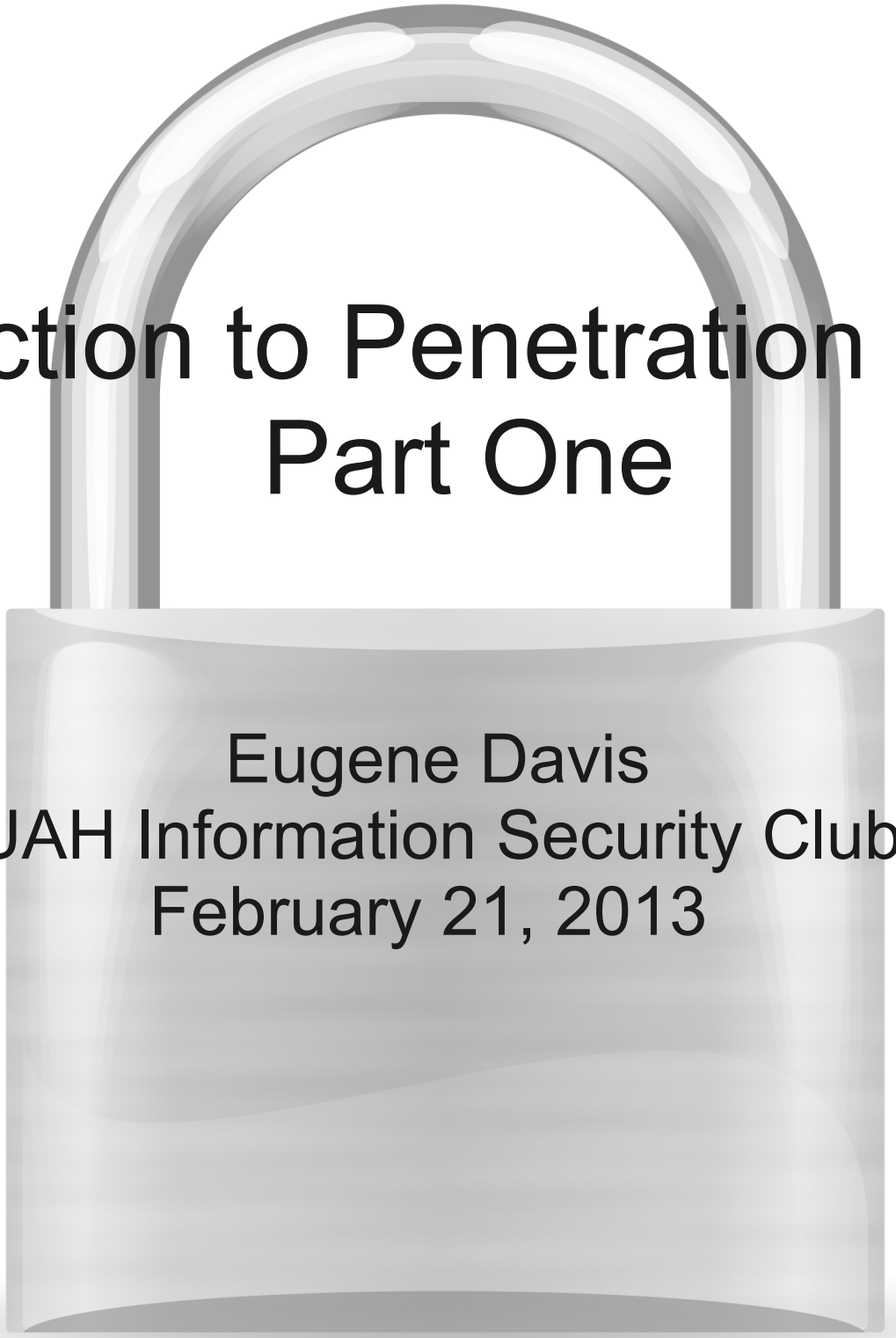


Introduction to Penetration Testing: Part One

Eugene Davis
UAH Information Security Club
February 21, 2013

Ethical Considerations: Pen Testing

- Ethics of penetration testing center on integrity
- (ISC)² Code Of Ethics Cannons
  - Protect society, the common good, necessary public trust and confidence, and the infrastructure
  - Act honorably, honestly, justly, responsibly, and legally
  - Provide diligent and competent service to principals
  - Advance and protect the profession
- Maintain privacy and confidentiality
- Acquire written permission from appropriate authorities before performing pen testing on systems

What is Pen Testing?

