

Sony Hack

A Nauseating Whodunit

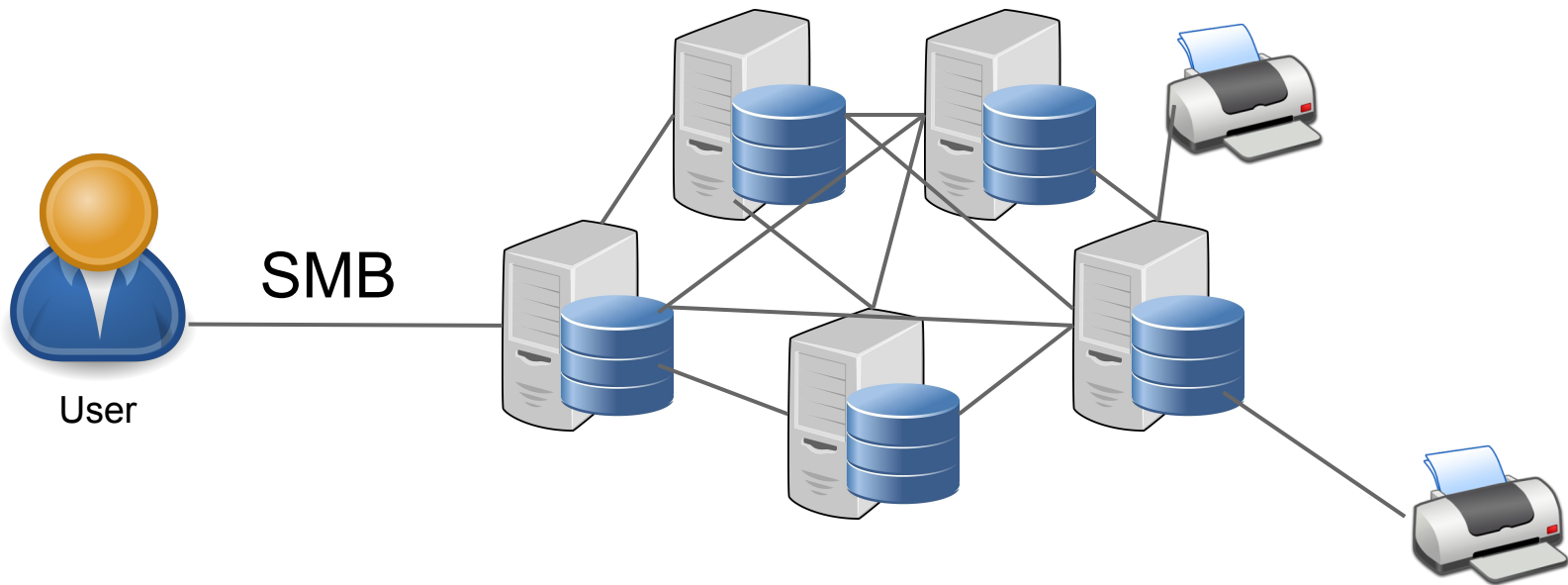
“North Korea threatened an attack if Sony Pictures released *The Interview*, forcing us all to pretend we wanted to see it.” -Amy Poehler

What Happened?

- November 21 - Email sent to Sony execs asking for money
- November 24 - Sony Picture's Entertainment hacked
 - Hackers named Guardians of Peace (#GOP)
- November 27 - Information begins to be leaked
 - 5 films dumped into file-sharing hubs
- December 5 - Employees asked to repudiate Sony; GOP threaten violence
- December 7 - North Korea denies all involvement
- December 8 - GoP demand that The Interview be pulled
 - Denies involvement in December 5th message
- December 19 - FBI concludes that North Korea perpetrated attack
- December 21 - North Korea threatens violence if US retaliates
- December 22 - US asks North Korea to compensate Sony

How was Sony breached?

