

# SIGPwny @ UIUC

Spring 2017

“A computer lets you make more mistakes faster than any other invention with the possible exceptions of handguns and Tequila.” - Mitch Ratcliffe

# Announcements

- New members - welcome!
- Old members - welcome back!
- UIUCTF Planning underway
- Manticore focus group
- Thotcon
  - May 4 & 5
- Ciphercon Group Buy



# News Over Break



- US formally accuses Russia of DNC hacks



# News of the week

- [Root PrivEsc fixed in systemd](#)
- [Root PrivEsc discovered in GNU screen](#)
- [RCE in Cisco WebEx](#)
- [China announces crackdown on VPN usage](#)
- [Kaspersky employee arrested for treason](#)
- [Scare over WhatsApp implementation vuln](#)
- [Crypto experts call for Guardian retraction](#)
- [Symantec issues more illegitimate certs](#)
- [Brian Krebs declares war on Mirai author](#)
- [Telegram protocol flaw](#)
- [Bernie can still win](#)

# Chairs

- Alex
- Adam
- Bart
- J.P.
- Eric



# What is SIGPwny?

- Special Interest Group focusing on offensive cyber security
- We like
  - Exploitation
  - Reverse Engineering
  - Network Security
  - Cryptography
  - Physical security
  - Ponies

# Our Goals

- Generate interest and raise awareness in cyber security
- Develop hands-on skills
- SORF a pony
- Win CTFs and other cyber security events
- Get you a job!

# What You Should NOT Expect

- To become an expert in one semester
- To learn about every security topic in depth



# Background knowledge

- Only “requirement” is an interest in security
- Basic programming knowledge is useful
- These things will also help
  - Operating system internals
  - Networking
  - Assembly languages
  - Scripting
  - Web stuff

# What you'll need

- Laptop
- Linux VM
  - We recommend Kali or Ubuntu
- A desire to break things :)

# Topics

- Physical Security
  - Lockpicking
- Web
  - SQL Injection, XSS, Directory Traversal, CSRF, Authentication Bypass
- Reverse Engineering
  - IDA Pro, Debuggers, x86, MIPS, ARM, Bug hunting
- Exploitation
  - Buffer Overflows, Shellcoding, ROP, Use after free
- Malware
  - Reversing, Rootkits, Post exploitation, Evasion, Persistence
- Network security
  - Wireshark, Metasploit, Nmap, Pentesting, Cobalt Strike
- Hardware
  - Embedded devices, firmware extraction and modification, exploitation
- Crypto
- Mobile
- Puns

# Careers in Security

- Vulnerability Researcher
- Reverse Engineer
- Penetration Tester
- System Administrator
- Security Software Developer
- Forensics and Incident Responder

# Where SIGPwny people end up

- Trail of Bits
- Raytheon Si
- Air Force Research Lab
- Sandia National Lab
- MIT Lincoln Lab
- FireEye
- ViaSat
- OPS Solutions (Startup)
- NCC Group

# Communication

- UIUC SIGPwny
  - <https://www.facebook.com/groups/439995656109426/>
- Mailing List
  - <https://www-s.acm.illinois.edu/mailman/listinfo/sigpony-l>
- Website
  - <http://sigpwny.github.io/>
- IRC
  - #sigpwny irc.Freenode.net

# Meetings

- 5-7 pm, Thursdays
- Meetings include:
  - News of the Week
  - Recap of previous week
  - Mini tech talk
  - Lecture, demo, tutorial
  - Exercises and challenges

# Focus groups

- Pentesting/Network Exploitation Lab
- Exploits and Vulnerabilities Group
- Embedded Device Hacking
- CTF Practice
- Malware Analysis and Reversing
- Semester Project (TBD)
- Start your own!
  - Cloud/Software Defined Networking Security
  - VR on Scada, industrial controls.
  - ROP defense / UC Irvine



# Capture the Flag (CTF)

- “Capture the Flag”
- Security competition
  - Jeopardy Style
  - Attack and Defend
- CSAW Quals
- UIUCTF

# Useful Resources

- <https://trailofbits.github.io/ctf/>
- <https://exploit-exercises.com/>
- <http://opensecuritytraining.info/>
- <http://io.smashthestack.org/>
- <https://microcorruption.com/login>
- <http://overthewire.org/wargames/>
- <http://captf.com/>
- <https://www.nostarch.com/>
- [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)
- <http://mynameisq.us/login>
- <http://www.hackthissite.org>

# Social Events

- Real life Capture the Flag?
- Movie night?
  - black hat, mr robot, hackers, imitation game
- Barcrawl?
- LAN party? (Quake, unreal, tf2, warcraft 2, cs go, broodwar, )
- Tshirt???

