camera: Hackers Monitor you.

- We owned the Operating System that was connected to the internal network.
- BONUS: 10x optical zoom.
- Ref.: https://www.trustwave.com/spiderlabs/advisories/TWSL2010-006.txt

Client-Side: Payloads matter!

- As we all know client-side with phishing e-mails are an awesome way to compromise companies.
- However, we missed a robust payload for client-side because:
- Antivirus, x64 compatible, very restricted outgoing policy.

Client-Side: Payloads matter!

- Launch the attack and go to beach and wait for the evidence to arrive. ☺

Date/Time	Sender	Subject	Action
Fri, 11:57am	srod	PenTest-ClientSide-Evidences	Deliver
Fri, 11:54am	llop	PenTest-ClientSide-Evidences	Deliver
Fri, 11:54am	lpat	PenTest-ClientSide-Evidences	Deliver
Fri, 11:52am	dgo	PenTest-ClientSide-Evidences	Deliver
Fri, 11:48am	dgo	PenTest-ClientSide-Evidences	Deliver
Fri, 11:41am	cloz	PenTest-ClientSide-Evidences	Deliver
Fri, 11:40am	cpe	PenTest-ClientSide-Evidences	Deliver
Fri, 11:36am	gsa	PenTest-ClientSide-Evidences	Deliver
Fri, 11:32am	agu	PenTest-ClientSide-Evidences	Deliver
Fri, 11:22am	nmu	PenTest-ClientSide-Evidences	Deliver
Fri, 11:12am	pbe	PenTest-ClientSide-Evidences	Deliver
Fri, 11:12am	lorti	PenTest-ClientSide-Evidences	Deliver
Fri, 11:10am	fher	PenTest-ClientSide-Evidences	Deliver
Fri, 11:04am	ssie	PenTest-ClientSide-Evidences	Deliver
Fri, 11:04am	vgo	PenTest-ClientSide-Evidences	Deliver
Fri, 10:52am	mgc	PenTest-ClientSide-Evidences	Deliver
Fri, 10:52am	ydia	PenTest-ClientSide-Evidences	Deliver
Fri, 10:51am	dmf	PenTest-ClientSide-Evidences	Deliver
Fri, 10:50am	jaye	PenTest-ClientSide-Evidences	Deliver
Fri, 10:45am	crin	PenTest-ClientSide-Evidences	Deliver
Fri, 10:45am	lfore	PenTest-ClientSide-Evidences	Deliver
Fri, 10:41am	yroa	PenTest-ClientSide-Evidences	Deliver
Fri, 10:36am	dmf	PenTest-ClientSide-Evidences	Deliver
Fri, 10:28am	lher	PenTest-ClientSide-Evidences	Deliver
Fri, 10:27am	ydia	PenTest-ClientSide-Evidences	Deliver
Fri, 10:26am	lher	PenTest-ClientSide-Evidences	Deliver
Fri, 10:26am	sgu	PenTest-ClientSide-Evidences	Deliver
Fri, 10:15am	pes	PenTest-ClientSide-Evidences	Deliver

Breaking Into a Secure Environment!

- Internal penetration from Thin-Client (well hardened) workstations with restricted privileges.

- Require password and smartcard (dual factor authentication).

Modifying Database Traffic On-the-Fly

- Internal Penetration Test where just Oracle databases were accessible. Oracle databases well hardened, not successful on direct compromise.

- ARP Poisoning was possible, looking at the traffic for almost 2 hours and there was just Oracle. However no new sessions were established since we were looking.

Modifying Database Traffic On-the-Fly

- We used thicknet (thanks Steve Ocepek) 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

Modifying Database Traffic On-the-Fly

VIDEO / DEMO

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 small organizations with immature security programs. Most had a lot to lose.

- Types of organizations we are discussing include; multi-national banks, big restaurant franchise, major retail chains, large credit card processors.

Conclusion

Conclusion

- This talk focused on those complex or uncommon hacks that were nonetheless found in real life.

- You will not get this sort of intelligence unless you test your processes and controls thoroughly and manually.

Apply This

- When you get back to work, pick any random system (for example the one that controls the electronic door locks, or your HVAC system).
  - Imagine you are an attacker
  - Write down FOUR(4) different scenarios of how this system could be leveraged to get payroll data.
- Over the next few months
  - As you plan security controls for anything new, think of at least 4 or more ways every component could be used in an attack – even if it seems like a stretch.

Questions?

- Questions?

- Contact us:

whenrique <at> trustwave <dot> com

rhavelt <at> trustwave <dot> com