Gage Gutmann
Davis Lee
Alex Banning

Proposal

Due Date: 4:40pm on Thursday, Nov. 7th (both hard copy and Dropoff)

The proposal must contain which cyber attack or vulnerability your group has chosen, the key questions that your group will answer about the attack or vulnerability, and at least three sources you will use to answer the questions.

Attack: Sony Pictures 2014 Hacks
Sources:

https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

https://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12

http://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/

https://www.vice.com/en_us/article/bmvn3m/sony-hack-cyberweapons-report

https://privacyrights.org/data-breaches/sony-pictures

http://nymag.com/intelligencer/2014/12/sonys-very-very-expensive-hack.html

---

Key Questions:

What are you researching? Is it an attack or a vulnerability?

Attack

If your group is reporting on an attack:

o **When was the attack? Who was the perpetrator? Who were the victims?**

- November 24, 2014
- Guardians of Peace (GOP)
- Celebrities, Employees and Freelancers of Sony
    - People associated with Sony or its products

o **Give a detailed, technical account of what vulnerabilities the attackers exploited. In giving this account, you must apply concepts learned in this course. If the technical details are not known, your group must choose a different attack or vulnerability.**

- The GOP initially hacked into one server that was not so well protected, and escalated the attack to gain access to the rest of the network. Looks like Sony Pictures did not have a defense-in-depth approach to their security. The network was not layered well enough to prevent breaches occurring in one part of their network to affect other parts of the network. In addition, the password "password" is obviously not good enough, however this was used in 3 certificates. These certificates were published by GOP, and they were subsequently used to digitally sign malware. (Source: Lessons we can learn from Sony Pictures Hack)
- Weak servers that were not mediated well were compromised. Subsequent server paths were unprotected on the inside of the network, so once GOP broke through the outermost layer of security, it got easier as they went along.

o What countermeasures, technical or non-technical, would have prevented this attack? What countermeasures would have detected it sooner (especially if the attack was not detected while it was occurring)?

- Complete Mediation
- Strong Passwords
- Server and Network hardening
- Better cyber hygiene
- Logging and monitoring all server activity as well as a better-designed database would have helped detect sooner

How were confidentiality, integrity, and availability compromised during the attack or as a result of the vulnerability?

- Confidentiality: Worker profiles leaked
- Integrity: Data was deleted
- Availability: Computers were compromised, and the network had to be quarantined

What surprised the members of your group about this attack or vulnerability? What does it teach us about computer security? (E.g., how does it reinforce one of the security design principles?)

I found it very surprising that in 2014 Sony was still storing plaintext passwords anywhere in their database. Furthermore, the fact that there were employee SSNs (full, not last 4 digits) stored in plaintext as well is astounding. Finally, the fact that Sony's servers were all interconnected to vulnerable entry points is very surprising. A company as large and tech-based as Sony should have had a better-designed system.

These vulnerabilities help display the importance of encrypting data and creating secure, completely mediated database environments. At the very least, if a company's servers aren't undeniably secure, they should be encrypting the data stored on it; ideally, both conditions should be true.

What outstanding questions do you have about the attack or vulnerability? What would you research further if you had the time?
Optional

If your group is reporting on an attack:

o When was the attack discovered? Who discovered it? How?

- Discovered November 24th. (unknown when attack was initiated)
- Employees of Sony
- Message appearing on computers stating they'd been hacked

o If the attack was a data breach, how many records were stolen? (If it is not known, include what experts have estimated.) Which types of sensitive data were stolen?

- 47,000 people's personal data was stolen
- personal information, salaries and home addresses

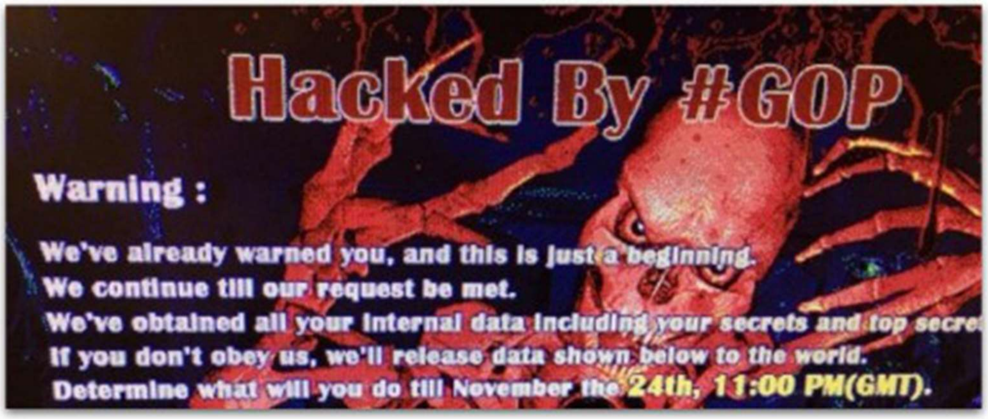
o If the victim was a third party, who were their clients?

The victim, Sony Pictures, took most of the brunt of the attack; however, many clients, employees, and partners of Sony took massive financial hits from this attack. Just the contributors of the movies *Annie*, *Mr. Turner*, and *To Write Love On Her Arms* alone experienced massive financial loss because GOP released these movies for free on Torrent sites, where they were downloaded well over 100,000 times in total. Additionally, all of the employees (former and current) who had their SSNs leaked certainly experienced a great amount of hardship dealing with the repercussions of re-securing their identities.

o Was the vulnerability known before it was exploited? If so, were countermeasures put in place? If not, why not? If so, how did the countermeasures fail?

The vulnerability was not known before the attack. The attackers left the following threatening message on all Sony network computers and displayed all of the data they had stolen. They also deleted original copies of the data from Sony computers.

Image:



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).

The counter measures that took place after the attack include:

- Hardened servers in Sony Network to be more secure and vigilant
- Updated corporate password policy
- Educated employees on the importance of security
- Implemented continuous logging and monitoring systems and updated software/firmware of existing ones

o Organizational losses:

§ Were any fines or judgments levied against the organization at fault? By whom, for what, and for how much?

§ Were the organization’s operations or services disrupted? For how long?

§ Did the attackers steal money? How much? From the organization or from its clients?

§ Were information assets or physical assets damaged or destroyed?

§ How much money is the organization estimated to have lost as a result of the attack?

How does the attack or vulnerability relate to one or more of the major legal and ethical questions surrounding computer security or privacy?