WELCOME TO:

ADVANCED PENETRATION TESTING

SME: Timber Wolfe @lonegray

CYBRARY.IT

SO YOU WANT TO BE ADVANCED?

- You have to learn the tools you are testing from the admin and engineering perspectives!
- This is going to take time and tenacity
- Not for the faint of heart!
- You are going to have questions along the way!
- You have to learn some scripting

- **Kali is a Vulnerable OS!**

SCOPE OF PENETRATION TEST (DOCUMENT THOROUGHLY)

- **Wired LANs only?**
  - Only this process?
  - Remote SKIDs?
- **Wireless Networks?**
  - Zigbee
  - WIFI (WIFI Honeypot)
  - Bluetooth? (Ubertooth one)
  - HAM
  - Others?
- **All services on All Ports?**
- **GRE Routing of IPs for honeypot usage**
- **In and off limits?**
- **Major Concerns of penetration testing?**

LEGAL CONCERNS TO ADDRESS IN A CONTRACT

- What if you find illegal content?
  (Child Porn, Classified Documents, etc…)
- Rules of Engagement
- What if your testing brings down the network?
  - Are you working on critical infrastructure?
  - Hospital?
- What if you leave 'something' behind?
- Wall of Sheep and employee Agreements
- Storage of files and network traffic

Address these and other concerns in the pentest contract and or make your employer/area manager aware of these concerns.

CYBRARY.IT

Valuable Reference Books

- Gray Hat Python
- Violent Python
- Advanced Penetration Testing in Highly Secured Environments
- Web Hackers Handbook 2nd Edition
- www.safaribooksonline.com

TOOLS & FRAMEWORKS

Useful tools, frameworks -
deployable and forgettable
(i.e.: can be left in the secured network)

GOOGLE BOOKMARKS

- Bookmarks.google.com
- This can be used to keep track of all of the URLs we will be visiting and covering
- May be used for documentation after the penetration test has been performed

MAGIC TREE

- Penetration Test Data Collection and Reporting Tool
- Java Application
- Applications/BackTrack/Reporting Tools/Evident Management/magictree
- XML data imports and has XSLT transforms for many popular formats:
  - NESSUS
  - Nikto
  - NMAP
  - BURP
  - Imperva Scuba
  - Open VAS

DRADIS FRAMEWORK

- Information Sharing Framework
  (geared for pen testing and vulnerabilities)
- Applications/BackTrack/Reporting Tools/Evidence Management/Dradis
- http://dradisframework.org/
- Learn to backup your databases!
  - Mysqldump –A –u username –p > filename.sql
  - Lots of tools on sourceforge.net

PRIVATE INTERNET ACCESS (PIA)

- Why?
  - IDS Tests (does it flag romanian connections)
  - Does a particular server act differently when it is hit from a particular IP space?
- How?
  - https://www.youtube.com/watch?v=fHhbuHFGvcI
- Costs: $50.00/Year Max
- Download Speed Estimates: ~4Mb
- Blinds the ISP and Eliminates Restrictions
- Flexibility
  - Can be used on just about any device
  - Utilizes Open VPN

DIG (1 of 2)

- Zone Transfers (AXFR):
  - Dig @ns1.example.com example.com axfr
- Listing Bind Version:
  - Dig +nocmd txt chaos VERSION.BIND ns1.example.com +noall +answer
  - Dig +nocmd txt chaos VERSION.BIND @ns1.example.com +noall +answer
- Reverse DNS Lookup:
  - Dig +nocmd +noall +answer –x.y.z.a

(Lab Time: Perform a zone transfer)

DIG (2 of 2)

- Dig +trace example.com
  - Note serials
  - Note Paths (can monitor these for changes)
  - Batching with DIG:
  - Make entries, line by line, in a txt file
  - Dig –f inputfile.txt
- www.robtex.com (LAB Time)
  - Use to validate commands in DIG
  - Use via Python Requests Library

BIND and DNS

- What else can you get from DNS? (Internal IPs)
- Have you ever setup a DNS server?
- What are some other DNS server besides BIND, why is bind the most popular?
  - Bind receives a lot of coding time and quick response updates and scrutiny (ie: hacking)
  - Lab time – how do we obtain a list of DNS servers? http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software
- Do you want to configure a DNS record?
  - What does an internal DNS record look like?
  - Any surprisingly disparate records? (make sure the records have not changed, should be monitored for changes constantly) HUUUUGE corporate security issue!

