

(S\$\$)

ixia



Hexcellents

Session 0x01 Exploration Tools

Security Summer School

ACS/Ixia/Hexcellents

Motivation



- Why do we need security?
- What could possibly go wrong?
- What's the worse that could happen?

Security against Whom?

Security against Whom?

- neighbors that sniff your Wi-Fi

Security against Whom?

- neighbors that sniff your Wi-Fi
- script kiddies that try to bruteforce your SSH login

Security against Whom?

- neighbors that sniff your Wi-Fi
- script kiddies that try to bruteforce your SSH login
- disgruntled employees that know your network topology and all running services (and the ones that are not updated)

Security against Whom?

- neighbors that sniff your Wi-Fi
- script kiddies that try to bruteforce your SSH login
- disgruntled employees that know your network topology and all running services (and the ones that are not updated)
- nation state actors that have exploits to undisclosed vulnerabilities in software you use

Security against Whom?

- neighbors that sniff your Wi-Fi
- script kiddies that try to bruteforce your SSH login
- disgruntled employees that know your network topology and all running services (and the ones that are not updated)
- nation state actors that have exploits to undisclosed vulnerabilities in software you use
- agencies that use quantum computers to break encryption

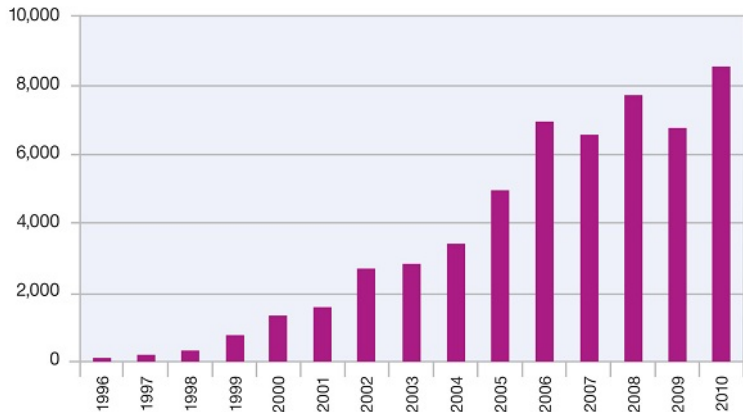
Security against Whom?

- neighbors that sniff your Wi-Fi
- script kiddies that try to bruteforce your SSH login
- disgruntled employees that know your network topology and all running services (and the ones that are not updated)
- nation state actors that have exploits to undisclosed vulnerabilities in software you use
- agencies that use quantum computers to break encryption

Vulnerabilities on the Rise

Vulnerability Disclosures Growth by Year

1996-2010

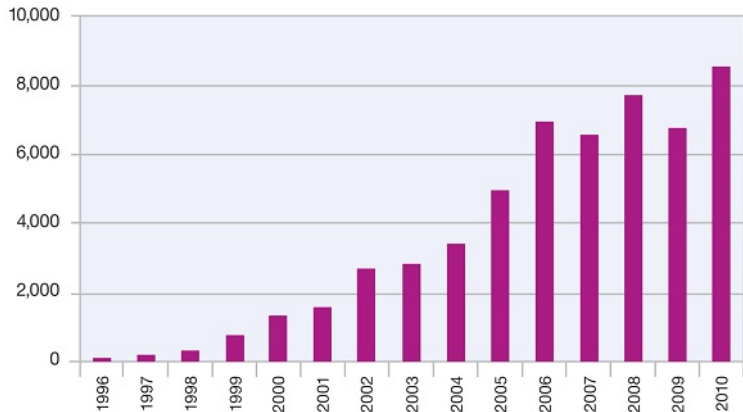


Source: IBM X-Force®

Vulnerabilities on the Rise

Vulnerability Disclosures Growth by Year

1996-2010




















Source: IBM X-Force®

Security should be of paramount importance but we aren't getting safer. 4 / 23

The Good

- companies have started realizing how important security is
- these now offer bug bounty programs
- yearly contests award researchers money for exploits in common software
- hackers can try out their skills legally and make \$\$\$\$

 InVision 90 Bugs closed \$100 Minimum bounty	 Flash IBB 7 Bugs closed \$2,000 Minimum bounty	 Secret 24 Bugs closed
 Yahoo! 849 Bugs closed \$50 Minimum bounty	 Sandbox Escape IBB 2 Bugs closed \$5,000 Minimum bounty	 The Internet IBB 3 Bugs closed \$5,000 Minimum bounty
 Phabricator IBB 12 Bugs closed \$300 Minimum bounty	 Ruby on Rails IBB 1 Bug closed \$1,500 Minimum bounty	 Ruby IBB 1 Bug closed \$1,500 Minimum bounty
 Python IBB 2 Bugs closed \$1,500 Minimum bounty	 Django IBB 0 Bugs closed \$250 Minimum bounty	 Nginx IBB 2 Bugs closed \$500 Minimum bounty
 OpenSSL IBB 1 Bug closed \$2,500 Minimum bounty	 PHP IBB 2 Bugs closed \$1,500 Minimum bounty	 Perl IBB 0 Bugs closed \$1,500 Minimum bounty
 Apache httpd IBB 0 Bugs closed \$500 Minimum bounty	 HackerOne 40 Bugs closed \$100 Minimum bounty	

Show off your security skills: announcing Pwnium 4 targeting Chrome OS

Thursday, January 23, 2014

Security is a [core tenet](#) of Chromium, which is why we hold [regular competitions](#) to learn from security researchers. Contests like Pwnium help us make Chromium even more secure. This year Pwnium 4 will once again set sights on Chrome OS, and will be hosted in March at the [CanSecWest](#) security conference in Vancouver.