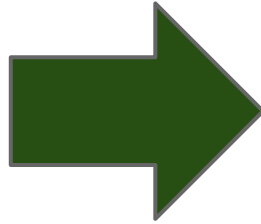
- Sony uses a file sharing network known as *Server Message Block* (SMB)
- SMB connects users to file shares and printers throughout a network



How SMB works



User



Connect to Host
Running SMB



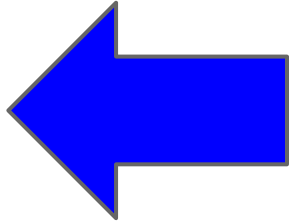
SMB Network

The user connects to a host using TCP through port 445 (SMB runs on port 445)

How SMB works



User



Authentication

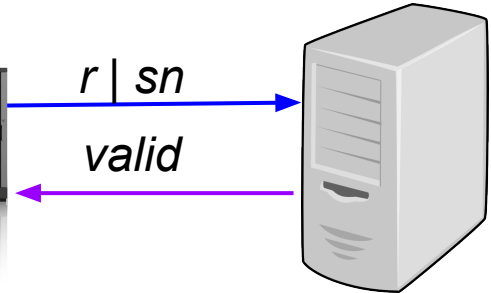
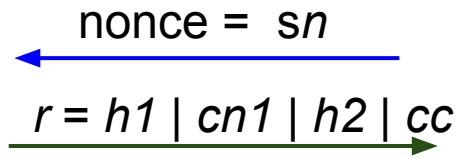
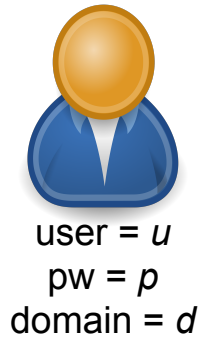


SMB Network

The user connects to a host using TCP through port 445 (SMB runs on port 445)

The server initiates the authentication process (Challenge/Response)

Challenge/Response Authentication



Security Account
Manager
(SAM)

SAM will calculate $h1$ and $h2$ based on $cn1$, cc , and sn
if $h1 == SAM-h1$ && $h2 == SAM-h2$ then valid == TRUE

create 2 client nonces = $cn1$, $cn2$ **MD5**

$cc = (time, cn2, d)$

$x = \text{HMAC-MD5}(\text{MD4}(p), u, d)$

$h1 = \text{HMAC-MD5}(x, sn, cn1)$

$h2 = \text{HMAC-MD5}(x, sn, cc)$

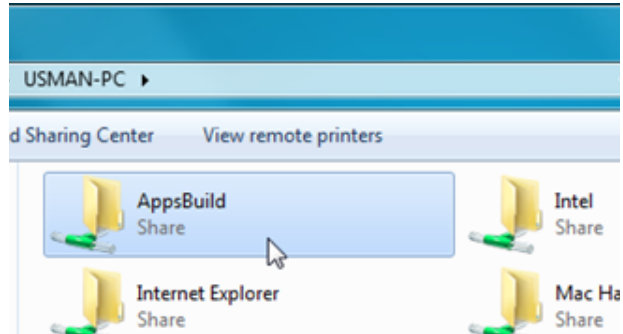
A cryptographic hashing algorithm

HMAC (Hashed-based Message Authentication Code)

