Markos Gogoulos
https://unweb.me

Who am I

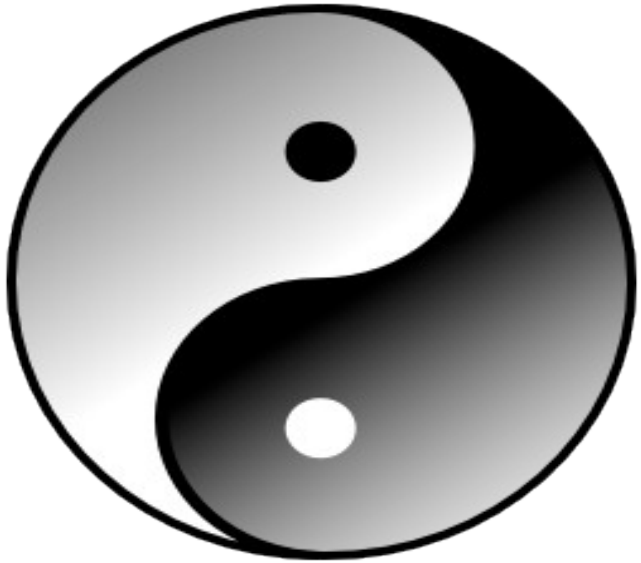
- free & open source software user and developer
- network security enthusiast
- *unweb.me* member

Open Source and Security

- a whole culture around Open Source and Security
- Programmers comply with standards and secure programming practices

This leads to

- a plethora of security related protocols and standards
- (mostly) secure programs and operating systems
- even operating systems dedicated to security!



Why open source software is more secure

- **Code is open to anyone**, gets reviewed by many eyes (eg expert programmers)
- Programmers have to comply with standards (to get their code accepted)
- Very flexible teams/ really low response and patching time
- Complexity is deliberately avoided

Open source communities try to solve problems, rather than distract their users and try to hide them

- Open security lists
- Tools and techniques for the job (runtime analysis, fuzzing, static analysis)
- No backdoors!

Closed source software and security

- Some vendors claim that their software is more secure because it's secret:

NONSENSE!

- Vulnerabilities will be found eventually.
- decompilers,disassemblers that turn the machine code back into source code
- fuzzers, static analysis tools etc
- code leaks by employees, hackers

Closed source software and security

- Keeping Vulnerabilities Secret Doesn't Make Them Go Away
- Blackhats might already know (use/sell) them
- Vulnerabilities' underground market: blackhat/cracker networks, IT security companies (gain commercial advantage), antivirus companies etc

- **Example: 0day MS IIS 5.0 FTP Server Remote SYSTEM exploit (known in the underground for months)**

Closed source software and security

Borland's InterBase server (CERT advisory CA-2001-01)

- **a backdoor account existed for 6 years!!! Allowing root compromise**

found in Dec 2000, when Borland released the code

***backdoor* could be easily found by looking at an ASCII dump of the program**

A *quick* overview of some Open source Programs/Protocols

Linux OS and Security

- **Quick and easy mechanisms for software updates**
- **unnecessary services are disabled**
- **packet filtering with iptables**
- **privilege management with sudo (avoids use of root)**
- **A plethora of kernel patches and security standards available (selinux, PAM, etc)**

Open source tools: OPENSSH

SSH: network protocol that allows data to be exchanged using a secure channel between two networked devices.

typically used:

to log into a remote machine and execute commands

tunnel, forward TCP ports and X11 connections

transfer files (sftp, scp)

- **OPENSSH: open source software implementation of ssh protocol (more robust than closed source implementations)**

Open source tools: TOR

- **A free software and open network that helps protect privacy and anonymity.**
- **Works by bouncing communications around a distributed network of relays run by volunteers all around the world (onion routing).**
- **Data travells around the net encrypted**
- **Used by activists, journalists, citizens in countries where internet is prohibited/filtered, hackers, corporations etc**

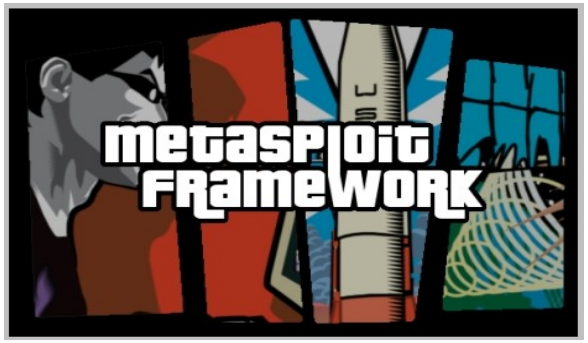
Open source tools: BACKTRACK

Ultimate security tools collection, packed on a Linux distro!

- **enumeration (information gathering)**
- **network scanners, port analysis, vulnerability scanners**
- **Sniffers, network analyzers, session hijacking, spoofing**
- **tools for exploiting vulnerabilities (e.g. Metasploit Framework)**
- **a set of Exploits (publicly available)**
- **proxy tools, fuzzers, denial of service tools**
- **web application penetration, password crackers, brute-forcers**
- **debuggers, reverse enginnering software, disassemblers, decompilers**

Open source tools: Vulnerability Scanners

- **Nessus/Nmap/Webscarab/Ratproxy/Metasploit framework to name the most popupal**
- **Provide 99.x% of the closed source equivalents (if they exist), that often cost 10.000's...**



Open source tools: AIRCRACK-NG

- **The ultimate network analyzer/analysis suite for 802.11 wireless LANs**
- **Amongst the first OSS to implement WEP cracking, much earlier than any commercial/closed source program**
- **Also cracks WPA, detects hidden Aps, plus more**

Some advice for users

- be informed and suspicious... do not trust anyone asking you personal info!
- stay patched, install updates, use antivirus (M$ users)
- use open source software, support OS diversity
- stay away from questionable sites, or visit through a sandbox environment
- avoid open public wireless and other hostile environments
- in some cases, assume the worst!

Links

- Secure Programming for Linux and Unix HOWTO
http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/
- OSSTMM - Open Source Security Testing Methodology Manual
http://www.isecom.org/osstmm/
- Tor - https://www.torproject.org
- webscarab/paros web proxies
- nmap/nessus vulnerability scanners
- kismet/netstumbler(Windows)/aircrack-ng (wifi)
- wireshark/ettercap network analyzers/sniffers
- backtrack - www.remote-exploit.org/backtrack.html

Stay informed: www.securityfocus.com (IT Security portal)

thank you for your time!

Slides will soon be available at

https://unweb.me