There is nothing on this system

Tales of doom

Presented by Robert Smith
Disclaimer

• Opinions expressed are solely my own and do not express the views or opinions of the University of California.

• This is an educational presentation.

• Case studies are simple abstractions.
Case study - North UC

• System 1 – compromised – “nothing”
  • 100% public information
• But wait, it had credentials and permissions to access to 3 other systems
  • 2 of the other systems had access to sensitive information!
• Intrusion = yes
• Information disclosure = no (lucky)
• Just the external forensics costs ~$70K and weeks of staff time!
Heike Noller of Denver, CO

Lake Powell in the Ticaboo Mesa area, 260’ rappel
Multi-sport athlete, she excelled in diving, cycling, skydiving, kickboxing and other sports “I felt like it was nothing special anymore...and that’s, you know, the danger”.

Heike Noller of Denver, CO
Case study – So Cal UC

• A system in admissions
• Local policy – *nothing* stored on PCs
• Reality – long term UC person
  • Testing applications
  • Custom reports
  • Wonderful assortment of Excel Kung Fu
  • SSNs
• $11K spent to meet “no disclosure” threshold
Anatomy of a pivot
Anatomy of a pivot
Step 0: Attacker places content on trusted Site
Step 1: Client-side exploitation

“Nothing on this machine!”

Vector: Social engineering, phishing, watering hole, spoofed e-mail
Step 2: Establish command and control – “C2”
Steps 3 & 4: Dump hashes and use pass-the-hash attack to pivot
Step 5: Pass the hash to compromise others
Steps 6 and 7: Exfiltration

- “Nothing”
  - Account information
    - Credentials
    - Help Desk
  - Web history
  - Network history
  - Key loggers
    - Everything every user does

- “Sensitive information”
  - Financial Aid
  - PHI
  - Employee records
  - FERPA
  - Research
  - PCI – credit cards
Case Study – North UC

• 3 systems impacted
  • Attackers entered through one system
  • Unpatched Java on one system let the attackers in
    • Researcher had simply visited a popular website offering help on the use of Microsoft Excel formulas.

• But wait!
  • 30K files encrypted
    • “… which contained critical data collected for several ongoing multi-year studies.”
  • Some data lost forever …
  • “Had we been subject to the HIPAA regulations or if the terms of our grants had included requirements that we meet federal information security standards, we could have faced millions of dollars in fines, termination of our grants, and the potential for an adverse determination in future grant applications.”
How hard is this?
Video Demo

• Part 1: https://youtu.be/a08m53W3xUw
• Part 2: https://youtu.be/4sKFKNyMw8Y
How hard is this?

Selling lucky find of over 1000 FULLZ
Discussion in 'General Fraud Discussion' started by BaronClodfelter, May 13, 2016 at 4:53 PM.

Tags: database, dumps, futz

Go to First Unread

BaronClodfelter
New Member

[Image: @bangbang786]

Thanks to a stroke of luck and some help from @bangbang786 I have come across a medical database with over 1000 FULLZ see pic below:

[URL]https://anonimgur.com/[URL]

Looking to sell the whole thing PM me if you're interested!!!!
YouTube

[Image of YouTube search results for "hack apache web server"]

[Image of YouTube search results for "hipster site builder"]

[Image of YouTube search results for "how to hack wordpress"]

[Image of YouTube search results for "how to hack websites"]

New Directions in Risk and Safety
Case Study - So Cal UC - Nothing

- Compromised web server
- Got admin credentials
- Got onto a system with nothing on it
  - But wait
  - That system had visibility to 500+ more systems
  - And the attacker was now “admin”
- Ransomware!
- Just the forensics > $50K
  - + org impact
- Near miss
Wrap
Summary

• Climbing third hand
  • “Not too long ago, people thought that backing up rappels was strictly for sissies, or something you'd only resort to in special situations - bringing down an injured or incompetent climber, for example.”
  • Today - virtually every guide and climbing safety course teaches the use of an autoblock or third hand.
    • We assume something will go wrong
    • Many points of failure
    • Known good way reduce risk!

• Nothing on that system
  • Asymmetry of information security
    • The good guys have to protect all the points of entry ….
    • Christoffer - “A defender can never win, he can only delay the inevitable, the eventual victorious attacker. The defender have to protect against all attacks, arguably a somewhat difficult task.”
  • The bad guys just need one way in.
  • Asymmetric warfare is war between combatants whose relative power differs significantly or whose strategies or tactics differ significantly.
  • Even systems with nothing on them need to be appropriately secured.
    • Known good way to reduce risk!
    • Information security third hand
Sources

- [https://www.sans.org/](https://www.sans.org/)
- [Backpacker Magazine - 2016](http://canyoncollective.com)
- [Video demo of pivot attack](https://youtu.be/a08m53W3xUw)
  - Brandon McCann
  - [https://youtu.be/4sKFKNyMw8Y](https://youtu.be/4sKFKNyMw8Y)
Contact Page

Email: robert.smith@ucop.edu

Phone: (510) 587-6244