Pen testing

What is pen testing?

Pen testing is both art and science

- Humans **probe** and **interact** with a system, looking for different weaknesses or attack vectors
  - Employing **cleverness, adaptation, ingenuity**
- Once patterns of exploration and exploitation emerge, you write computer programs (tools) to do the work
  - **Ingenuity automated**

> Science is what we understand well enough to explain to a computer. Art is everything else we do.
> *—Donald Knuth*

Pen tester's bag of tricks

A pen tester approaches a target knowing …

- **the workings of the target domain** (e.g., the web)
- .. **how systems are built** in that domain
  - **Protocols** (e.g., HTTP, TCP, …)
  - **Languages** (e.g., PHP, Java, Ruby, …)
  - **Frameworks** (e.g., Rails, Dream Weaver, Drupal)
- .. **common weaknesses** in the software/system
  - **Bugs** (e.g., SQL injections, XSS, CSRF, …)
  - **Misconfigurations, bad design** (e.g., default passwords, "hidden" files, …)

Web hacking: A professional's view

Eric Eames
of FusionX

70% messing with parameters

If the URL is `http://tgt.com/buy?item=1&price=5.00`

Then change it to:

- `/buy?item=1&price=0.01`
- `/buy?item=10&price=5.00`
- `/buy?item=1&price=5.00<script>alert("test");</script>`
- `/buy?item=1&price=5.00'`

Client parameters (unwisely) trusted?

Susceptible to XSS?

Susceptible to other injection?

Web hacking: A professional's view

Eric Eames
of FusionX

10% default passwords

- Always research the default password and try it
  - Works way more often than you'd think

10% hidden files and directories

- Look through the manuals for clues
- Directory brute forcing

10% other

- Authentication problems (bypass, replay, …)
- Insecure web services
- Configuration page gives away your root password

Tools

We'll consider a few.
A comprehensive list is at
http://sectools.org/

- Pen testers use tools to
  - **Probe** a target
  - **Gather information** and **test** hypotheses about it
  - **Exploit** a vulnerability (or attempt to)

- Which tool depends on the **goal**, and the **target**
  - If an **enterprise network**, want to find, probe, and exploit machines, routers, topology, etc.
  - If a **single machine**, want to consider installed software, running programs, interesting files
  - if a **single program**, want to explore and exploit possible inputs and interactions

`Nmap` for network probing

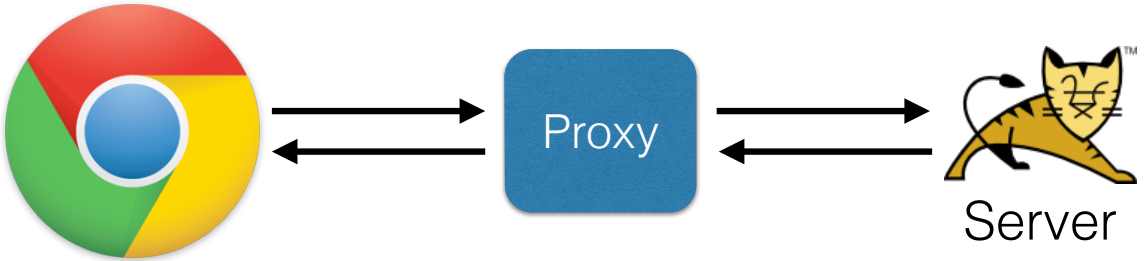
- `Nmap` stands for “network mapper”. Figures out
  - what **hosts** are available on the network,
  - what **services** (application name and version) those hosts are offering,
  - what **operating systems** (and OS versions) they are running,
  - what type of **packet filters/firewalls** are in use
  - *… and more*
- Works by **sending raw IP packets** into the network and **observing the effects**
- Free, open source (commercial tools too) http://nmap.org/

Finding hosts, services

- `Nmap` will ***ping*** a specified **range of IP addresses**
  - ICMP Echo Request and/or Timestamp request
    - Standard “ping” protocol
  - TCP SYN to port 443, TCP SYN/ACK to port 80
    - Looking for running HTTPS or HTTP servers
  - Other things, as determined by the operator
    - Protocol-specific UDP packets to particular ports
    - Probes to other TCP ports
    - Probes that elicit different responses on different OSes (“fingerprinting”)
- **Be stealthy**
  - A flurry of scanning activity may be detected
  - Control the rate of scanning to “work under the radar”

Web proxies

- **Web applications** are common pen testing targets
- Web proxies sit *between* the **browser** and **server**
  - **Displaying** exchanged packets
  - **Modifying** them as directed by the tester



  - Some proxies have additional features for vulnerability scanning/exploitation, site probing, etc.

