SANS Slingshot distro

The most trusted source for information security training, certification, and research.

WHOAMI

HEAD OF CYBER SECURITY - NETSECURITY

CERTIFIED INSTRUCTOR - SANS

@chrisadale

GCIH GIAC Certified Incident Handler
GPEN GIAC Certified Penetration Tester
GSLC GIAC Security Leadership
GIAC Mobile Device Security Analyst
GDAT GIAC Defending Advanced Adversaries

Why another distribution?

- Lab and research
  - A place where you go to practice, develop, lab and research.
- Consistent
  - Work on what matters, rather than debug tools and environment.
- Familiar distribution
  - Tie a week of learning back to practice when you get home.

The focus

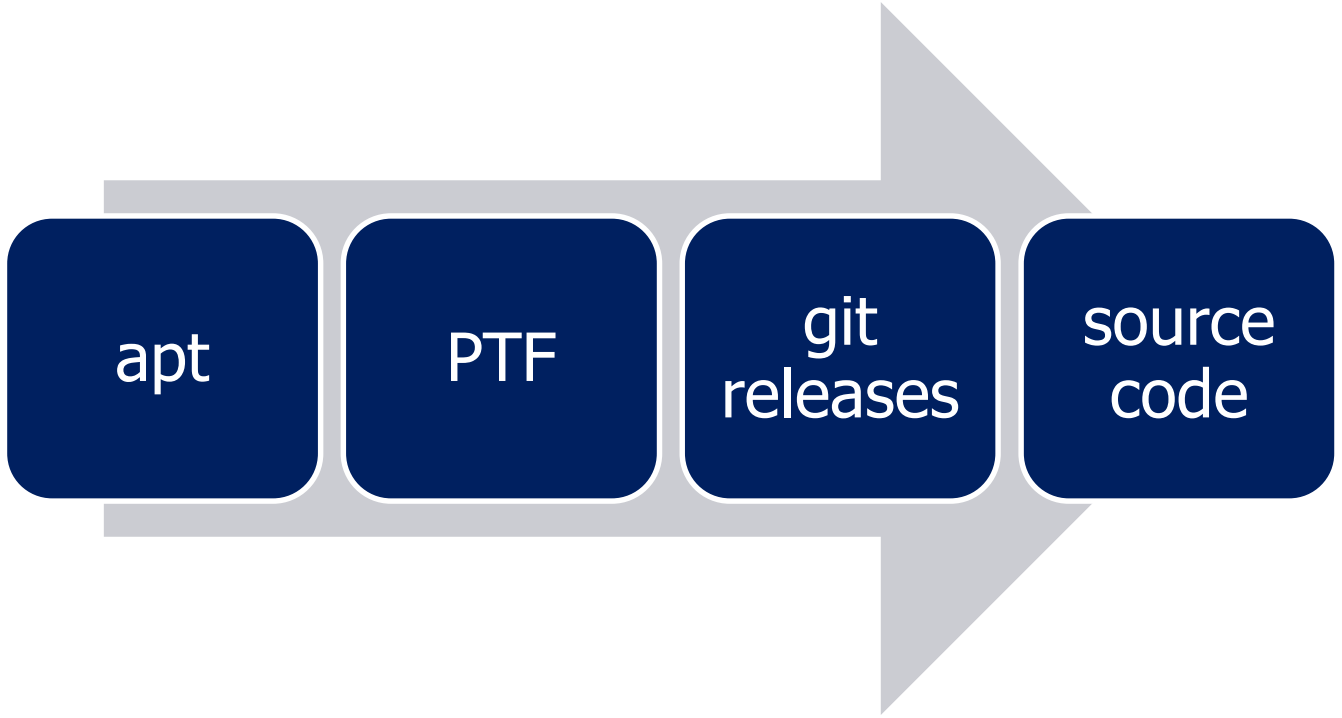
- Invested on reliability
- Updates and upgrades
  - Environment designed not to break.
- Robust and reliable build process
  - Using Ansible and Vagrant
- Prepped distro
  - Rigoruous test cycle

How?