FIERCE – DNS BRUTE FORCING TOOL

- http://ha.ckers.org/fierce/
- Looks up Targets DNS servers via locally specified DNS server, then switches to target DNS servers.
- Attempts to dump SOA records
- Begins guessing names common across many companies.
- https://www.youtube.com/watch?v=Sgs6p0DqE4I

SHODAN

- www.shodanhq.com
- **Indexes:**
  - HTTP
  - FTP
  - SSH
  - Telnet

Look at writing your own SHODAN in Python for LAN usage.

UNICORNSCAN

- **Unicornscan**
  - apt-get install Unicornscan
- **Fast**
- **Light Weight**

There are a plethora of really good scanners out there. Keep in mind that scanners can have their own indicators and the traffic may be null routed when running them. Always try more than one. Always look at samples of your own traffic!

ADVANCED NMAP

- SYN Scan: sudo nmap –sS x.y.z.a
- TCP Connect Scan: nmap –sT x.y.z.a (not advanced, this is done all the time)
- Sudo nmap –sU
- Null Scan: Probing with TCP
- FIN Scan: Solicits TCP ACK scan (for targets behind firewalls)
- Christmas Scan (URG, FIN, PSH) Sudo nmap –sX x.y.z.a

ADVANCED NMAP (CONT.)