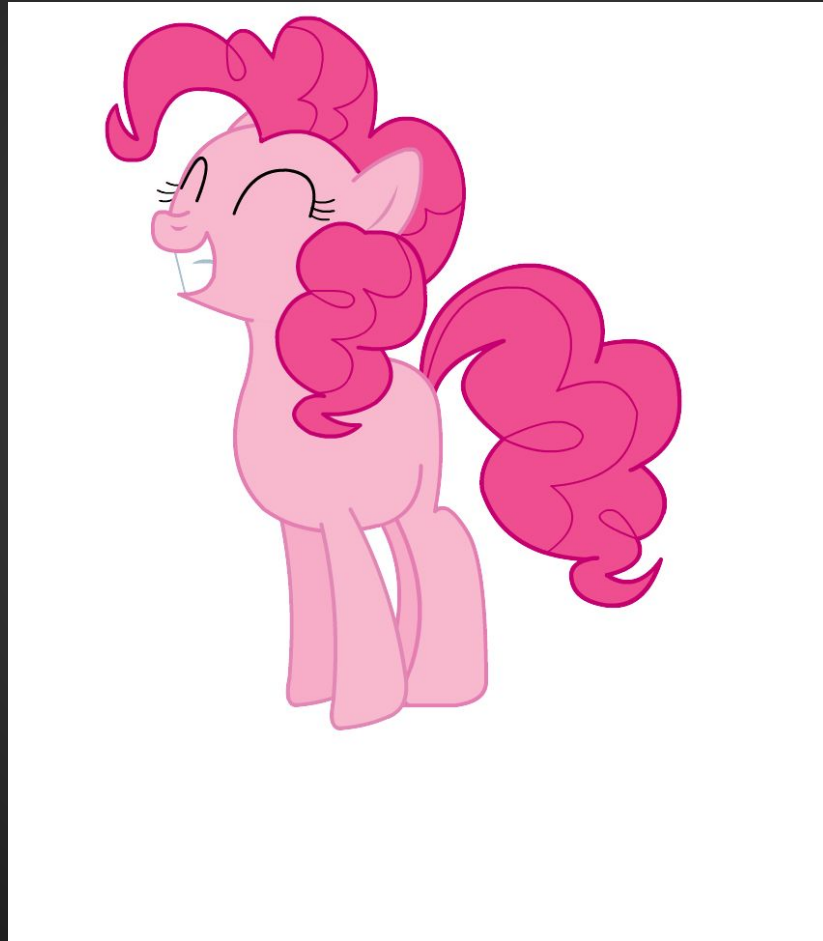
# Want more security news?

- Reddit
  - [/r/netsec](#)
  - [/r/reverseengineering](#)
  - [/r/malware](#)
  - [/r/crypto](#)
  - [/r/securityctf](#)
- [Google Project Zero, Online Security Blog](#)
- <http://www.darkreading.com/>
- <http://krebsonsecurity.com/>
- <https://www.schneier.com/>
- <http://www.zdnet.com/blog/security/>
- SANS
  - [Internet Storm Center](#)
  - [Mailing Lists](#) - @RISK and NewsBites
- [Hacker News](#)
- [Lobsters](#)
- [Full Disclosure](#)
- Twitter

# Security Classes at UIUC

- CS 460: Security Lab
  - Hands on security lab
- CS 461: Computer Security I
  - Security basics, lots of definitions
- CS 463: Computer Security II
  - More research-y security, emphasis on privacy and information
- Digital Forensics
  - Digital evidence, legal, file recovery