- 1 FTE with SANS to maintain the platform
  - Ryan O'Grady
- With support from Joshua Wright, Steve Sims, Daniel Pendolino and other SANS instructors.
- Target version is LTS

Tool install process

- The tools are installed in Slingshot as follows:



- Near future goal: Slingshot repository with packages

What you get

- Distro based out of Ubuntu 18.04 LTS
- Includes many penetration testing tools
- Includes PTF
  - Install
  - Update
- Includes utilities

Some of the tools installed

- Aircrack-ng
- Asleap
- BeEF
- Burp Suite
- coWPAtty
- Docker
- Empire
- Ettercap
- EyeWitness
- Golang
- hashcat
- hping3
- John the Ripper
- Kismet
- Metasploit Framework
- Nikto
- Nmap
- OpenVAS
- Powershell Empire
- Recon-ng
- Responder
- RITA
- Social Engineer Toolkit
- sqlmap
- tcpdump
- THC-Hydra
- Unicornscan
- Veil Evasion
- Wapiti
- weirdAAL
- Wireshark
- WPScan
- ZAProxy

PTF – Pentest Framework

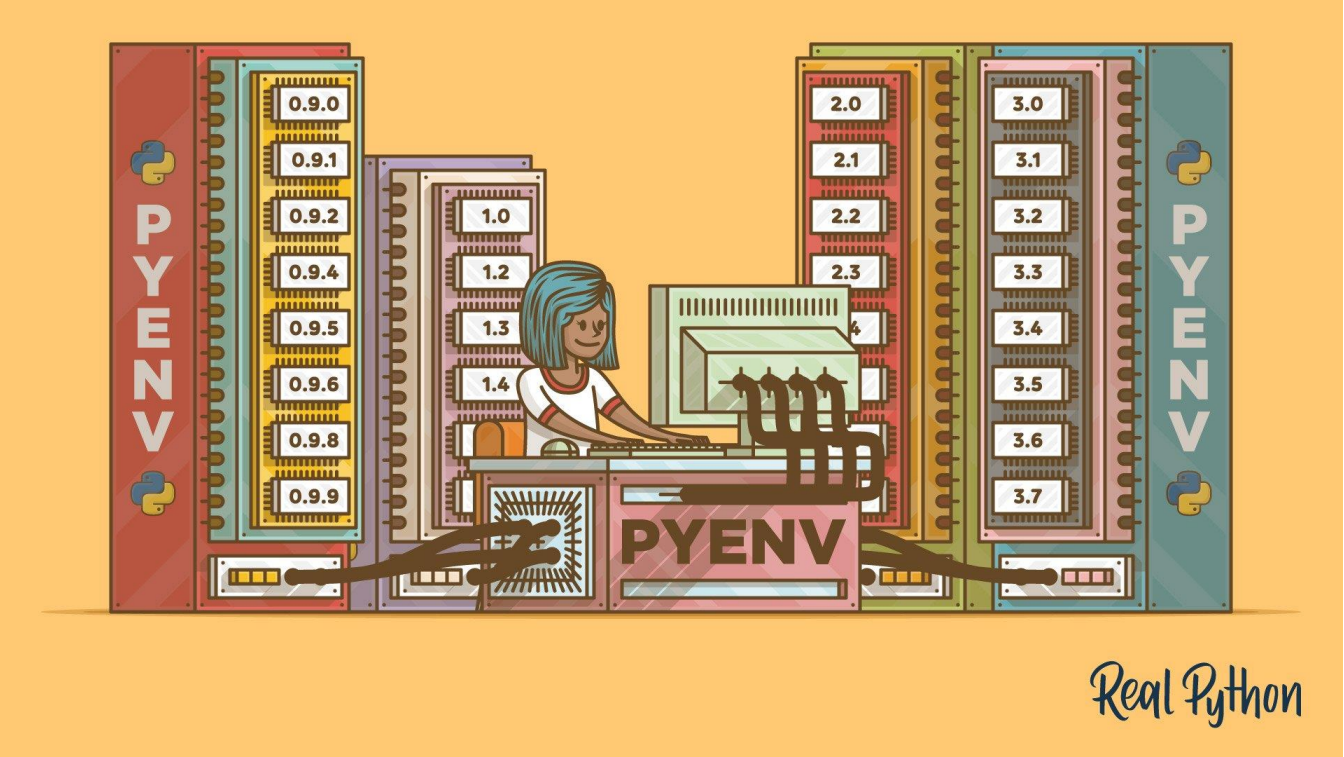
The PenTesters Framework (PTF) v2.3.3

File Edit View Search Terminal Help

```
[*] Operating system detected as: DEBIAN
[*] Welcome to PTF - where everything just works...Because..Mr. Robot

For a list of available commands type ? or help

ptf> ?
Available from main prompt: show modules, show <module>, search <name>, use <module>
Inside modules: show options, set <option>,run
Additional commands: back, help, ?, exit, quit
Update or Install: update, upgrade, install, run
ptf> show modules


The PenTesters Framework Modules
================================

   Name                                          Description
   ----                                          --------------