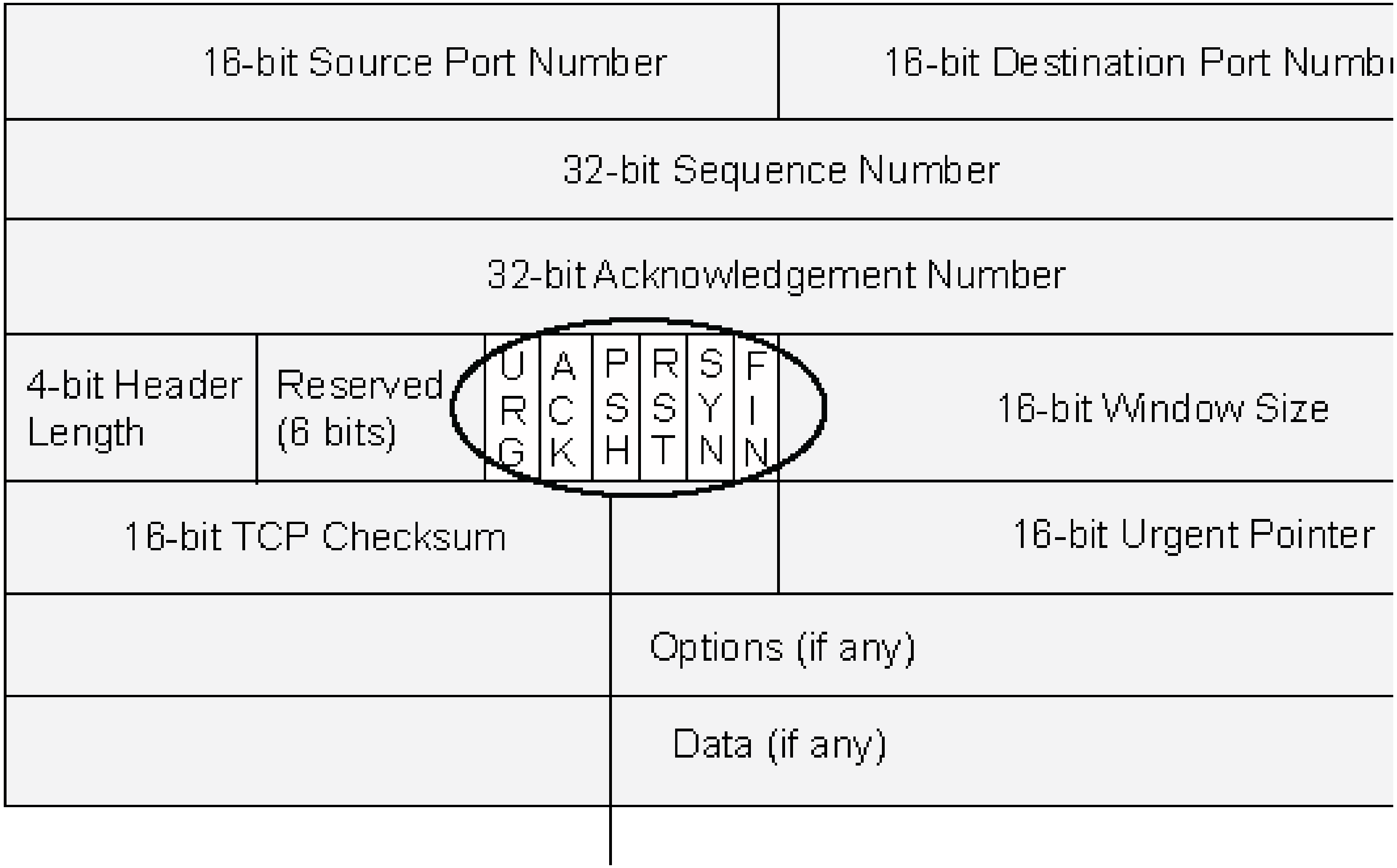
- **Sudo –scanflags ACKPSH x.y.z.a (can add more)**
  - TCP Flags: SYN, ACK, RST, PSH, URG, FIN
- **Nmap –sA (looks for firewall, filtered ports)**
- **Sudo Nmap –sO x.y.z.a (longer, target yields protocols, server state)**
- **Raw TCP Packets: nmap –send-eth x.y.z.a (sends a raw TCP packet, naturally implied)**
- **Raw IP Packet: nmap –send-ip x.y.z.a (sends a raw IP packet, naturally implied)**

ADVANCED NMAP (CONT.)

- **What is a SYN scan?**
  - AKA: Half scan
- **FIN scan**
- **What is a NULL scan?**
- **What is a Christmas Scan**
  - AKA: xmas scan
- **ACK scan? (Fast)**
- **ICMP Echo Request Ping**
- **TCP Window Scan**
- **Idle scan (more complex) (Page 92) http://nmap.org/book/idlescan.html**

CYBRARY.IT

NMAP (TCP FLAGS)



16-bit Source Port Number								16-bit Destination Port Numb
32-bit Sequence Number								
32-bit Acknowledgement Number								
4-bit Header Length	Reserved (6 bits)	URG	ACK	PSH	RST	SYN	FIN	16-bit Window Size
16-bit TCP Checksum								16-bit Urgent Pointer
Options (if any)								
Data (if any)								

None of the flags is set.

NMAP (FIREWALL DETECTION)

- **When you see responses like “Filtered” then you know you have some kind of a stateful FW.**
- **What is a stateful FW?**
  - Keeps track of Sessions
  - Allows outgoing connections (ZeuS)
  - Performs deep packet inspection
  - Gov Usage (required in gov environments)
  - Not common in industrial environments that are aging
  - Common in enterprise environments
- **Why do we care about this (finding a FW)?**

NMAP (CUSTOMIZING)

- NSE – NMAP Scripting Engine
  - **Do NOT blindly run scripts that come with NMAP on production networks!!!!! Especially in industrial and highly trafficked networks**
- nmap --script-help
- nmap --help
- Locate *.nse (/usr/share/nmap/scripts)
- nmap --script-help “banner.nse” (Lab Time)
- http://Nmap.org/nsedoc / nmap-script-updatedb
- Do we have programmers in house?
  (if so cover scripting further if not leave it to
  them to copy and paste functionality)