A secure way to hash values that need to be verified

Null Session Attack

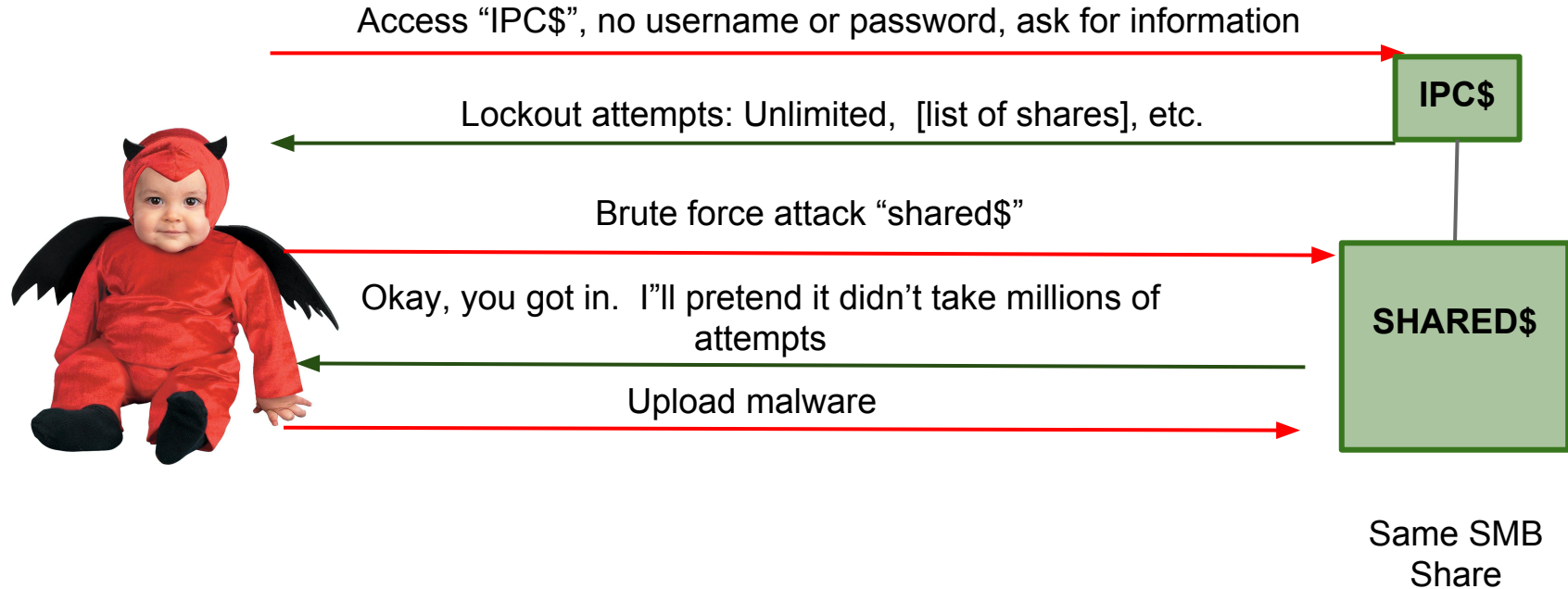
- SMB Shares



















```
Administrator: C:\Windows\system32\cmd.exe
C:\sec>enum -P 172.16.16.131
server: 172.16.16.131
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
cleaning up... success.
```

- Users have access to shares
 - Some shares are hidden (append a "\$")
- SYSTEM processes can gain access to "IPC\$"
 - No need for username or password
 - Called a Null Session
- Can enumerate usernames, shares and password requirements in a null session
- Learning this information makes brute force attacks easier

So how you can you exploit this?



Listening Implant / Backdoor

 SPI Employees Levels_401(k) sort _passwordv2.xls	Oct 16, 2014, 7:51 PM	62 KB	Micros...ksheet
 SPIRIT_Password_History_16.xls	Oct 16, 2014, 7:48 PM	28 KB	Micros...ksheet
 sppbwa02 user.txt	Oct 16, 2014, 7:04 PM	19 KB	text
 SSL Certs on Windows Servers.xlsx	Oct 16, 2014, 6:59 PM	10 KB	Spreadsheet
 Starz_User Password Horizon_AfterGoLive_072407.xls	Oct 16, 2014, 6:16 PM	27 KB	Micros...ksheet
 Story Computer Passwords.doc	Oct 16, 2014, 7:35 PM	56 KB	Word
 Systems userids and passwords.xlsx	Oct 16, 2014, 7:54 PM	17 KB	Spreadsheet
 territoriespassword.xlsx	Oct 16, 2014, 6:21 PM	14 KB	Spreadsheet
 The Interview Budget Final 10_10_13.pdf	Oct 16, 2014, 8:21 PM	1.8 MB	PDF Document
 unix_servers May 2014 v2.xls	Oct 16, 2014, 7:24 PM	173 KB	Micros...ksheet
 Unlock ID and reset password 110-9-10_INC0113716.xlsx	Oct 16, 2014, 7:39 PM	9 KB	Spreadsheet
 UPS Login & Password.xls	Oct 16, 2014, 6:17 PM	14 KB	Micros...ksheet
 UserNames&Passwords.xls	Oct 16, 2014, 5:57 PM	16 KB	Micros...ksheet
 VARIANCE 061414 .pdf	Oct 16, 2014, 8:20 PM	93 KB	PDF Document
 website passwords.xls	Oct 16, 2014, 6:39 PM	14 KB	Micros...ksheet
 YouTube login passwords.xlsx	Oct 16, 2014, 6:18 PM	18 KB	Spreadsheet