- Penetration Testing, a.k.a ethical hacking
  - Uses the same techniques as hackers to find weaknesses in systems
  - Testing can be done by employees of an organization or by trusted third parties
  - Can be broken down into phases of attack

Phase 1: Reconnaissance

- Finding information about a target
- Can learn about the assets on the target's network
  - Network structure and potential vulnerabilities are of especial value
- Most organizations leak a large amount of data on a regular basis
  - Requires a strict policy to prevent it

Info from the Web and Trash

- Websites might have documents meant for internal consumption
- Employees post questions on forums revealing sensitive network details
- Dumpster diving can turn up passwords, old CDs, manuals and more
- Especially vulnerable when an employ is moving

Social Engineering

- Most common is talking your way in
  - Acting like you belong is key
  - Uniforms can help
- Spoofing phone numbers
  - Make the call report an internal number
  - Ask like you've forgotten something or are a new hire

Defenses

- User education
- Monitor what information is allowed online
- Have firm policies about destroying media
- Strictly enforce ID checking if your organization requires it

Phase 2: Scanning the Target

- Search for open access points into the network
- Scanning is an active form of reconnaissance
- Determine what open ports are on a system and firewall
- Looks for vulnerabilities on the systems in the network

War Dialing

- Some users still attach modems to their computers for easy remote access
- War dialing is targeting the block of telephone numbers assigned to an organization
  - Generally uses automated software capable of checking thousands of numbers in a few hours
- A successful connection results in direct access to the computer

War Driving

- With a laptop, GPS, and a chauffeured car an attacker can search for open wireless access points
- Many users do not setup encryption on their wireless networks
- In a city, this may turn up dozens, even hundreds of unencrypted or WEP encrypted access points in a short time

Scanning Tools

- Port scanners reveal what TCP ports will respond to attempted connections
- Firewalk is a technique to see what ports are open in a firewall
- Vulnerability Scanners search for exploitable vulnerabilities on the network

Nmap Uses

- Nmap, or Network Mapper, scans IPs to detect open ports
- Can attempt to detect the service on a port, even the version
- Is capable of discovering some operating systems
- Can also perform some network mapping

Nmap Examples

- Perform a ping scan to see what hosts are on the network:
  nmap -sn 192.168.0.1/24
- Scan for OS and version for a particular target
  nmap -A -T4 192.168.0.122
- Scan UDP ports with fragmented packets
  nmap -sU -f 192.168.0.124
- And far, far more

Firewalk and Nessus

- Firewalk maps a network from a remote location
- By using traceroute, it can determine at what point a firewall kicks in
- Can determine what ports are being blocked by a firewall

- Nessus is a proprietary (with a non-commercial free version) vulnerability scanner
- This looks for known vulnerabilities on the area being scanned, and alerts the initiator of the scan

Phase 3: Exploits and Compromises

- The attacker gains control of machines on the target network
- Operating system attacks allow control over individual systems
- Network attacks can reveal methods to control many machines on the network
- DoS attacks take machines or services offline

Operating System Attacks

- Buffer overflow exploits can allow remote code execution
- Password guessing is an obvious method for gaining control
- Malicious web applications and scripts may seize control
- SQL injection commonly targets servers