Note: in man pages beware the -- in MS products is auto converted to –
(dash dash converted to one long dash)

SNMP

- Locate *snmp*.pl
- apt-get update
- Mib = ? (Management Information Base)
  Entity database for SNMP
- MiB = Medibyte
  (don’t confuse them and know the difference)
- May be enabled on any type of device! While disabled on most ‘systems’ always try it on FWs and devices
- onesixtyone (lab time) (replaces snmpenum.pl)
- snmpcheck (lab time)

APT / YUM (LINUX 101)

- apt-get install xyz
  Install xyz app
- apt-cache search xyz
  Search the cached repo list on this machine for xyz
- apt-get update
  Update the repository cache to get a current list of repository entries, ie: update our cache with the mirror.
- yum search xyz
- yum install xyz
- yum update
- dpkg --get --selections (to view installed packages)

MYSQL

- **2 parts: Client/Server**
  - Do we need to cover this?
  - Colleges try to prepare the student to be well rounded, that is what is required here.
- **Administrator Tools:**
  - phpmyadmin
  - SQL Pro (OS X)
- **mysqldump –u –p –A > yyyymmdd.sql**

POSTGRESQL

- **apt-get install postgresql**
- **sudo su postgres –c psql**
- **/etc/init.d/postresql start | restart | stop**
- **Systemctl start | restart | stop postgresql.service**
- **Type: psql (if you get error ‘root’ DNE; su postgres)**
- **‘\?’   ‘\h’   ‘\q’=exit   (psql help and SQL Help)**

- **Postgresql crash course:**

http://www.itworld.com/data-centerservers/196745/crash-course-postgressql-part-1?page=0,1

CYBRARY.IT

HAPROXY

- **Load Balancing Tool**
- **Be sure nothing else is running on port 80 before starting this daemon**

EVASION TECHNIQUES

How hackers fly under the radar and make administrators work for it!

Enumeration Avoidance

- **Naming Conventions**
- **Port Knocking**
- **Trigger Points (Honeypots, Canary)**
- **SNMP Lockdown**
- **Hiding in a sea of traffic and decoys (think DDoS)**
- **Obfuscation**
  The longer it takes to find stuff the better the odds they will trip IDS and or get noticed. Keep this in mind for recommendations.
- **Naming Conventions**
  - Systems
  - Servers
  - DNS

HASHING

- Getting by whitelists
- MD5, SHA256/SHA512, Whirlpool, Tiger
- Do we know how to use them?
- Do we need to cover this?
- One way or Two way?
- Rainbow Tables (show lists on TPB)
- Collisions!
- http://www.mscs.dal.ca/~selinger/md5collision/
- Your customers will fear you for this!
- Incredibly Important to know about this!

OTHER METHODS

- **PIA (Discussed under tools)**
- **7 Hops Min. in Real Life**
- **Faking your MAC Address (Tumbling)**
- **Verify your traffic before using it in production, you never know where those ‘lists’ will end up. This is INCREDIBLY important.**

Pen Testing Training and Honing

Honing the skills

Exploitable Systems and OSs for Practice 1

- http://www.rapid7.com/resources/free-tools.jsp
- http://www.offensive-security.com/metasploit-unleashed/Requirements
- http://www.amanhardikar.com/mindmaps/Practice.html
- http://www.dvwa.co.uk/
- http://www.r00tsec.com/2011/02/pentest-lab-vulnerable-servers.html
- http://pwnos.com/
- http://ghostinthelab.wordpress.com/2011/09/06/hackademic-rtb1-root-this-box/
- http://www.kioptrix.com/blog/test-page/
- https://www.owasp.org/index.php/Category%3aOWASP_WebGoat_Project
- http://www.irongeek.com/i.php?page=mutillidae/mutillidae-deliberately-vulnerable-php-owasp-top-10
- https://www.pentesterlab.com/exercises/
- https://www.mavensecurity.com/web_security_dojo/
- http://www.pynstrom.net/