Propagation of Wiping Tool



Initial infection with SMB Worm



Accessed Network shares using hardcoded IP addresses, usernames, and passwords



Hardcoded IP address



Received destructive malware from infected computer – access any available network shares and delete files



Possess shares with infected computers



Had network shares with infected computer – shared files deleted

Destruction of Files

Wipes all files in the local disk except Program Files or Windows folder

Eldos Software RawDisk kernel driver

- overrides Windows OS to grant raw disk access
- uses this to overwrite the MBR

Wipes any files it can access through remote shares

Displays the ransom message

Puts computer to sleep for two hours, after which it reboots with new MBR

- Finishes wiping any files it couldn't get while Windows was running

Sony hack prompts Congress, White House to back cyber bills

Published time: January 14, 2015 18:07

Edited time: January 14, 2015 19:07



White House just endorsed CISPA measures, two years after veto threat

Lawmaker Reintroduces CISPA “Cybersecurity” Bill

CISPA encourages Internet companies to share your private data with the feds



Kit Daniels

Prison Planet.com

January 14, 2015

The Cyber Intelligence Sharing and Protection Act (CISPA), which encourages Internet companies to share your private data with the government under the guise of “cybersecurity,” was [reintroduced to Congress](#) by Rep. Dutch Ruppersberger (D-Md.)

...s hacks and cyberattacks, the U.S. government now supports
...t indemnifies tech companies from sharing private user data.

...for Between the Lines | January 13, 2015 -- 21:18 GMT (13:18 PST)

...ttaker 9,917 followers

[Get the ZDNet Security newsletter now](#)

Reuters



Two of the
Congress
cyber thr
emerging



CISPA - HR 234 (previously HR 634 (previously HR 3523))

- Reintroduced to the House January 8, 2015
- Criticized for vague wording which could allow
 - Aggressive countermeasures (hack backs)
 - Providing customer's personal data to third parties
 - private companies authorized to send PII
 - Lack of transparency
- Government would be able to hold information with very little reason
- Companies cannot be held liable if "acting in good faith"
- Overrules all previous legislation

"CISPA 2015 would provide for an even cozier relationship between Silicon Valley and the US government at the detriment of civil liberties and privacy for everyone else." -Rachael Tackett

What does this mean?

- No explicit security requirements enforced
- If a company feels threatened it can use hack backs
 - Example: breaking into computers to retrieve stolen information
- Government needs no warrants, has no limits or oversight
- Companies immune to lawsuits for sharing information
- Network traffic could be restricted

Things We Did Not Cover (and you might want to)

- Who perpetrated the attack

- The real details (we speculated)

Questions?



References for Malware

McAfee's Description: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25630/en_US/McAfee_Labs_Threat_Advisory_Trojan-Wiper.pdf

US-CERT's Description: <https://www.us-cert.gov/ncas/alerts/TA14-353A>

Eldos: <https://www.eldos.com/rawdisk/>

Description of a possible SMB attack: <http://www.sans.org/security-resources/malwarefaq/bh01.php>

Sources for Timeline & CISPA

<http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/>

<https://www.eff.org/cybersecurity-bill-faq>

<https://www.congress.gov/bill/114th-congress/house-bill/234/text>

<http://rt.com/usa/222695-sony-hack-cfaa-cispa/>

<http://www.prisonplanet.com/lawmaker-reintroduces-cispa-cybersecurity-bill.html>

http://www.huffingtonpost.com/2014/12/24/facebook-lawsuit_n_6378076.html

Sources for SMB

SMB Exchange - [https://msdn.microsoft.com/en-us/library/windows/desktop/aa365236\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa365236(v=vs.85).aspx)

SMB Eryption - http://en.wikipedia.org/wiki/NT_LAN_Manager

Passwords in the clear - http://gawker.com/sonys-top-secret-password-lists-have-names-like-master_-1666775151

Null Session Attack - http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Anatomy-Nul-Attack.html

Sony passwords in plaintext - http://gawker.com/sonys-top-secret-password-lists-have-names-like-master_-1666775151