Operating Systems Security
And Why It (Mostly) Doesn't Matter

Patrick Hof - RedTeam Pentesting GmbH
patrick.hof@redteam-pentesting.de
https://www.redteam-pentesting.de/

Radboud University, Nijmegen, 19 December 2016
• Founded in 2004 at RWTH Aachen University
• 9 penetration testers
• Conducting penetration tests world-wide
• Specialisation exclusively on penetration tests
• Targets and attacker-model defined in preliminary meeting
• Conducted from the attacker's perspective
  → Same methods as “bad guys”
• Individualised search for security vulnerabilities
• Detailed documentation
If you look at the security-related headlines in 2016, we're pretty much doomed

Large data breaches 2016 (just to name a few):
- Dec 14th, Yahoo: More than 1B(!) user accounts (from August 2013)
- Nov 23rd, AdultFriendFinder: 421M user accounts
- Sep 2nd, Dropbox: 68M user accounts (from 2012)
- May 17th, LinkedIn: 117M user accounts (from 2012)
- and the list goes on...¹

¹ Source: https://www.identityforce.com/blog/2016-data-breaches
We even have logos now! Finally, people will understand the severity of the situation!

- **DIRTY COW**
  - CVE-2016-5195

- **Lock icon**
  - CVE-2016-0800

- **Wizard with wand**
  - CVE-2016-3714

- **Ghost with smiley face**
  - CVE-2015-0235

- **Shell icon**
  - CVE-2014-6271

- **Heart with blood**
  - CVE-2014-0160
Why do we see so many incidents?
There seem to be more security-related incidents than ever
In our pentests, we usually can achieve what we agreed before should not happen, why is that?
Defense Mechanisms Are Getting More Advanced

- IDS/IPS
- Traffic analysis up to application layer
- Antivirus
- Security appliances combining all of the above
- Operating systems security (ASLR, DEP/NX etc.)
- 2FA
- Centralized security, e.g. group policies on Windows
- …
When we started 10 years ago, “pentests” were not widely known

Now, companies are investing more than ever in IT security (search for “Hot Cybersecurity Stocks 2016” on Google, I dare you)

Shouldn't this reduce the amount of incidents?
Ok, so maybe things are not as bad as I make it look like.
Why so Many Incidents?

- Theory: Working as a pentester only shows very vulnerable companies, everyone else is secure and therefore doesn't do pentests.
Theory: Working as a pentester only shows very vulnerable companies, everyone else is secure and therefore doesn't do pentests.

Answer: No, those who do pentests are rather security-aware, otherwise they wouldn't bother.
Why so Many Incidents?

- Theory: The media are giving a skewed view on things for the sake of making scary headlines about “the cybers”, therefore making it seem worse than it actually is.

“So we have to get very, very tough on cyber and cyber warfare. It is a, it is a huge problem. I have a son. He's 10 years old. He has computers. He is so good with these computers, it's unbelievable. The security aspect of cyber is very, very tough.”

– Abraham Lincoln
Why so Many Incidents?

- Theory: The media are giving a skewed view on things for the sake of making scary headlines about “the cybers”, therefore making it seem worse than it actually is.

- Answer: Might be partly true, but apart from the usual media sensationalism, many hacks are real. We do see a lot of vulnerable systems in our work and we also get feedback from clients about breaches they had that were never reported to anyone.
• Theory: There is so much money in the security industry that everyone is interested in scaring people into buying as much “security” as possible.
Why so Many Incidents?

• Theory: There is so much money in the security industry that everyone is interested in scaring people into buying as much “security” as possible.

• Answer: Partly true, there's a lot of very questionable stuff out there that makes millions in profits, but as I already said: we do see a lot of very insecure systems in our work, and if you look at the recent security research, others do too.
Some ideas what the real problems could be:

- Everything is online these days, or in the process of going online: Banking, shopping, social interaction...
- IT is more and more prevalent in every company, (almost) nobody works without IT or the Internet
- Employees should be able to work from anywhere (and be available 24/7), so remote access is needed even from private hardware (BYOD)
- Things change fast, companies are trying to keep up with the latest trends
- There is a huge market for cheap gadgets and the “Internet of Things”
Complexity breeds bugs, bugs are vulnerabilities waiting to be exploited

Companies add more features instead of securing the already available

Attackers are interested in data, not necessarily a root shell
The Real Problems

- Malvertising: Ad networks currently have a huge malware problem
- Content Delivery Networks (CDN):
  - One hack, millions of victims
  - Hide behind the “big name” when delivering malware
- JavaScript bloat
  - March 2016: The “left-pad fiasco”\(^1\): 2,486,696 downloads in February alone for a module that left-pads strings!
  - Again: hack one developer, target *loads* of applications

\(^1\): [http://www.haneycodes.net/npm-left-pad-have-we-forgotten-how-to-program/](http://www.haneycodes.net/npm-left-pad-have-we-forgotten-how-to-program/)
The Real Problems

More Buzzwords:
- Internet of Things (IoT)
- The Cloud
- Antivirus
- Smartphones
9.12.2016: Netgear, 8 models can be exploited like it's '99:

http://<router_IP>/cgi-bin/;COMMAND

- This is how I exploited my Linksys WRT54G Wi-fi router to install Linux, in 2002! Even then, command injections were already a well-known vulnerability.
- There are exploit kits used by malvertisers to open up home routers with vulnerabilities like this one.
Antivirus software is often indistinguishable from a kernel root kit

Embeds itself deeply into the system, hooking kernel functions

Check out Tavis Ormandy's work at Google Project Zero

- Exploits for Symantec and Norton, Avast, Trend Micro...

Recent research (12.12.2016) by Andrew Fasano: McAfee Virus Scan for Linux, 10 vulnerabilities that can be chained to achieve remote command execution as root

1: https://nation.state.actor/mcafee.html
• Problem: Transparently sending objects back and forth blurs the distinction between untrusted client and trusted server for programmers

• One of the newer tools (released 2015): ysoserial¹

```java
ObjectInputStream.readObject()
AnnotationInvocationHandler.readObject()
[...]
Runtime.getRuntime()
InvokerTransformer.transform()
Method.invoke()
Runtime.exec()
```

¹: https://github.com/frohoff/ysoserial
Operating Systems Security:
Mostly Post Exploitation
aka: we already got the data, but while we're at it...
In many cases: Once you are part of the domain, it is just a matter of time until you are domain admin.

Get local user hashes/tickets from memory.

If not already domain admin: Access other machines with credentials/hashs/tickets found until you have a domain admin account.

Game over, connect to domain controller and create for example a golden ticket.

mimikatz\(^1\) implements all this.

---

\(^1\): https://github.com/gentilkiwi/mimikatz
Linux is found mostly on servers

There, you have the usual problem: Only few install their patches on time
→ Outdated kernel, glibc etc.

Use local privilege escalation to get root

More fragmented, rather individual how you can get access to more systems

E.g. passwords in the .bash_history, private SSH keys, weak passwords, open shares, config files with credentials...
We start to see that consumers demand security, but only when it hurts (e.g. Ransomware).

Nobody cares if they're part of a botnet, everyone cares if their family photos are encrypted (or for companies: their precious Excel reports).
Are We Really Doomed?

- Reduce complexity (KISS) instead of increasing it
- Make security part of the development cycle
- Patch your systems regularly!
- Not everything needs to be connected to the Internet
Thank you for listening!