Exploitable Systems and OSs for Practice 2

- http://sourceforge.net/projects/lampsecurity/files/
- http://www.neildickson.com/os/
- http://security.stackexchange.com/questions/1735/servers-for-penetration-testing/1739#1739
- http://www.felipemartins.info/2011/05/pentesting-vulnerable-study-frameworks-complete-list/
- http://www.irongeek.com/i.php?page=security/wargames
- http://www.hackthissite.org/
- http://smashthestack.org/wargames
- http://www.astalavista.com/
- http://www.governmentsecurity.org/forum/topic/15442-war-games-server-rules-intro/
- http://overthewire.org/wargames/
- http://www.krash.in/bond00/pWnOS%20v1.0.zip
- http://www.damnvulnerablelinux.org/
- http://www.bonsai-sec.com/en/research/moth.php
- http://www.oldos.org/

Remote Exploitation

Demonstrating discovered vulnerabilities

are actually exploitable

Make sure it is in scope!

EXPLOIT DB

- **http://www.exploit-db.com/**
- **Contains POC code and the exploits**
- **(Lab Time) – Lets do the walk through in the book.   PAGE 126**
- **Virus Share**
- **BE 100% SURE OF YOUR TARGET!**
- **Coders in the room?**
  - Do we want to look at some of these?
  - Any questions?

LEARN TO EXPLOIT EVERY SERVICE

- **Look in /etc/services and learn to exploit every one of these services**
- **Learn to pull a list of vulnerabilities for each of these services**
- **Learn remediation, you will often be asked to do remediation**
- **Lets look at the architectures the exploit-db reflects /usr/share/exploit-db/platforms**
- **Whew – okay done with all of that, now what**
  - Siemens
  - AB
  - Rasberry PI
  - Detect WIFI Pineapple / Can I destroy it?
  - Routers/Switches?

DELIVERY SYSTEMS

- **Drive By Downloads**
- **Watering Hole Attacks**
- **Direct Upload via FTP/TFTP**
- **Email**
- **Conflicker Worm (without replication)**
- **Metasploit (manual)**
- **MITM Intercept**

PASSWORD LISTS

- **May be generated with some work and time.**
- **May be downloaded (4TB repositories)**
  - Use PIA to facilitate the downloading with uTorrent (Micro Torrent)

- Keeping in mind these lists are TBs in length, you need a beefy machine to facilitate usage of these files.

THC HYDRA (LAB TIME)

- https://www.thc.org/thc-hydra/
- hydra
- xhydra
- Lets take a look at the services list: https://www.thc.org/thc-hydra/network_password_cracker_comparison.html
- Comparison of Hydra/Medusa/Ncrackhttps://www.thc.org/thc-hydra/network_password_cracker_comparison.html
- Password List Generator: http://digi.ninja/projects/cewl.php

METASPLOIT FRAMEWORK (PAGE 148)

- **msfupdate**
- **msfconsole**
- **Uses PostgreSQL (by default)**
- **/etc/init.d/metasploit start|restart|stop**
- **Systemctl restart|start|stop metasploit.service**

- **Watch –d ‘lsof –nPi | grep LISTEN’ (look for listen on 3750)**
- **Two way to access it:**
  - https://127.0.0.1:3790
  - Msfconsole

Web Application Exploitation

More Tools and Methodologies

In the spirit of Finitus

BACKGROUND

- **Should learn web servers**
- **Default configurations of all daemons involved (Databases, Name Servers, Web Servers, mail servers, Frameworks, Scripting Languages)**
- **How to use and configure the daemons**
- **Attack default configurations, left over web files (phpinfo.php), etc…**
- **Understand how MTUs/MTAs work: Sendmail, store and the email workflow.**
- **The attackers are after data, the penetration tester has to know where it is stored and flows to understand where to test and look for it being exposed**

HTTPS://WWW.PFSENSE.ORG/

- **Open Source Firewall**
- **May be used to create a WAF**
  - WAF = Web Application Firewall
  - What do these do? (See slide notes)
  - WAFs are very expensive
  - Require extensive testing and research
    (Add $ to the estimate with a specific subsection for this!)

