Networks & Server Structures

LAMP Servers

Security Threats

Authentication

Malware

LAMP Servers

I love LAMP

LAMP

- Linux
- Apache
- MySQL
- PHP

Linux

- The operating system that runs the applications
- Minimal hardware requirements
- Fast
- Free
- Can be run with or without a GUI

Using Linux

- Installing programs in Linux depends on what distribution you are using
- Package - distributions of software, applications and data, also contain metadata, and a list of dependencies necessary for the software to run properly
- Repository - a storage location from which software packages may be retrieved and installed on a computer
- Package manager - a collection of software tools to automate the process of installing, upgrading, configuring, and removing software packages

Linux Package Types

- rpm - originally developed by Red Hat
- deb - originally developed by Debian

Linux Package Managers

- For RPM packages
  - Yum
- For DEB packages
  - dpkg
  - Apt
    - apt-get
    - Aptitude (includes gui in command line)
    - Synaptic
- Pick one method and STICK WITH IT!

APT

- apt-get install
- apt-get remove
- apt-get update

Linux

- Everything is either a file or a process
  - File = collection of data
  - Process = an executing program
- All configurations are done by editing configuration files

Linux

- Big difference between root user and standard user
- Root user has complete access to and authority over the system
  - Home folder is /root
- Standard users do not have complete access to the entire system and only have the ability to perform certain tasks
  - Home folder is typically /home/username

Apache

- Web Server
- Fast
- Virtual hosts
- Most popular web server
- Can serve static web pages and execute scripts
- Free

MySQL

- Structured Query Language
- Relational database management system
- Fast
- Can store various types of data quickly and efficiently with minimal effort
- Databases are important for creating dynamic websites
- Free

PHP

- PHP Hypertext Preprocessor
- Originally stood for Personal Home Page
- Server-side scripting language
- Fast
- Free

Client Side vs Server Side

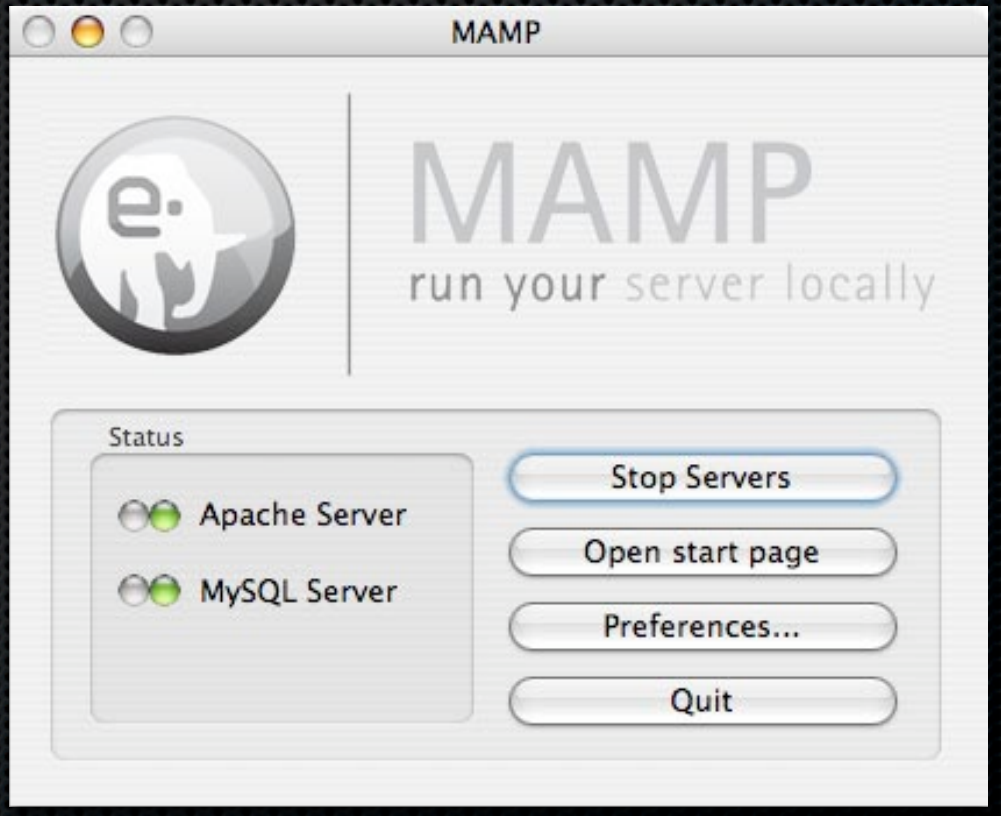
- Server Side
  - User's request is fulfilled by running a script directly on the web server
- Client Side
  - Scripts are run by the web browser

