

The Development of a Virtual Environment for Teaching Cybersecurity

Graduate Student: Carlos Y. Velez

Advisor: Dr. Alfredo Cruz

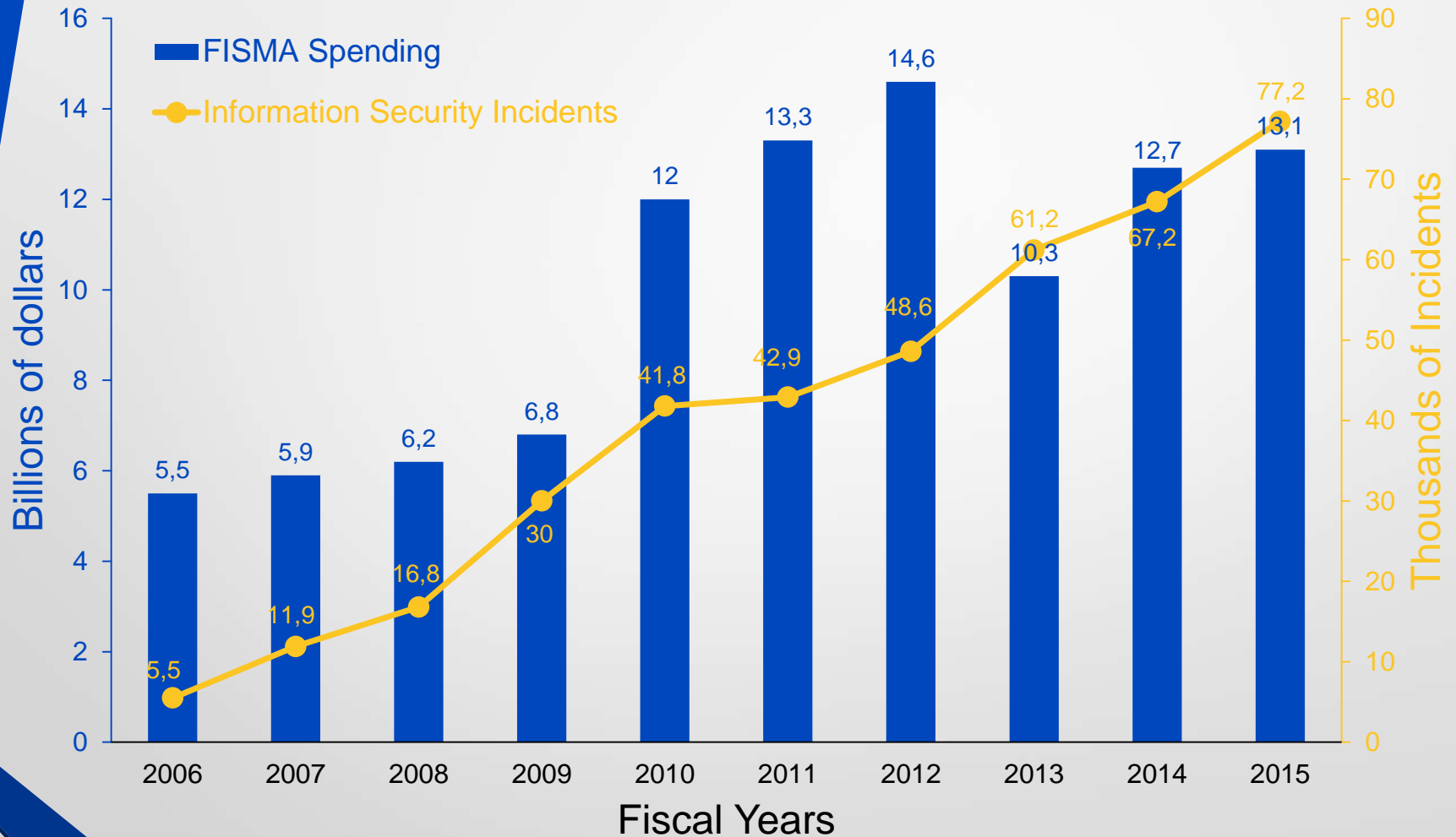


Outline

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



Federal cybersecurity spending and total federal information security incidents



Virtual Environment

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



Virtual Environment (cont'd)

The screenshot shows the Hyper-V Manager interface. The 'Virtual Machines' table lists several VMs, with 'VM_Windows 8' selected. Below the table, the 'Checkpoints' section is empty. The 'VM_Windows 8' details are shown, including a thumbnail image and various configuration parameters.