PRACTICE, PRACTICE, PRACTICE

- **http://www.irongeek.com**
  (see slides above with vulnerable systems)
- **Kioptrix is used in the book here**
  - Page 161
  - Kioptrix Level 3 (version 1.2)
  - Increasing difficulty through each level accomplished
- **Are you aware of the 'revert' feature of VMWare, Virtual box?**
- **Are you aware of the VMWare Clone feature?**
- **Do we need to cover Virtual Machines?**
  VMWare Fusion, VMWare Workstation, Virtual Box?
- **VM System Requirements? (16GB RAM, 1TB HDD, Quad Core CPU)**

DHCP SERVER CONFIGURATION

- **DHCP – Distributes IP addresses to devices connecting to the network**
- **Dynamic and Static Mapping Concepts**
- **IP => MAC Address**
- **MAC => IP Address**
- **Most Popular?**
- **DHCPD (/etc/init.d/dhcpd start|stop|restart**
- **Systemctl restart|start|stop dhcpd.service**
- **UDHCPD – Busy Box implementation for Kali**
- **http://www.busybox.net/ (has a live VM)**

LOAD BALANCER DETECTION (PG. 177/178)

- Why is this Important?
- /usr/bin/lbd
- In Kali: lbd gemprinting.com (Lab Time)
- In Kali: lbd amazon.com (Lab Time)
- What is the significance of the output? (we have the list of or a target IP now)
- Not all servers are secured equally
- If you are on a LAN you can map MACs to IPs and quickly begin to filter through a sea of traffic or TBs of traffic if you are looking at a MOLOCH Store.

MORE ON LOAD BALANCERS

- **An attacker needs one server!**
- **A penetration tester needs to check and document them all.**
- **Not all servers need to be ‘popped’. An example or two here and there is sufficient proof for the customer and less risk of taking something offline and ‘undo’ work for the penetration tester (Remember to clean up infected or popped machines before your window is closed)**

WAF DETECTION

- **WAFW00F**
  https://code.google.com/p/waffit/
- (Lab Time)
- wafw00f gemprinting.com
- wafw00f amazon.com
- Actually called: WAFFIT
  (if you are a programmer this is important)

W3AF

- **Web Application Attack and Audit Framework (w3af)**
- **Great Description at the bottom of page 182**
- **Uses multiple plugins (implication is there are more, Explore this!)**
- **(Lab Time)**
- **Launch the graphical tool**
- **Look at each menu and note all of the options that need to be explored and the plethora of tools w3af is utilizing**

WEB PROTOCOL PROXIES

- **Web Proxies may be used to log traffic and activity for the reporting information required**
- **Web Scarab**
  - Lab on Pg. 196 (its long)
  - https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
  - **Note**: No longer being maintained, so that is why safaribooksonline.com is even more important to have.
- **Fiddler (OS X / Windows) http://www.telerik.com/fiddler**
- **HTTPScoop (OS X) $15.00 http://www.tuffcode.com/**

MORE ON PROXIES

- **Proxies exists for all different types of connections, not just for web traffic**
- **SSL Speedy is an example of something that traverses 443 (HTTPS) but that wont be carved or understood by an HTTPS proxy**
- **Be aware that proxies are protocol carvers**
  - They understand the protocols
  - They can dissect them, etc…
  - They are ONLY good for the protocols they understand

We cover BURP in a bit – slide 59

MANTRA (PAGE 197)

- http://www.getmantra.com/
- http://www.getmantra.com/tools.html
- **Many tools compiled into one**
- **The user has to understand the individual tools to run them**
- **Becoming stale**
- **WAPPALYZER – Identifies apps used on a page being visited. (Droopal, PHP, Jquery, etc…)**
  - Once you have this information you can use testing tools specific to those platforms.