Zap

- *OWASP* **Zed Attack Proxy** (Zap)
  - GUI-based inspection/modification of captured packets
  - Can set “breakpoints” to allow packets through until a certain condition is met
- Additional features
  - **Active scanning**: attempts XSS, SQL injection, etc.
  - **Fuzzing**: context-specific payloads
  - **Spider**: explores a site to construct a model of its structure
- Free, open-source https://code.google.com/p/zaproxy/
- See also the **Burp suite** http://portswigger.net/burp/

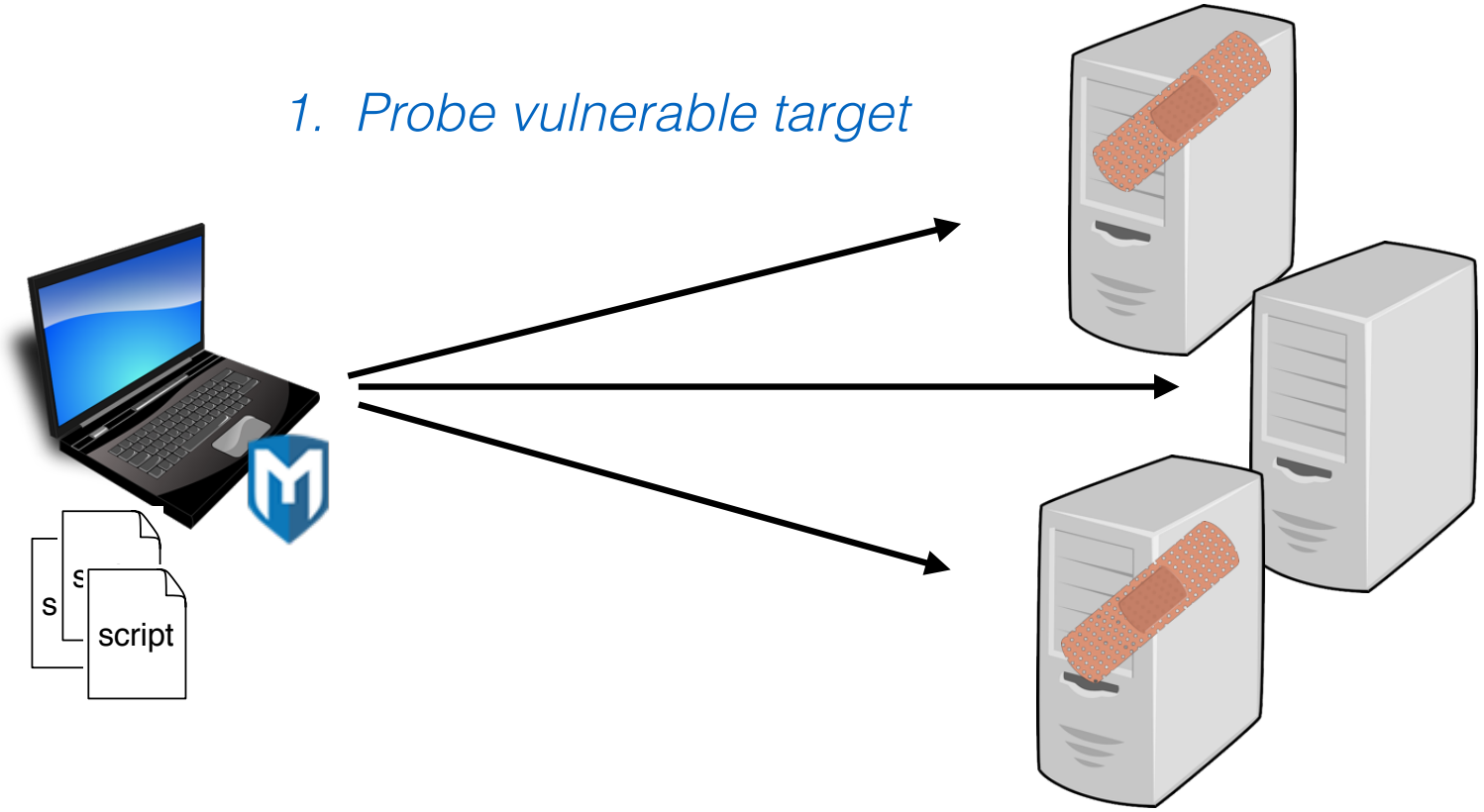
Metasploit

- Metasploit advanced open-source **platform** for **developing, testing,** and **using exploit code**.
  - Boasts an **extensible model** through which *payloads*, *encoders*, *no-op generators*, and *exploits* can be integrated