# Questions?

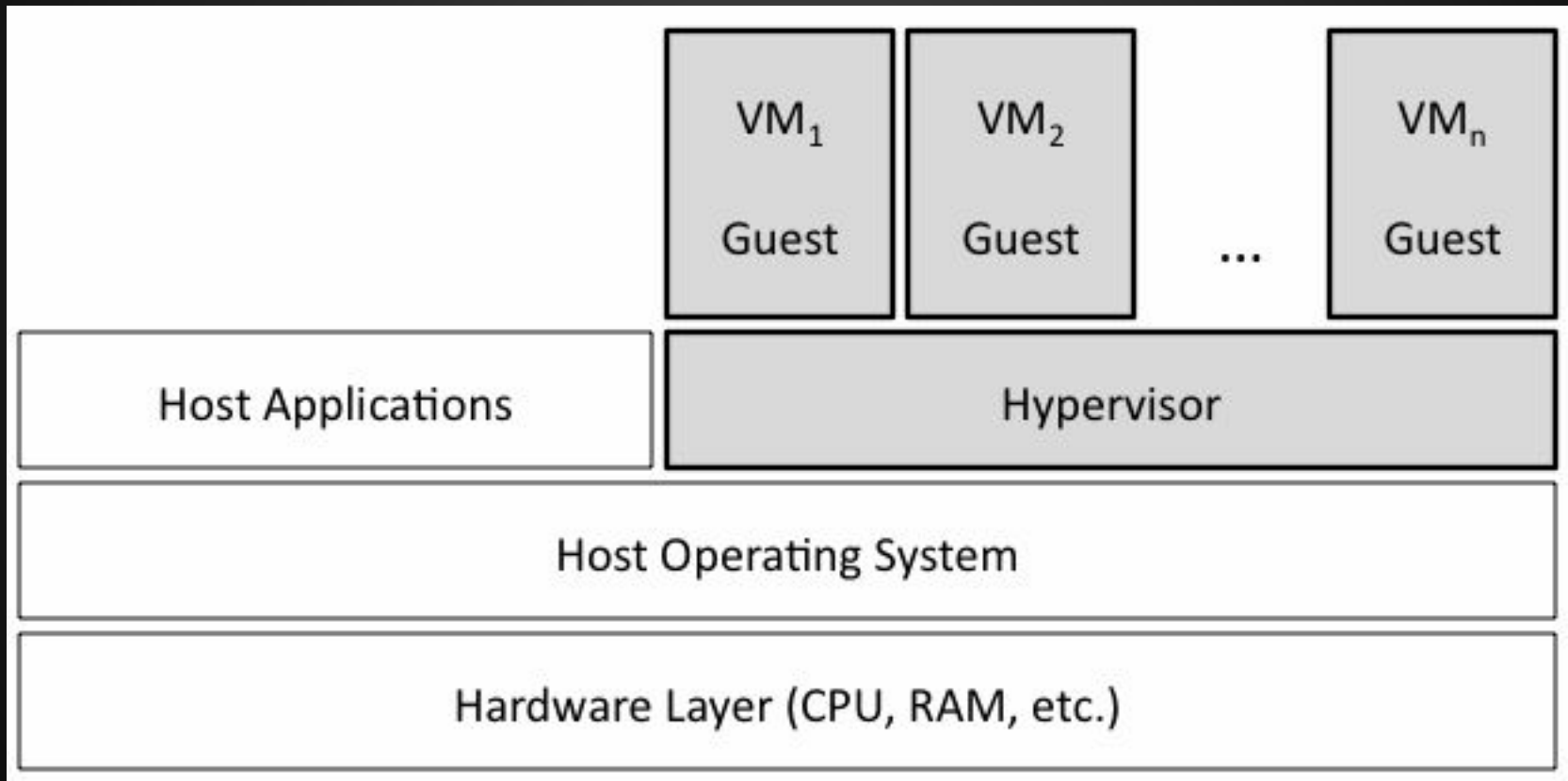


# Setting up a Virtual Machine

- Isolate guest OS from host OS
- Can use different OS's
- Snapshot and restore virtual machine state



# Setting up a Virtual Machine





# Setting up a Virtual Machine

- Windows, Linux, OS X
  - [VirtualBox](#)
  - [VMWare](#)
- OS X
  - Parallels
  - BootCamp
- Masochists
  - QEMU