LAMP

- Any part is interchangeable
- XAMP - OSX, Apache, mySQL, PHP
- LAMP - Linux, Apache, mySQL, PERL
- LAMP - Linux, Apache, mySQL, Python
- WAMP - Windows, Apache, mySQL, PHP
- WIMP - Windows, IIS, mySQL, PHP

MAMP

- Mac Apache MySQL PHP
- http://mamp.info/en/mamp.html



Network Security

You're at risk right now!

3 Rules of Security

- Robert Morris, Cryptographer
  - Do not own a computer
  - Do not power it on
  - Do not use one
- Risk vs Benefit
- There’s no such thing as full perfect security

Network Security

- Network security is the process by which digital information assets are protected.
- Security = protection against malicious attack by outsiders

Three Goals of Security

- Integrity
- Confidentiality
- Availability

Integrity

- Assurance that data is not altered or destroyed in an unauthorized manner
- Integrity is maintained when the message received is identical to the message sent

Confidentially

- Protection of data from unauthorized access by or disclosure to a third party
- Only authorized parties should be granted access to info that has been identified as confidential

Availability

- The assurance that computer services can be accessed when needed
- System downtime = lost revenues

Security Threats

- **CONVENIENCE IS THE ENEMY OF SECURITY!!!**

Security Threats

- Examples
- Corporate espionage
  - $100 Billion in lost profits due to info theft
- Identity theft
  - 700,000 Americans have their personal info used illegally each year
- Computer viruses
  - $13.2 Billion dollar impact in 2001

Security Threats

- 4 Primary Sources
- Technology weaknesses
- Configuration weaknesses
- Policy weaknesses
- Human error or malice

Technology Weaknesses

- TCP/IP - Open Standard
- Operating Systems - need the latest patches, updates and upgrades
- Network Equipment - must be protected

Configuration Weaknesses

- Unsecured Accounts - packet sniffers
- System Accounts - easily guessed passwords
- Misconfigured Internet Services
- Unsecured Default Settings
- Misconfigured Network Equipment

Human Error & Malice

- Accident
- Mistaken destruction, modification, disclosure, or incorrect classification of information
- Ignorance
- Inadequate security awareness or lack of knowledge
- Workload
- Too many or too few system admins

Human Error & Malice

- Dishonesty - fraud, embezzlement
- Impersonation - try to persuade users to give out usernames and passwords
- Disgruntled employees
- Snoops - corporate espionage
- Denial of Service attacks - engulf the network equipment with useless noise causing systems to crash

Authentication

- The process of determining whether someone or something is, in fact, who or what it is declared to be
- 3 Layers
  - What you know
  - What you have
  - What you are

What You Know

- Username
- A unique identifier that we use to identify ourselves to a computer or network system
- Password
- A secret combination of key strokes that authenticates you to the computer or network system

Password Guidelines

- Passwords must be memorized
- Passwords must be different for each separate application or site (can’t trust someone else with your security!)
- The longer the password the better
- Passwords should contain a mixture of letters (uppercase & lowercase) numbers, and other characters such as %, !, $, &, etc.

How Long to Crack?

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Password Creation

- Should be easy to remember but difficult to recognize
- PassPhrase
- H4x0r l337 5p33k

Password Hacking

- Your partner, child, or pet's name, possibly followed by a 0 or 1
- The last 4 digits of your social security number.
- 123 or 1234 or 123456.
- "password"
- Your city, or college, football team name.
- Date of birth – yours, your partner's or your child's.
- "god"
- "letmein"
- "money"
- "love"

Password Hacking

- Your partner, child, or pet's name, possibly followed by a 0 or 1
- The last 4 digits of your social security number.
- 123 or 1234 or 123456.
- "password"
- Your city, or college, football team name.
- Date of birth – yours, your partner's or your child's.
- "god"
- "letmein"
- "money"
- "love"

Covers ~20% of the population!!!