   modules/install_update_all                    This will install or update all tools with modules within PTF
   modules/update_installed                      This will update all installed tools within PTF
   modules/reversing/binwalk                     This module will install/update binwalk - a Firmware Analysis Tool
   modules/reversing/cfr                         This module will install/update cfr, a tool for decompiling java classes
   modules/reversing/cminer                      This module will install/update cminer - a code cave identifier
   modules/reversing/flare                       This module will install/update flare actionscript extractor
   modules/reversing/flasm                       This module will install/update flasm a command line Flash assembler/disassembler.
```

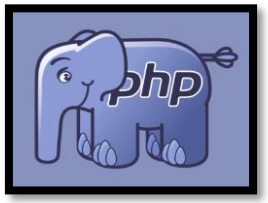
pyenv, rbenv

- Manges managing multiple versions of the interpreters easier.
- Allows you to download e.g. exploits and run them with a specific version.
- Support tools on different versions



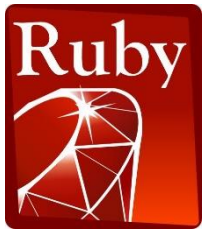
Interactive environments

- PHP 7.2.24



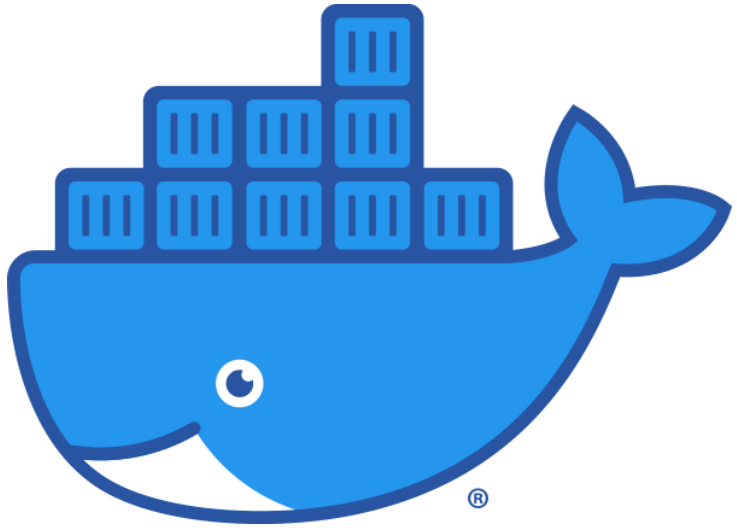
- Python2.7
- Python3

Ruby 0.9.6



Docker

- docker pull <name>
  - Pull an image from Docker Hub
- docker images
  - See which images you have ready
- docker build –t <tag> PATH|URL
  - Build from a Dockerfile

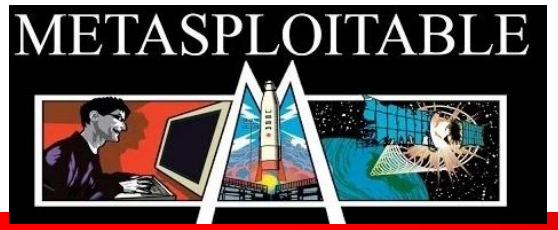


Running images as containers

- docker run [options] IMAGE [command] [arg…]
- docker ps
  - List running containers
- docker containers ls
- docker container stop <name>
- docker container rm <name>
  - Docker container prune