NEXPOSE (RAPID7)

- http://www.rapid7.com/products/nexpose/
- Vulnerability Scanner
- http://www.rapid7.com/products/nexpose/capabilities.jsp
- Scanner / Reporting Tool / Auditing Tool
- I have had many instances where clients have called or forwarded me emails with an attacker showing them their vulnerabilities with a nexpose report.
- It is free!
- http://www.rapid7.com/products/nexpose/compare-downloads.jsp

NEXPOSE (RAPID7) I

- Download the VM
- (Lab Time)
- Lots of Tutorials: https://www.youtube.com/results?search_query=nexpose+tutorial

BURP SUITE

- **May be used for EVERYTHING! (Just about…)**
- **http://portswigger.net/burp/**
- **Version Differences: http://portswigger.net/burp/download.html**

- **Extensive learning curve and proxy understanding required, spend some time learning it.**

Exploits and Client Side Attacks

ADD THE C/C++ SUPPORT FOR ECLIPSE

- **Applications, Systems Tools, Add/Remove Programs**
- **Search for: eclipse, plugin for C/C++**
- **Search for: plugin for django (Python Support)**
- **To test it:**
  - Launch eclipse
  - File
  - New
  - C/C++ Project

ASLR

- **Address Space Layout Randomization**
- **Loads DL files in random places, this prevents predictable manipulation of the registers.**
- **How to turn it on and off**

BUFFER OVERFLOW

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

int main()
{
    char lstring[10];
    printf(“Enter a long string: “);
    scanf(“%s”, lstring);
    printf(“You entered: %s\n”, lstring);
    return(0);
}
```

REFERENCES

- **Smashing the stack for fun and profit**
- **Buffer Overflow Tutorial**
- **Tutorials and forums:** **http://sickness.tor.hu**

FUZZING

- Testing inputs at and beyond the bounds
- For different input types altogether
- Many different fuzzing tools (Fuzzers)
- Make note of any crashes you are able to cause and especially those you can repeat. Be sure to include the input.

FUZZME.C