What You Have

- Security Token
  - Authentication device that has been assigned to a specific user by an appropriate administrator
- Passive Token
- Active Token

Passive Token

- Act as storage devices for base keys
- Most common type are cards with magnetic strips (ATM cards, credit cards, card keys)
  - Cheap to manufacture
  - Easy to carry
  - Easy to copy
  - Usually paired with a PIN number

Active Token

- Actively creates another form of the base key
- Examples
- One-time password
- Encrypted form of the base key

One-Time Password

- A password that is used only once for a very limited period of time and then is no longer valid
- Typically generated using a counter-based token or clock-based token

What You Are

- Biometric Authentication
- Based on an individual's unique physical or behavioral characteristics
- Fingerprints
- Hand geometry
- Retinal and iris patterns
- Facial characteristics
- Expensive

Attacks & Malicious Code

- Denial-of-service attacks
- Distributed DOS attacks
- Man in the middle attacks
- Spoofing
- Social engineering
- Software exploits

Denial of Service Attack

- DoS Attack
- Any attack that consumes or disables resources in order to interrupt services to legitimate users
- Objective is to disrupt normal operations, not to steal or destroy data

Denial of Service Attack

- SYN Flood
- Prevents users from accessing a target server by flooding it with half-open TCP connections

Denial of Service Attack

- Smurf
- Uses a third-party's network segment to overwhelm a host with a flood of ICMP packets

DDoS Attack

- Distributed Denial of Service Attack
- Attacker manipulates multiple hosts to carry out a DoS attack on a target.

Man in the Middle

- The attacker places himself between two communicating hosts and listens in on their session
- Both hosts think they are communicating with each other but they are in fact communicating with the attacker
- Done through ARP poisoning and ICMP redirects

Spoofing

- IP address spoofing
- ARP poisoning
- Web spoofing
- DNS spoofing

Social Engineering

- using con tricks to persuade people to do what criminals and hackers want them to do or to gain access to a secure network

Social Engineering

- Appeal to greed, fear or scarcity
- Authority figures. We are more likely to do something for ‘the boss’
- Friendliness. We are much more likely to trust someone we like
- People generally want to be helpful and are afraid of confrontation
- We don’t like to appear foolish or uninformed but get confused by technical details and tend to be unwilling or unable to check facts
- Reciprocity. We often feel obliged to return a favor

Social Engineering

- Consistency. Generally people want to appear consistent and trustworthy so we tend to try to behave in ways which are consistent with earlier behaviour, even if it was foolish.
- We assume people are telling the truth so conmen will mix a little lie with a big truth.
- Social proof: we tend to follow the crowd, rather than appear isolated or foolish.
- A hook: a naked celebrity or a link to current events.

