Professional Pen Testing
&
Learning From Your Mistakes

Who / What / Why

Who am I?

- Adam Compton
  - security researcher, pentester, programmer
  - **NOT** a presenter

What am I presenting?

- A ***VERY*** basic engagement methodology
- Lessons learned from over a decade of engagements

Why should you listen to me?

- I have ~~**made**~~ seen LOTs of mistakes ;)

Sample Methodology

- Pre-Engagement Interactions
- Information Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation/Post Exploitation
- Report Writing
- Report Delivery/Follow-up Call

*You can also check out **http://www.pentest-standard.org***

Pre-Engagement Interactions

SALES ENGINEER
YOUR SALES REP TOLD US THAT THE PRODUCT HEALS ITSELF. IS THAT TRUE?
IT'S TOTALLY TRUE... THAT HE SAID THAT.
LET ME ASK THIS ANOTHER WAY...
NOOO!!! ONE WAY PER QUESTION!
www.dilbert.com scottadams@aol.com
1-9-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.

© Scott Adams, Inc./Dist. by UFS, Inc.

*"Our team **WILL** find **ALL** of the vulnerabilities."*

…

"You don't want us to use any computers, OK, we can do that."

So, who is bored?

The sad story of the world's most unfortunate consulting team.

Once upon a time ...

... there were three information security consultants ...

A New Engagement ...

... for a large international diaper company ...

External Information Gathering ...

... without verifying the provided IP addresses ...

Social Engineering ...

... reused old phishing template ...

... forgot to replace all instances of old customer names ...

External Penetration Test ...

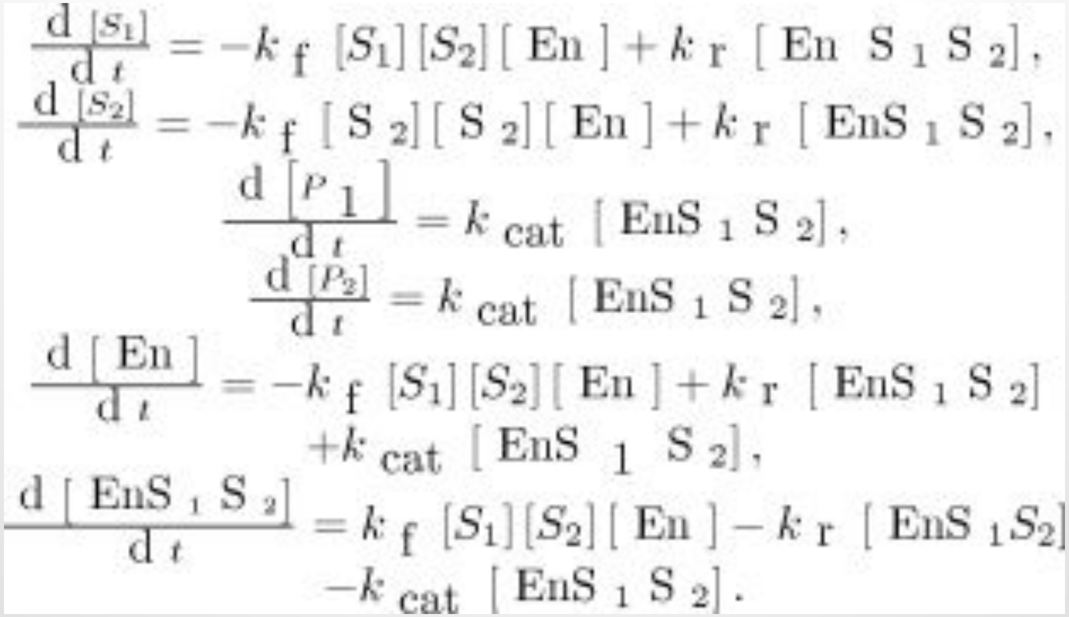
... enabled the host firewall on the compromised system ...

Time for Travel ...

... got their shots, bought their tickets, gathered their equipment, and flew to
"Kiss-My-Ass-Goodbye"-astan ...

Internal Assessment ...

... during the dividing of the targets, one network range was forgotten/overlooked ...



$$\frac{\mathrm{d}\,[S_1]}{\mathrm{d}\,t} = -k_{\mathrm{f}}\,[S_1][S_2][\,\mathrm{En}\,] + k_{\mathrm{r}}\,[\,\mathrm{En}\ \ \mathrm{S}_1\,\mathrm{S}_2],$$

$$\frac{\mathrm{d}\,[S_2]}{\mathrm{d}\,t} = -k_{\mathrm{f}}\,[\,\mathrm{S}_2][\,\mathrm{S}_2][\,\mathrm{En}\,] + k_{\mathrm{r}}\,[\,\mathrm{EnS}_1\,\mathrm{S}_2],$$

$$\frac{\mathrm{d}\,[P_1]}{\mathrm{d}\,t} = k_{\mathrm{cat}}\,[\,\mathrm{EnS}_1\,\mathrm{S}_2],$$

$$\frac{\mathrm{d}\,[P_2]}{\mathrm{d}\,t} = k_{\mathrm{cat}}\,[\,\mathrm{EnS}_1\,\mathrm{S}_2],$$

$$\frac{\mathrm{d}\,[\,\mathrm{En}\,]}{\mathrm{d}\,t} = -k_{\mathrm{f}}\,[S_1][S_2][\,\mathrm{En}\,] + k_{\mathrm{r}}\,[\,\mathrm{EnS}_1\,\mathrm{S}_2] + k_{\mathrm{cat}}\,[\,\mathrm{EnS}\ _1\ \mathrm{S}_2],$$

$$\frac{\mathrm{d}\,[\,\mathrm{EnS}_1\,\mathrm{S}_2]}{\mathrm{d}\,t} = k_{\mathrm{f}}\,[S_1][S_2][\,\mathrm{En}\,] - k_{\mathrm{r}}\,[\,\mathrm{EnS}_1 S_2] - k_{\mathrm{cat}}\,[\,\mathrm{EnS}_1\,\mathrm{S}_2].$$

Internal Pentest ...

... spent a few hours pentesting each other's machines ...

Setting off the Egress Alerts ...

... the consultants had forgot to disable all of their p2p clients ...

Wireless Audit ...

... had never noticed how suspicious he looked
... until he was surrounded by guards ...

Wireless Audit ...

... had never noticed how suspicious he looked
... until he was surrounded by guards ...

Going Home ...

... it was totally ok to leave the country with 1 plastic coat hanger ...

Lost a Co-Worker ...

... quit while onsite at a customer ...

Report Writing ...

... everyone had thought that the others were going to gather the screenshots ...

Report Delivery ...

Finally, the report was completed and delivered to the customer... with many many mistakes and issues...

© Ron Leishman * www.ClipartOf.com/439412

General Lessons Learned

"Measure twice, cut once.”

When unsure, ask questions.

Never assume you know everything.

...

Share your mistakes.

Questions/Contact Info

THANK YOU

Any questions?

I can be contacted at:
@tatanus
@PentestLessons