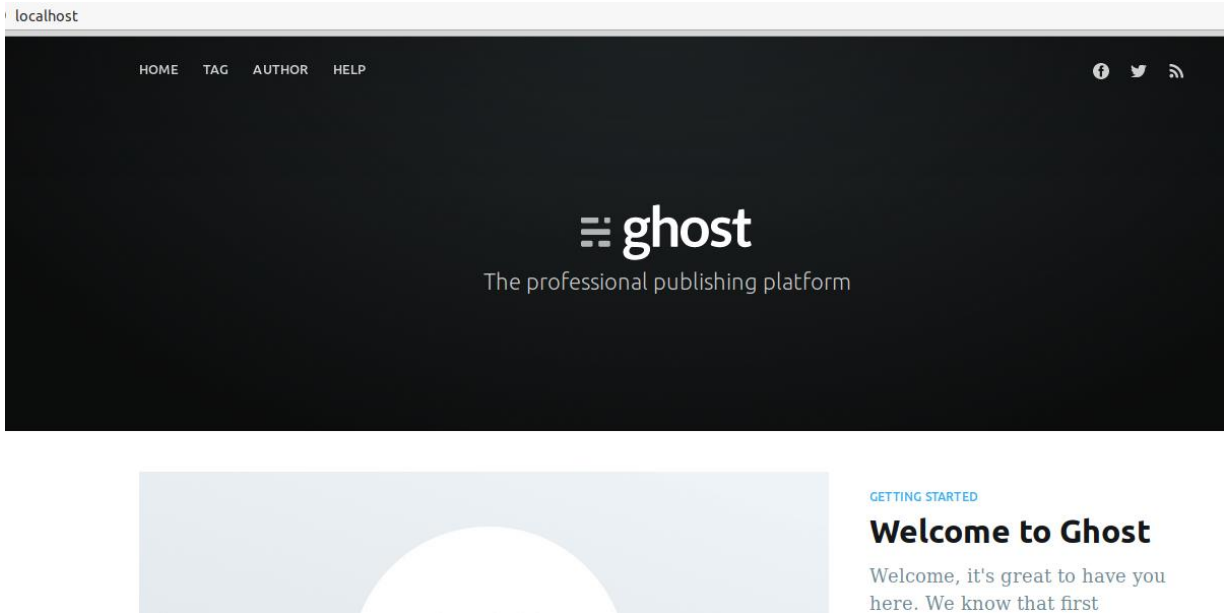
Get to hacking in no time!

- https://hub.docker.com/
- **DVWA**
  - docker run --rm -it -p 80:80 vulnerables/web-dvwa
  - Login with admin/password
- **Metasploitable**
  - docker pull tleemcjr/metasploitable2:latest
  - docker run -it tleemcjr/metasploitable2:latest sh -c "/bin/services.sh && bash"



Lets use Docker for some research

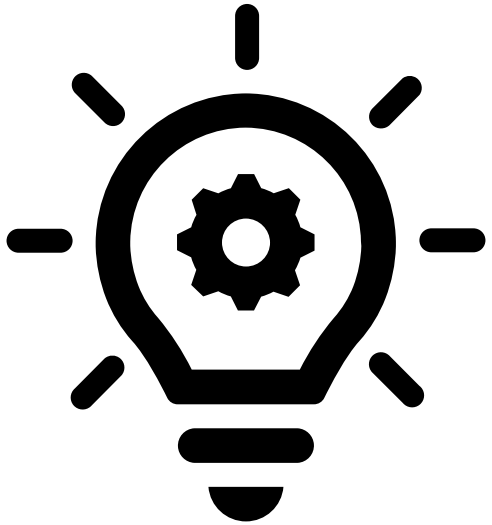
- docker run --rm -it -p 80:2368 ghost
  - Goto /ghost
- Create wordlist
- Start scans
- Do some 0day hunting



Connecting to HackTheBox

Tips for ease of use with host

- Consider adding a shared folder
  - Perhaps you have repos and what not here.
  - Tools and other things you want accessible
- Drag and drop support
- Shared clipboards



Future content

- Offline labs and challenge type content
- Quarterly CTF-type events
- Quality and stability efforts continue
- Continuity between classroom experience and community experience
- Content: Challenge and Educational
- User experience. Potentially for cloud syncing settings, etc.

Where can I get started?

- https://www.sans.org/slingshot-vmware-linux

Credentials: slingshot / slingshot

Slingshot has a counter-part

DOWNLOAD & INSTALL SIFT WORKSTATION

Option 1: SIFT VM Appliance Download:

- Download SIFT Workstation Virtual Appliance (.ova format)

- Login = **sansforensics**
- Password = **forensics**

Option 2: SIFT Easy Installation:

1. Download Ubuntu 16.04 ISO file and install Ubuntu 16.04 on any system
   - http://www.ubuntu.com/download/desktop
2. Install SIFT-CLI using these install instructions
3. Run '**sudo sift install**' to install the latest version of SIFT
4. Congrats -- you now have a SIFT workstation!!
   - Login = **sansforensics**
   - Password = **forensics**

Finding any bugs or install issues? If you are experiencing errors in SIFT itself, please submit errors, bugs, and recommended updates here: https://github.com/sans-dfir/sift/issues

Thank you for listening!

https://netsecurity.no/en

@chrisadale

https://www.linkedin.com/in/chrisad