Feeling Vulnerable?

Jamie S. Herman, C|CISO, CISM, CISSP
Balazs Bucsay, OSCE, OSCP, GIAC, GPEN
A Little About Us...

Balazs Bucsay

- Hungarian Hacker
- 14 years of experience in IT-Security
- Strictly technical certificates: OSCE, OSCP, GIAC GPEN
- Currently working for world’s second largest mobile company (Vodafone)
A Little About Us…

Jamie Herman

- Manager of Information Security (Ropes & Gray LLP)
- 15 years of IT, information security and risk mgmt. experience
- BS Computer & Digital Forensics
- Certified C|CISO, CISM, CISSP
Enterprise Risk Management

- Information security is a risk management exercise conducted across all business units and technologies.

- The security conversation needs to be engrained in the early stages of a project/process lifecycle, not after it’s in progress.
SANS Institute Critical Security Controls 1 through 4:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
Understand Your Risk

Technical concerns:
- Identify key areas of internal and external access
- Outdated systems rarely updated
- Shadow IT systems
- Network peripherals
- Telecom equipment
- Elevated accounts (user, service, domain admin)
- Sensitive data
- Out of date software (big challenge for law firms)
Understand Your Risk

**Administrative/Process Concerns:**

- Business behavior (data and account use)
- Business system owners thought process
- Project workflow
- Vendor selection
- IT behavior
  - Patching/software updating
  - Software installations
  - Vulnerability remediation SLA’s
Vulnerability Management Challenges

- Keeping software current due to compatibility and integration issues
- Microsoft patches (#$%^) historically create business visible problems
- Resource intensive to patch and update Java, Flash, Acrobat, etc. frequently
- Selling value of remediation vs. project deliverables
- Understand CVE and details around vulnerability
- Change Management (office openings, changes, etc.)
The Great Debate

Authenticated or Unauthenticated scans against devices on your network?

Authenticated:
- Fewer vulnerability false positives
- Less intrusive on the devices

Unauthenticated
- “See what attackers see” mentality
- Security team doesn’t need admin credentials
Scanners

- Free
  - OpenVAS

- Other Tools
  - Nexpose
  - Nessus
  - QualysGuard
  - GFILanGuard
  - Tripwire
  - SAINITscanner
  - Lumension
Hands on

- Real hacking demo
- More practical
- No deep knowledge needed!
- We will just scratch the surface, it will be easy to understand
- But first some explanation
Secure Sockets Layer (SSL)

- It is like a gift, you need to wrap it to hide the content
- You are wrapping the traffic with strong encryption
- The content will be unreadable for third parties
- This is secure in certain circumstances
Journey of the message

plaintext → encryption → Coded Hex Text → decryption → plaintext
Heartbleed

- One of the modules of SSL is called Heartbeat.
- Heartbeat can check whether the service is alive or not.
- Part of that implementation was vulnerable.
- It was possible to read the decrypted data from memory.
Heartbleed explained / XKCD

**HOW THE HEARTBLEED BUG WORKS:**

Server, are you still there? If so, reply "POTATO" (6 letters).

User Meg wants these 6 letters: POTATO.

User Ida wants pages about "irl games". Unlocking secure records with master key 5130985733435 makes "cheese and beer sends this message: "

15
Heartbleed explained / XKCD
Heartbleed explained / XKCD

SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).

User Olivia from London wants pages about "how bees in car why". Note: Files for IP 375.381.383.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 347 connections open. User Brendan uploaded the file self-file.jpg (contents: 334b:962c:0b9ff89b43b4f89).
Heartbleed explained / XKCD

User Olivia from London wants pages about "mat bees in car why". Note: Files for IP 375.381.383.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 345 connections open. User Brendan uploaded the file self.jpg (contents: 034b962c28f2f0f0b3b6f8f).

HMM...
Heartbleed explained / XKCD

Server, are you still there? If so, reply "HAT" (500 letters).

User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to change account password to "CoffeeBag". User
Heartbleed explained / XKCD

User Meg wants these 500 letters: HAT.
Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534".
Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoRaC". User wants picture of user.
SYSTEM user

- On Windows the highest privileged user is SYSTEM
- More powerful than Administrators
- It has access to everything (files, memory, etc.)
- This user can even destroy the whole operating system, install backdoors, key loggers without any trace
mimikatz

- One of my favourite tools
- Capable to do lots of different things, for example dumping passwords
- In certain circumstances it can get the cleartext password as well
- SYSTEM privilege is needed!
DEMO

HACKER CAT

is hacking u
Vulnerabilities

- Obsolete and vulnerable OpenSSL version was installed
- Obsolete and vulnerable webserver version was installed
- Vulnerable Webmail was used - Business logic flaw
- Webserver was running as SYSTEM - Configuration flaw
Scanner vs. Vulnerabilities

- Heartbleed vulnerability can be found by a scanner
- Webmail vulnerability possibly can be found by a scanner
- Configuration errors most probably cannot be found by a scanner
Hackers vs. Vulnerabilities

- Heartbleed vulnerability will be found by a hacker
- Webmail vulnerability will be found by a hacker
- Configuration errors will be exploited by a hacker
Fixes

- Upgrading OpenSSL and webserver to the newest one
- Use a proper webmail client (for example: Outlook Web App)
- Rethink the configurations, use the lowest privileged user for everything
Vulnerability scans

- Up-to-date vulnerability scanners are must haves nowadays
- Scanners can find massive volume of vulnerabilities in shorter time
- Restless, but possible false positives
- Relatively cheap
Penetration tests/Ethical Hacking

- Done by experienced ethical hackers
- They can find and exploit the most critical bugs on the network
- Simulating real life
- Less vulnerabilities, but more criticals and no false positives!
- More expensive
Takeaways

- Try a free scanner!!!
- Ensure you are capturing all IP’s on network
- Consider multiple scanners to balance network load
- Document network for asset class segmentation
- Don’t try to digest all information at once
- Be careful with firewalls, VC equipment, print devices, etc.
- Prioritize and don’t get data overloaded
Distrust and caution are the parents of security
- Benjamin Franklin