Name	State	C...	Assig...	Uptime	Status
VM_Android	Running	0 %	512 MB	00:02:52	
VM_Kali 2016	Running	0 %	2000 MB	00:03:15	
VM_Ubuntu	Running	0 %	512 MB	00:03:10	
VM_Windows 7	Running	0 %	512 MB	00:07:38	
VM_Windows 8	Running	19 %	1914 MB	00:06:20	
VM_Windows 10	Running	0 %	512 MB	00:03:30	
VM_Windows Server 2008	Running	0 %	512 MB	00:02:17	

VM_Windows 8

Created: 31-Dec-00 20:00:00 **Clustered:** No
Version: 5.0 **Heartbeat:** OK (Applications Healthy)
Generation: 1 **Integration Services:** Update required
Notes: None

Summary | Memory | Networking | Replication

WINDOWS2012R2: 1 virtual machine selected.

Physical server with multiple VMs



UNIVERSIDAD
POLITÉCNICA
PUERTO RICO

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.

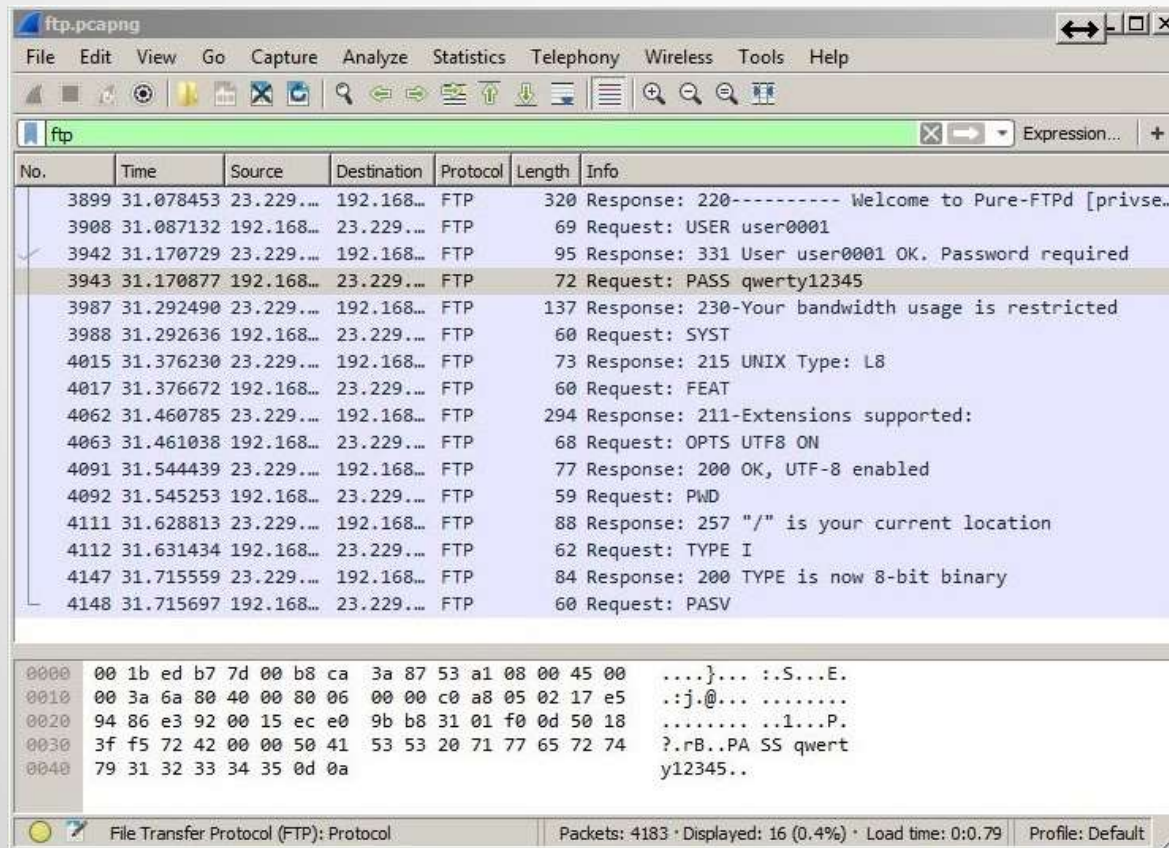


Lab 3 Scanning and Enumeration

- **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)