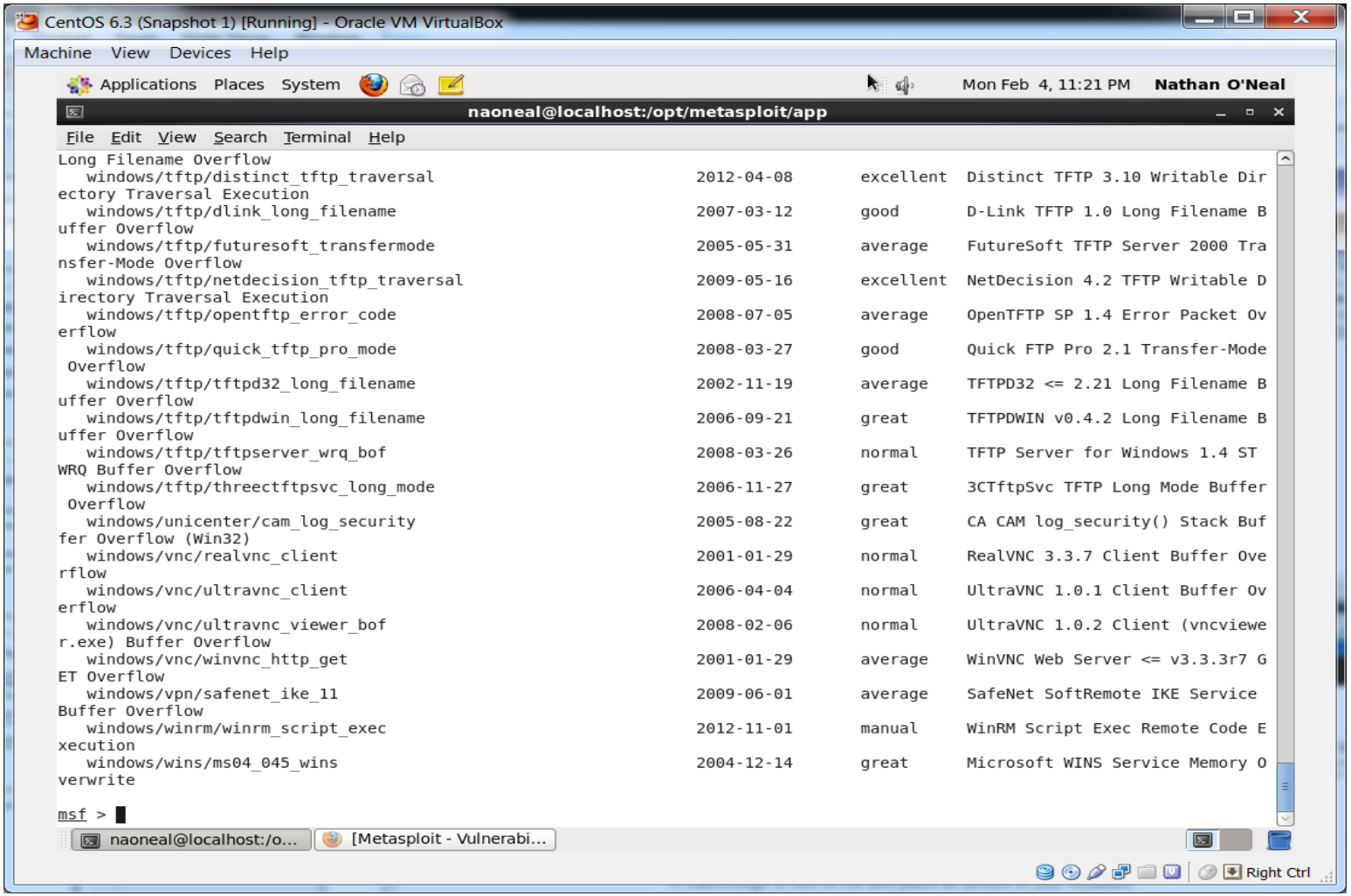
Buffer Overflow Exploits

- Stack Buffer Overflow (smashing the stack)
  - Overwrite a local variable near the buffer to alter the execution of the program
  - Change the stored return address after function execution allowing for the possibility of arbitrary code to be executed
- Heap Buffer Overflow
  - Just as dangerous at Stack Buffer Overflows
  - Used to overwrite function pointers that exist in memory, pointing it back to the attackers code
  - Also allows access to user data within the scope of the program

Automating the Exploit Process

- Identifying individual vulnerabilities on a target and knowing which exploit to use is time consuming
- Tools such as Metasploit can be used to automate the process
  - Metasploit will map vulnerabilities that were found (even by other tools such as Nmap and Nessus) to the appropriate exploit within Metasploit
  - Metasploit lists exploits in best-to-worst likelihood of success, thus saving time in choosing which attack to launch against a target system

Automating the Exploit Process



Password Guessing

- Brute force
  - The most widely known attack that tries to use every possible character combination as a password
- Account Harvesting
  - Involves the gathering of email addresses and possible user names from various sources on the internet
  - These can then be used in a phishing attack against an individual target to try and obtain more personal information
  - If you are told that the user name is valid/invalid, guessing becomes easier
- Both of these processes are usually automated
  - Current versions of Backtrack contain tools used in both types of attacks

Compromising the Web Browser

- Cross-Site Scripting (XSS)
  - Malicious scripts are injected into trusted websites, generally in the form of a browser side script, and sent to another end user
  - The end user's browser will then execute the malicious script
- SQL Injection
  - Allows an attacker to spoof their identity and alter, insert or delete data from a database
  - Allows for the complete disclosure of all data on the system
  - Attacker can become administrator of the server

Defenses

- Employ the use of strong passwords
- Keep systems updated and patched with the latest fixes
- Use an Intrusion Detection System (IDS)
- Use parameterized SQL

References and Links

- CounterHack Reloaded by Ed Skoudis
- Nmap - http://nmap.org/
- Firewalk - http://packetstormsecurity.com/UNIX/audit/firewalk/
- Nessus Vulnerability Scanner - http://www.tenable.com/products/nessus
- (ISC)² Code Of Ethics - https://www.isc2.org/ethics/default.aspx
- EC-Council - http://www.eccouncil.org
- Open Web Application Security Project (OWASP) - https://www.owasp.org

License