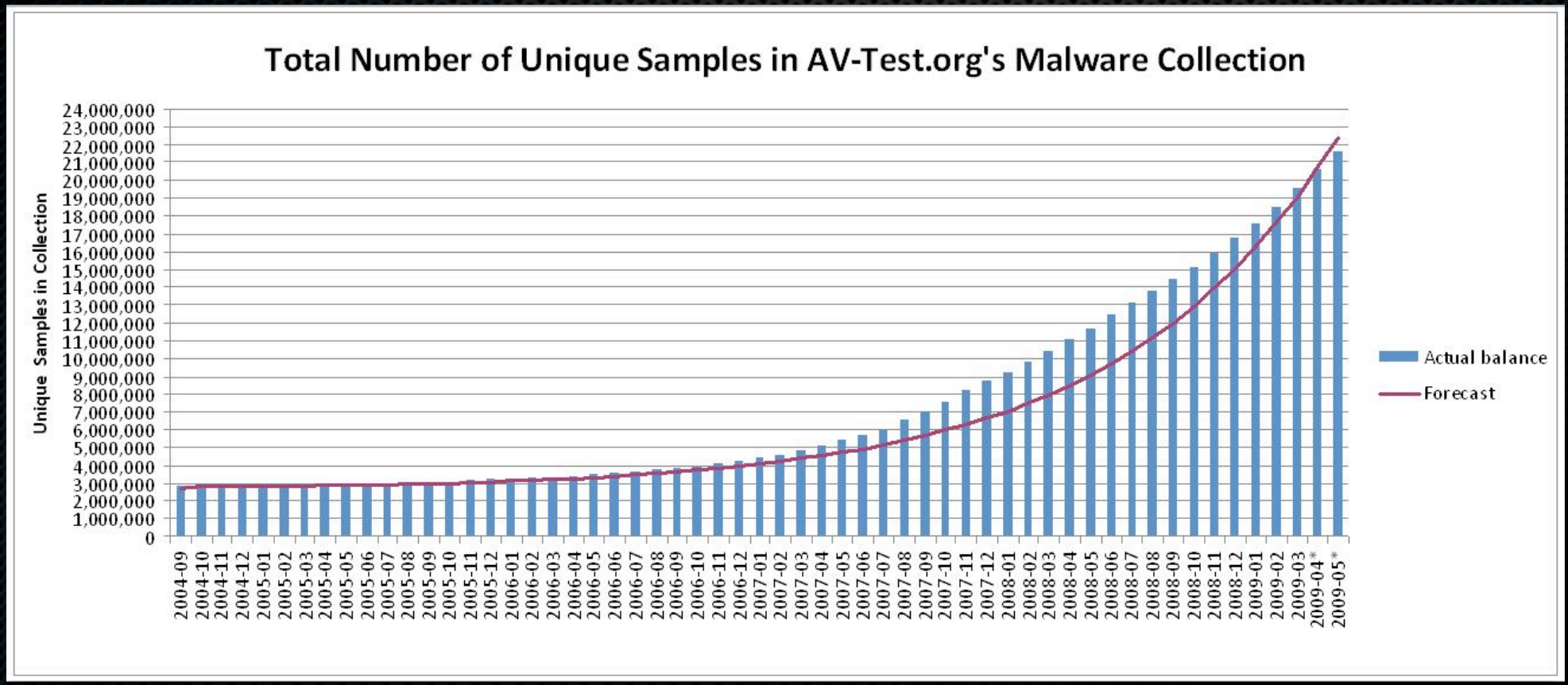
Software Exploitation

- Software Vulnerabilities
- Buffer Overflows
- SQL Injections

Malware

- Viruses
- Worms
- Spyware
- Crapware

Malware


Total Number of Unique Samples in AV-Test.org's Malware Collection
Unique Samples in Collection
24,000,000
23,000,000
22,000,000
21,000,000
20,000,000
19,000,000
18,000,000
17,000,000
16,000,000
15,000,000
14,000,000
13,000,000
12,000,000
11,000,000
10,000,000
9,000,000
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
2004-09
2004-10
2004-11
2004-12
2005-01
2005-02
2005-03
2005-04
2005-05
2005-06
2005-07
2005-08
2005-09
2005-10
2005-11
2005-12
2006-01
2006-02
2006-03
2006-04
2006-05
2006-06
2006-07
2006-08
2006-09
2006-10
2006-11
2006-12
2007-01
2007-02
2007-03
2007-04
2007-05
2007-06
2007-07
2007-08
2007-09
2007-10
2007-11
2007-12
2008-01
2008-02
2008-03
2008-04
2008-05
2008-06
2008-07
2008-08
2008-09
2008-10
2008-11
2008-12
2009-01
2009-02
2009-03
2009-04*
2009-05*
Actual balance
Forecast

Virus

- Self replicating programs that spread by infecting other programs

Virus Types

- Boot sector
- File infector
- Macro viruses - application specific, VBA
- Companion
- Polymorphic - mutates as it copies itself

Trojan Horse Virus

- Trojan War
  - Achaeans (Greeks) waged war on city of Troy
  - Couldn’t penetrate the wall around Troy
  - Constructed a large wooden horse left it for the Trojans and pretended to sail away
  - Trojans brought horse into city walls
  - At night 30 Achaeans hidden inside came out and opened the city walls
  - Achaean army came in and destroyed the city

Trojan Horse Virus

- Malware which presents itself as something useful or beneficial
- Can look like games, pictures, MP3's, screen savers or pornography
- Installs backdoor/remote control programs or deletes or modifies files

Rootkit

- Software that enables privileged access to a computer while actively hiding its presence by subverting standard operating system functionality
- Changes the way the OS works for the express purpose of hiding malicious software
- Usually installed on a victim's machine via social engineering

Worms

- Self contained program that uses security flaws such as buffer overflows to remotely compromise a victim and replicates itself to that system
- Does not require the execution of an infected application

Spyware

- Collects information about users without their knowledge
- May be innocent or nefarious
- Adware - displays advertisements based on what it finds from “spying” on the user
- Keylogger - records your keystrokes and possibly mouse clicks
  - Can grab passwords

Crapware

- Software already installed on a computer bought from an OEM (Original Equipment Manufacturer)
- Cost effective
- Mostly useless and unwanted
- Sometimes difficult to remove