With a total of \$2.71828 million USD in the pot ([mathematical constant e](#) for the geeks at heart), we'll issue Pwnium rewards for eligible Chrome OS exploits at the following levels:

- \$110,000 USD: browser or system-level compromise in guest mode or as a logged-in user, delivered via a web page.
- \$150,000 USD: compromise with device persistence: guest to guest with interim reboot, delivered via a web page.

Source: [2]

The Bad

- malware
- ransomware

The Ugly

- security is now part of warfare
- stuxnet was the first to be termed a cyberweapon
- based on four 0-day vulnerabilities

0-day Market

————— A six-figure price for a single hacking technique may sound extravagant, but it's hardly unique. Based on speaking with sources in this secretive but legal trade, I've assembled a rough price list for zero-day exploits below.

ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

Source: [5]

0-day Market

Vulnerability/Exploit	Value	Source
"Some exploits"	\$200,000 - \$250,000	A government official referring to what "some people" pay [9]
a "real good" exploit	over \$100,000	Official from SNOsoft research team [10]
Vista exploit	\$50,000	Raimund Genes, Trend Micro [8]
"Weaponized exploit"	\$20,000-\$30,000	David Maynor, SecureWorks [11]

Source: [6]

Where to Start?

- “To know your Enemy, you must become your Enemy.” - Sun Tzu
- to be able to secure first learn how to attack

What About?

- make first steps into the security world
- focus on binary analysis and exploiting, i.e. runtime application security
- make it practical, CTF-like
- strong collaboration with Ixia
- social, prizes
- Have fun and happy hacking!

- 32 participants, 2 rooms
- improve content
- as always, support from Ixia/Keysight, huge thanks!

Schedule

- 1 18-Jun-2018: 0x01. Exploration Tools
- 2 19-Jun-2018: 0x02. Assembly Language
- 3 21-Jun-2018: 0x03. Executable File Formats
- 4 25-Jun-2018: 0x04. Static Analysis
- 5 26-Jun-2018: 0x05. Dynamic Analysis
- 6 28-Jun-2018: 0x06. Buffer Management
- 7 30-Jun-2018: Mid CTF
- 8 2-Jul-2018: 0x07. Shellcodes
- 9 3-Jul-2018: 0x08. Shellcodes (part 2)
- 10 5-Jul-2018: 0x09. Defense Mechanisms
- 11 9-Jul-2018: 0x0A. Information Leaks
- 12 12-Jul-2018: 0x0B. Return Oriented Programming
- 13 16-Jul-2018: 0x0C. Return Oriented Programming (part 2)
- 14 19-Jul-2018: 0x0D. Ixia Talks
- 15 21-Jul-2018: Final CTF
- 16 22-Jul-2018: Graduation Party

Exploration Tools

- static vs dynamic
- GUI vs CLI
- interactive vs automated
- goals: understanding, debugging, hacking/cracking, evaluation

Static Exploration

- forensics: look for data
- listing symbols, strings, links
- disassembling, decompiling
- unpacking, reversing

Static Exploration Tools

- file management: file, ls, stat, locate, grep
- file inspection: cat, xxd, hexdump, strings
- executable file inspection: readelf, nm, ldd
- disassembling: objdump, radare2, IDA
- binary rewriting/patching: hexedit, bless

Dynamic Exploration

- loader, dynamic linker, libraries
- files, sockets, shared memory
- network communication
- standard file descriptors
- system & library calls
- address space
- runtime environment

Dynamic Exploration Tools

- resources: pmap, lsof, ps, sysstat
- debugging: GDB
- tracing: strace, ltrace, ftrace (kernel level), DTrace (Sun, BSD, macOS)

Network Exploration Tools

- get info: nmap, netstat
- traffic inspection: tcpdump, Wireshark
- universal: netcat (swiss army knife)
- exploit: nessus, hydra, aircrack
- <http://sectools.org/>

Demos

- using ldd to show dynamic dependencies
- using strings to get strings
- using strings and show address/offset
- inspecting using strace and ltrace
 - show only certain calls
 - follow children
 - increase default string length
 - trace running process; trace running shell
- show strace vs ltrace: printf/write, malloc/brk
- create a server and a client using nc locally: TCP and UDP

Resources

- 1 hackerone.com
- 2 <http://sectools.org/>
- 3 blog.chromium.org/2014/01/show-off-your-security-skills.html
- 4 ehackingnews.com/2014/01/php-cgi-remote-code-execution.html
- 5 secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware
- 6 forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-expl
- 7 securityevaluators.com/knowledge/papers/0daymarket.pdf
- 8 www.zerodayinitiative.com
- 9 www.disclose.tv/action/viewvideo/157242/BBC_Horizon__Defeating_the_Hackers_HD