The image shows a Wireshark capture of FTP traffic. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 3943) is highlighted in yellow. Below the list, the packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII pane shows the FTP login sequence: '}.S...E.', 'j.@... ..', '.....1...P.', '?rB..PA SS qwerty12345..'. The status bar at the bottom indicates 'File Transfer Protocol (FTP): Protocol', 'Packets: 4183 · Displayed: 16 (0.4%) · Load time: 0:0.79', and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
3899	31.078453	23.229...	192.168...	FTP	320	Response: 220----- Welcome to Pure-FTPD [privse...
3908	31.087132	192.168...	23.229...	FTP	69	Request: USER user0001
3942	31.170729	23.229...	192.168...	FTP	95	Response: 331 User user0001 OK. Password required
3943	31.170877	192.168...	23.229...	FTP	72	Request: PASS qwerty12345
3987	31.292490	23.229...	192.168...	FTP	137	Response: 230-Your bandwidth usage is restricted
3988	31.292636	192.168...	23.229...	FTP	60	Request: SYST
4015	31.376230	23.229...	192.168...	FTP	73	Response: 215 UNIX Type: L8
4017	31.376672	192.168...	23.229...	FTP	60	Request: FEAT
4062	31.460785	23.229...	192.168...	FTP	294	Response: 211-Extensions supported:
4063	31.461038	192.168...	23.229...	FTP	68	Request: OPTS UTF8 ON
4091	31.544439	23.229...	192.168...	FTP	77	Response: 200 OK, UTF-8 enabled
4092	31.545253	192.168...	23.229...	FTP	59	Request: PWD
4111	31.628813	23.229...	192.168...	FTP	88	Response: 257 "/" is your current location
4112	31.631434	192.168...	23.229...	FTP	62	Request: TYPE I
4147	31.715559	23.229...	192.168...	FTP	84	Response: 200 TYPE is now 8-bit binary
4148	31.715697	192.168...	23.229...	FTP	60	Request: PASV

0000 00 1b ed b7 7d 00 b8 ca 3a 87 53 a1 08 00 45 00}... ..S...E.
0010 00 3a 6a 80 40 00 80 06 00 00 c0 a8 05 02 17 e5 ..j.@... ..
0020 94 86 e3 92 00 15 ec e0 9b b8 31 01 f0 0d 50 181...P.
0030 3f f5 72 42 00 00 50 41 53 53 20 71 77 65 72 74 ?.rB..PA SS qwert
0040 79 31 32 33 34 35 0d 0a y12345..

File Transfer Protocol (FTP): Protocol Packets: 4183 · Displayed: 16 (0.4%) · Load time: 0:0.79 Profile: Default

Wireshark showing ftp traffic



Lab 4 Encryption

- Students will learn basic encryption processes like Caesar, Vigenère 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
O	P	Q	S	T
U	V	W	X	Z

Plaintext:
MAYTHEFORCEBEWITHYOU

Playfair decryption process



UNIVERSIDAD
POLITÉCNICA
PUERTO RICO

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)

