The Development of a Virtual Environment for Teaching Cybersecurity

Graduate Student: Carlos Y. Velez

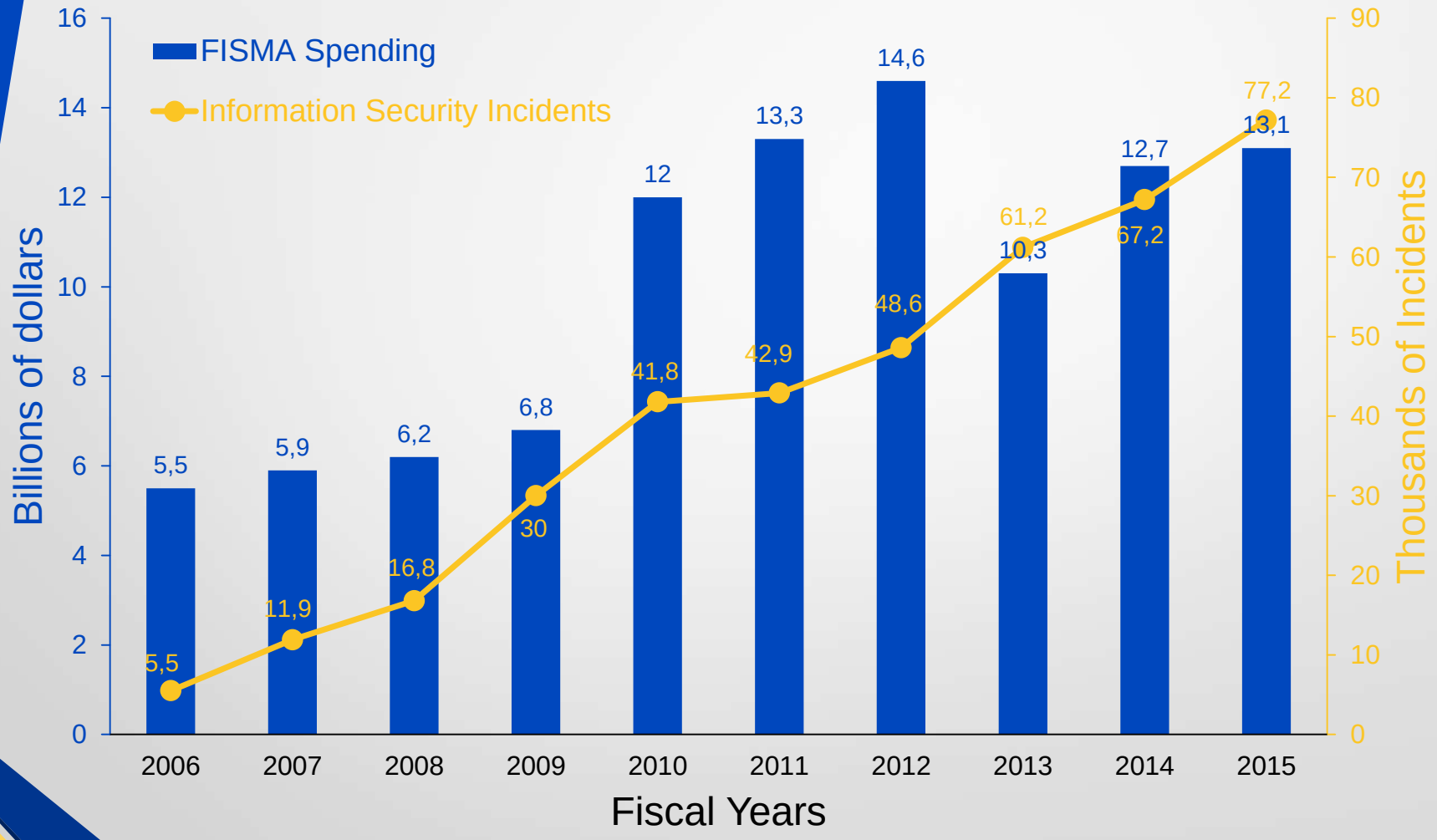
Advisor: Dr. Alfredo Cruz

UNIVERSIDAD POLITÉCNICA PUERTO RICO

Outline

1. Justification
2. Research
3. Lab Explanation
4. Conclusion

Federal cybersecurity spending and total federal information security incidents

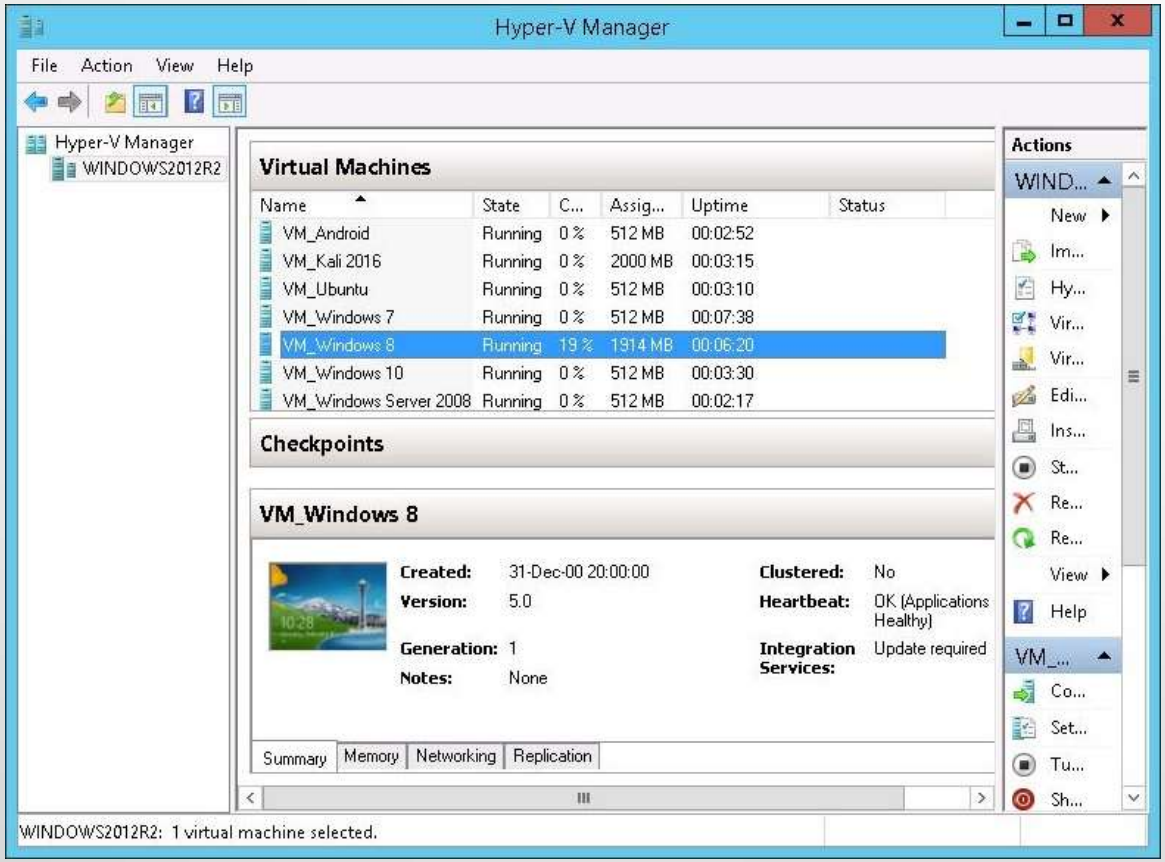


https://fas.org/sgp/crs/misc/R43831.pdf, http://www.gao.gov/assets/680/679877.pdf

Virtual Environment

- Physical servers with virtual machines
- Docker Containers with lab instances
- Outsourced services like GoDaddy, Amazon, Skytap

Virtual Environment (cont'd)



Physical server with multiple VMs

Laboratories

1. Commands for Linux and Windows
2. Footprinting
3. Scanning and Enumeration
4. Encryption
5. Password Cracking
6. Web Server Vulnerabilities

Lab 1 Commands for Linux and Windows

- A review of commands for both operating systems
- Concentrate in folder navigation, file and folder creation, deletion and naming
- Network debugging, identification of the computer's IP address, DNS and the trace route in both Linux and Windows systems.
- Ftp, Telnet and SSH connections