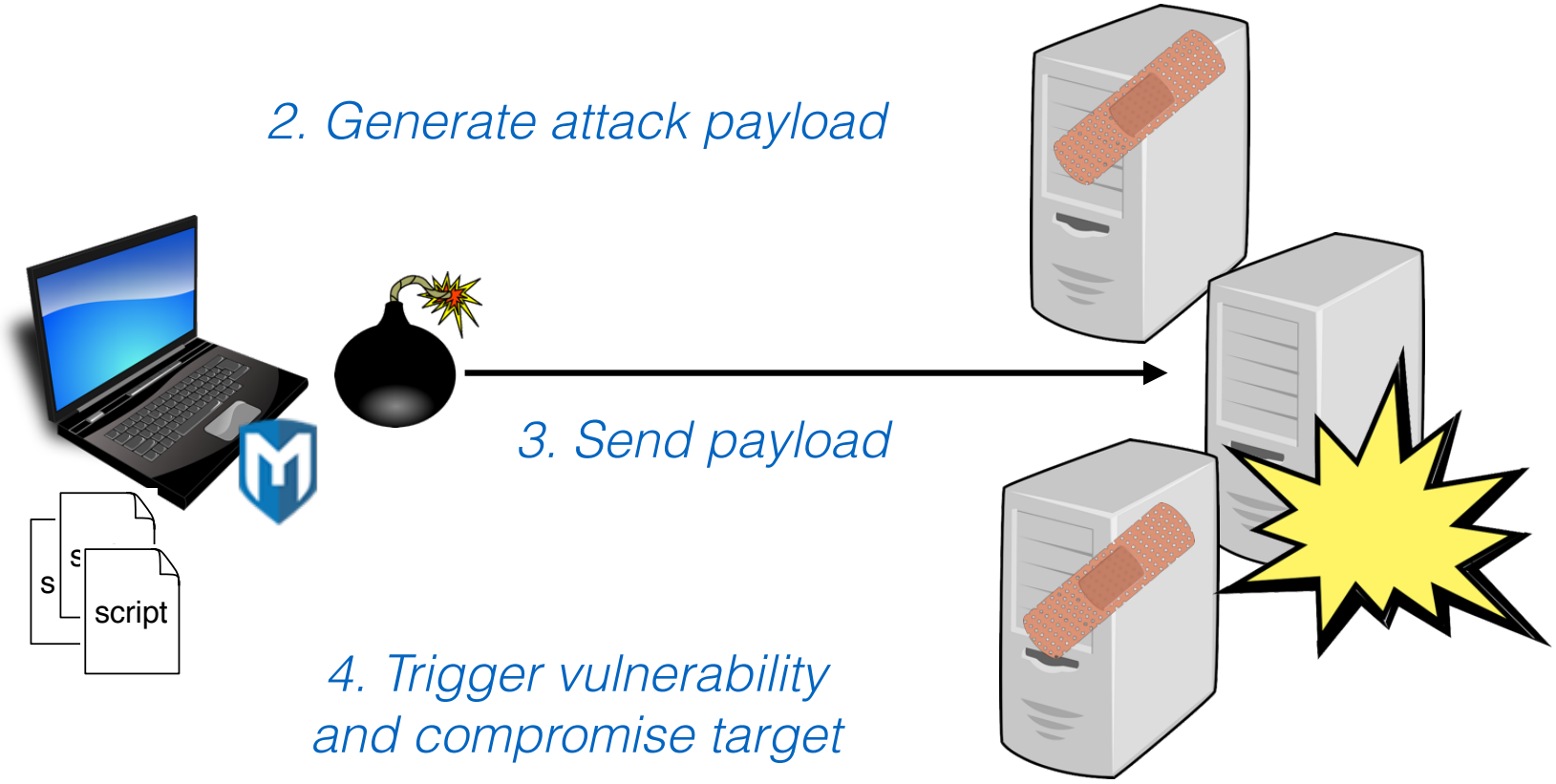
- **Scripting attacks**
  - **Probe** remote site looking for vulnerable services
  - **Construct** payload based on versions, other features
  - **Encode** payload to avoid detection
  - **Inject** payload
  - **Wait** for shellcode to connect back; **command prompt**!

Metasploit

1. *Probe vulnerable target*



Metasploit


2. Generate attack payload
script
3. Send payload
4. Trigger vulnerability
and compromise target

Metasploit UI

- `msfconsole` — **interactive console** for executing metasploit commands
  - Also web-based frontend and command-line interface
  - Supports **probing** and **communications commands**, **payload construction** (and **encoding**)
  - Supports **active** (*go get `em*) and **passive** (*wait til they come to us*) attacks
- *Meterpreter* - command processor injected into the target, e.g., in the memory of a compromised process
  - Permits the pen tester to probe more stealthily
- `msfpayload`, `msfencode` — generate (stealthy) shellcode

100's of modules, scripts

- **Exploits** against **particular vulnerabilities**
  - Along with stagers and other modifiers to generalize these exploits to different platforms
- **Password sniffing**
  - Reading unprotected passwords off of the network
- **Privilege escalation**
  - After penetrating, try to get SYSTEM privileges
- **Keylogging** and **backdoors**
  - For persistent presence
- *… and much more*

http://www.offensive-security.com/metasploit-unleashed/Main_Page

Kali

- Kali is a **Linux distribution** with many open-source **pen testing tools installed and configured**
- The ones we have already mentioned
  - Nmap, Zap, Metasploit, Burp Suite
- and **dozens more**
  - **John the Ripper** for password cracking
  - **Valgrind** for dynamic binary analysis
  - **Reaver** for Wifi password cracking
  - **peepdf** for scanning PDF files for attack vectors
  - *… and more*

http://www.kali.org/

Ethical Hacking

- Penetration testing tools are meant to **reveal security vulnerabilities**
  - **So they can be fixed**
  - *Not so they can be exploited in the wild*

Beware the dark side!

- **But** people use tools for **nefarious purposes**
  - **Don't be one of them!**