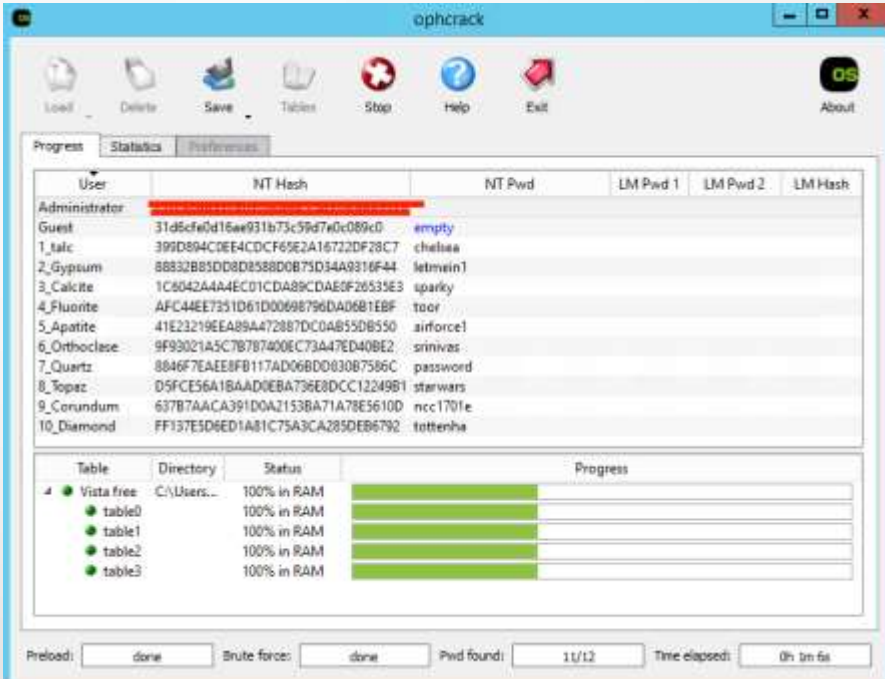
```
C:\Users\Administrator\Downloads\p0dhamo>Pallump7.exe
Pallump v7.1 - raw password extractor
Author: Andres Larasco ficuna
url: http://www.514.es

Administrator:500:NO PASSWORD-----NO PASSWORD-----
Guest:501:NO PASSWORD-----NO PASSWORD-----
1_talc:1028:NO PASSWORD-----399D894C0E14C0CF65E2A16722DF28C7...
2_Gypsum:1029:NO PASSWORD-----88832B85D08D8588D0B75D34A9316F44...
3_Calcite:1030:NO PASSWORD-----1C6042A4A4EC01CDA89CDAE0F26535E3...
4_Fluorite:1031:NO PASSWORD-----AFC44EE7251D61D00698796DAD0681EBF...
5_Apatite:1032:NO PASSWORD-----41E23219EE889472807DC68695D8550...
6_Orthoclase:1033:NO PASSWORD-----9F93021A5C7B787400EC73A47ED40BE2...
7_Quartz:1034:NO PASSWORD-----8846F7EAE8FB117AD06BD0030B7586C...
8_Topaz:1035:NO PASSWORD-----D5FCE56A1BAAD0EBA736E8DCC12249B1...
9_Corundum:1036:NO PASSWORD-----637B7AAAC391D0A2153BA71A78E5610D...
10_Diamond:1037:NO PASSWORD-----FF137E5D6ED1A81C75A3CA285DEB6792...

C:\Users\Administrator\Downloads\p0dhamo>Pallump7.exe >> hashes.txt
Pallump v7.1 - raw password extractor
Author: Andres Larasco ficuna
url: http://www.514.es

C:\Users\Administrator\Downloads\p0dhamo>
```

PwDump7 extracting the SAM file



The screenshot shows the ophcrack application interface. It features a menu bar with options: Load, Delete, Save, Tables, Stop, Help, Exit, and an About button. Below the menu is a progress bar and a statistics section. The main area displays a table of user accounts with their NT hashes, NT passwords, and LM hashes. A progress bar at the bottom indicates the status of the cracking process.

User	NT Hash	NT Pwd	LM Pwd 1	LM Pwd 2	LM Hash
Administrator	[REDACTED]				
Guest	31d5fe0d16e931b73c59d70c089c0	empty			
1_talc	399D894C0E14C0CF65E2A16722DF28C7	chelsea			
2_Gypsum	88832B85D08D8588D0B75D34A9316F44	letmein1			
3_Calcite	1C6042A4A4EC01CDA89CDAE0F26535E3	sparky			
4_Fluorite	AFC44EE7251D61D00698796DAD0681EBF	toor			
5_Apatite	41E23219EE889472807DC0A855D8550	airforce1			
6_Orthoclase	9F93021A5C7B787400EC73A47ED40BE2	srinivas			
7_Quartz	8846F7EAE8FB117AD06BD0030B7586C	password			
8_Topaz	D5FCE56A1BAAD0EBA736E8DCC12249B1	starwars			
9_Corundum	637B7AAAC391D0A2153BA71A78E5610D	ncc1701e			
10_Diamond	FF137E5D6ED1A81C75A3CA285DEB6792	tottenha			

Table	Directory	Status	Progress
Vista free	C:\Users\...	100% in RAM	[Progress Bar]
table0		100% in RAM	[Progress Bar]
table1		100% in RAM	[Progress Bar]
table2		100% in RAM	[Progress Bar]
table3		100% in RAM	[Progress Bar]

Preload: done Brute force: done Pwd found: 11/12 Time elapsed: 0h 0m 6s

ophcrack calculating possible passwords



UNIVERSIDAD
POLITÉCNICA
PUERTO RICO

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?