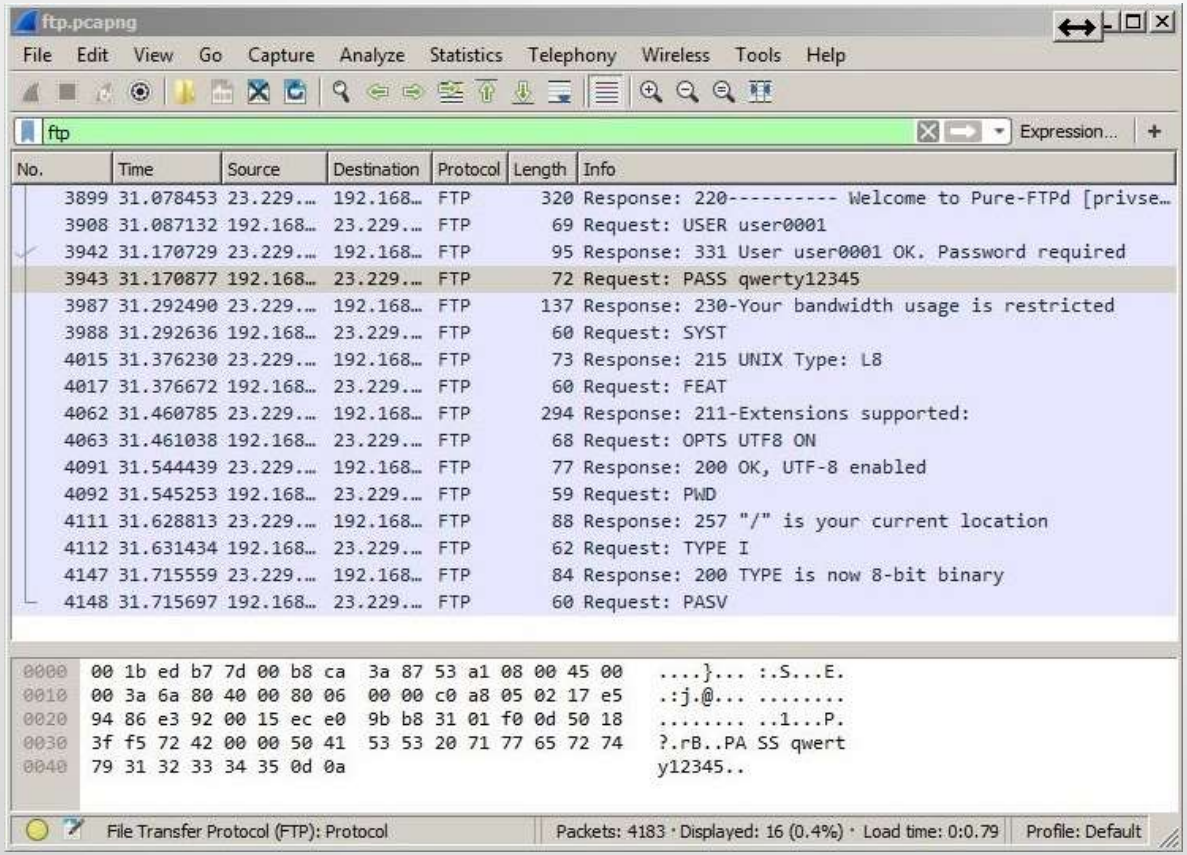
Lab 2 Footprinting

- **Firebug** to debug CSS, HTML and JavaScript to extract server name, version and framework.
- **Web Data Extractor** to scrap links, meta tags, phone numbers, emails, etc.
- **Path Analyzer Pro** to obtain trace routes, DNS and other routing information and registries from websites that are not well configured.

Lab 3 Scanning and Enumeration

- **Wireshark packet analyzer** to monitor data traffic within the network.
- **Nmap** scans on both Windows and Linux machines to see open ports and identify operating systems in the network.
- Types of scans Xmas Scans, ACK Flag Scans, UDP Scans, and IDLE Scans.

Lab 3 Scanning and Enumeration (cont'd)



Wireshark showing ftp traffic

Lab 4 Encryption

- Students will learn basic encryption processes like Caesar, Vigenére and Playfair ciphers.
- **Quick Checksum Verifier** and **HashCalc** tools. On Windows machines they will generate a checksum calculation of a given file, while on Linux they will use built-in commands.
- Encrypting and decrypting tools that will be used include **CryptoForge** and **CrypTool**.
- Usage of a web application that shows Fletcher, RC4, DES, and AES step by step checksum and encryption algorithms.

Lab 4 Encryption (cont'd)

Ciphertext:

IG RP GR AQ CY RE BX NO DR UC

Key:

CYBER

C	Y	B	E	R
A	D	F	G	H
I/J	K	L	M	N
O	P	Q	S	T
U	V	W	X	Z

Plaintext:

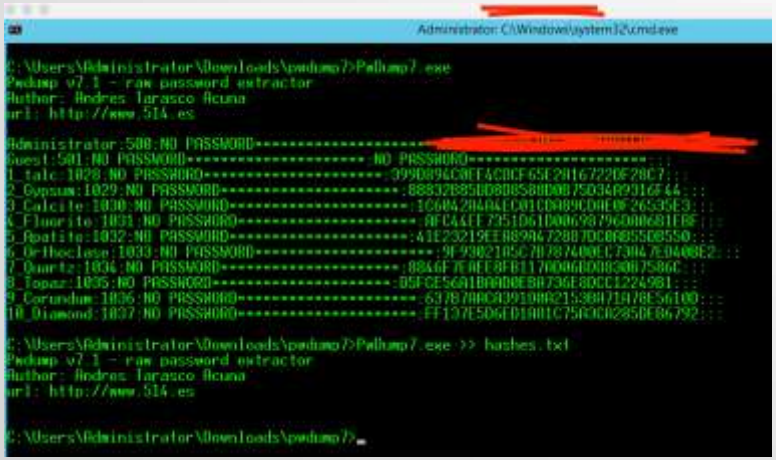
MAYTHEFORCEBEWITHYOU

Playfair decryption process

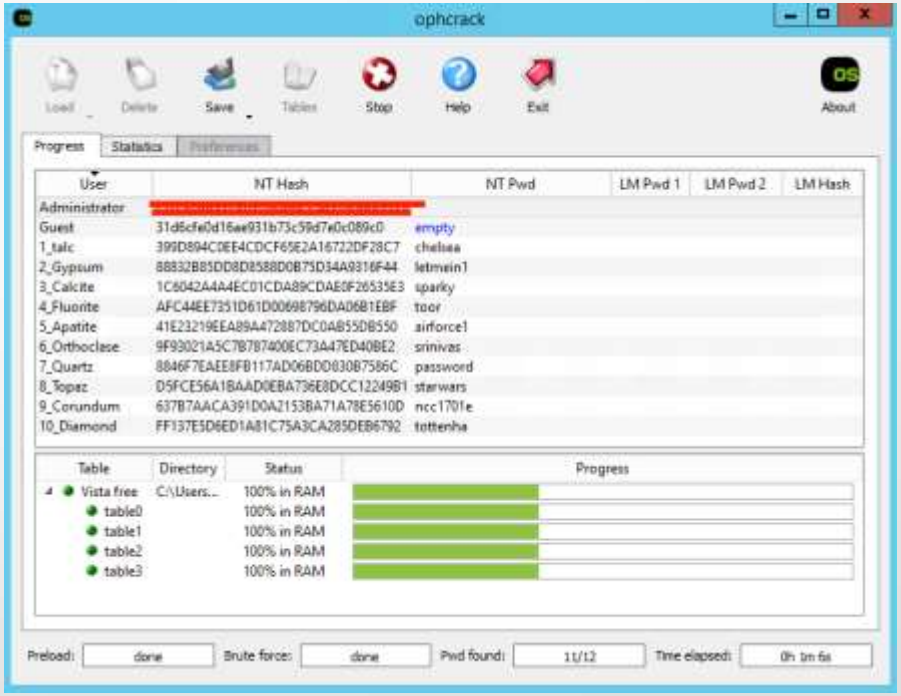
Lab 5 Password Cracking

- This lab teaches how the **pwdump7** tool extracts the SAM File on a Windows Machine.
- The use of the **ophcrack** tool with the addition of a rainbow table.
- Crack the passwords for the hashes provided in the SAM file.

Lab 5 Password Cracking (cont'd)



PwDump7 extracting the SAM file



ophcrack calculating possible passwords

Lab 6 Web Server Vulnerabilities

- This lab covers the use of **Metasploit**, **Meterpreter** and **Wpscan**
- Search for Vulnerabilities/Exploits
- Select payload/host
- Gain access

Conclusion

- Help entry level students understand cybersecurity in general.
- Promoted the use of tools and problem solving techniques.
- Foundation to more advanced classes.

Questions?

UNIVERSIDAD POLITÉCNICA
PUERTO RICO