```
#include <stdio.h>
#include <string.h>
int main(int argc, char** argv)
{
        bdcode(argv[1]);
        return 0;
}
int bdcode(char *bdinput)
{
        char stuff[200];
        strcpy(stuff, bdinput);
        printf(“You passed the following data to fuzzme: %s\n”, stuff);
        return 0;
}
```

KALI FUZZERS

- **SFUZZ (Pg 224)**
- **BED**
- **Peach Fuzzer**
- **Fuzz_ip6**
- **Ohrwurm**
- **Powerfuzzer**
- **Spike-generic: chunked, listen_tcp, send_tcp, send_udp**
- **dotdotpwn (Directory traversal fuzzing – great on webservers)**
- **Tons of others**

VULNERABLE SERVER (YAVS)

- http://www.thegreycorner.com/2010/12/introducing-vulnserver.html
- **Page 213**
- **Windows Based**
- **Configurable**

BRUTE FORCE EXPLOIT DETECTOR (BED)

- Extendable
  /usr/share/doc/bed/dummy.pm (skeleton file)
- Many open source and extendable tools out there
- There are also many fully extendable pythons tools out there as well.

WIRESHARK

- **What is wireshark?**
  - Protocol analyzer
  - winpcap / tcpdump are the packet capture pieces
- **Tshark – embedded non-graphical version**

PENETRATION TESTING AUTOMATION

- **Many times the WoE (Window of Engagement) is extremely finite. To combat this attack automation is used.**
- **Tools for attack automation:**
  - Fast-Track (book mentions it but its out of date)
  - Metasploit
  - SET (Social Engineering Toolkit)

BEEF

- **Browser Exploitation Framework (XSS)**
- **http://beefproject.com/**
- **May be used for ‘hacking back’**
- **/usr/share/beef-xss/beef ← cmd from tutorial**
- **There is also a daemon**
- **http://127.0.01:3000/ui (beef/beef)**
- **Locate the wiki on the main page**
- **(Lab Time) http://www.hacking-tutorial.com/hacking-tutorial/xss-attack-hacking-using-beef-xss-framework/#sthash.cJY8mF1N.dpbs**
- **Incredibly powerful**

POST EXPLOITATION

ROE (RULES OF ENGAGEMENT)

- **Are you allowed to add persistence and actually pop systems?**
- **Remember: Do not do it just for fun, make sure there is some point to the customer. Risk is assumed every time a system is touched.**

ARMITAGE

- This is a tool designed for Red Team Events like CCDC, etc…
- (Lab Time)
- Need more exploits for newer systems
- Exploit-DB exploits will work but need to be compiled (some knowledge required)
- Pivoting

OTHER KITS AVAILABLE

- **User mode root kit:** **https://github.com/linuxgeek247/rooty**
- **ZeuS 2.8:** **https://github.com/Visgean/Zeus**
- **RAT (Remote Access Toolkit) Poison Ivy:** **https://github.com/Xiobe/poisonivyscanner**
- **Exploit Kit:** **https://github.com/search?utf8=%E2%9C%93&q=exploit+kit**

Bypassing Firewalls

HPING3

- **Kali Linux/Information Gathering/Live Host Identification**
- **Network tool able to send custom TCP/IP packets and to display target replies like ping with ICMP.**
- **Used to test FW rules, Advanced Scanning**
- **Firewalk like usage**
- **TCP/IP Stack auditing**
- **Flooding**
- **Usage:** **http://sickbits.net/firewall-testing-using-hping3/**

TIMING IS EVERYTHING

- IDS systems look for patterns
- The statistical results are measured in entropy, The entropy should be kept very low
- The penetration tester should be verifying the IDS is well tuned and catching attacks, its not enough to 'just get by the IDS'
- Do not give your customers all bad news, the IT team will despise you
- Any DoS attack will cover you in IDS logs if the attack traffic has a low entropy. Work with IT not against them.

TAKE NOTES

- Note compromised machines
- Clean up all of the infections
- Use checklists

Wireless Honeypot

How to use a wireless honeypot on penetration tests

Useful for determining bad areas to setup, hunting hackers to the local LAN (i.e: where problems are reported)

ROMANHUNTER

- https://github.com/lonegray/romanhunter
- http://sourceforge.net/projects/romanhunter/?source=directory

- Open Source Python
- Can be done on embedded devices, like a pineapple or a rasberry pi
- Can be done for other protocols: ZigBee, BlueTooth, Industrial protocols, HAM Data connections, etc…
- Questions about this?

ROMANHUNTER

- This configuration uses WPA
- Passwords come from a configuration file
- Fully automatable and customizable
- Upon an Authentication it resets the password and logs the MAC address of the client. Then waits for yet another connection. It uses the PW list in a round robin fashion.
- Upon an Association nothing happens with this version. It is printed to the screen if the debugging is enabled. It should be modified to log all activity.
- AIR OS version coming soon!

UNDERSTANDING ATTACKS AGAINST SSL

CAs, Certs, Understanding the process,
Successful MITM Attacks

TERMINOLOGY

- **Shallow Packet Inspection: Looking into TCP, UDP header – the second layer. This is also called stateful Packet Inspection. (the first layer is the IP header)**
- **Deep Packet Inspection (DPI): Consists of looking at anything or everything past the stateful packet inspection.**
- **http://en.wikipedia.org/wiki/Deep_packet_inspection**

CAS

- CA = Certificate Authority
- If I have a companies Certificate on my machine does that allow them to MITM my SSL traffic?
- How does that work?
- Can I read someone elses SSL traffic if I have a cert on their machine or do I have to own the proxy or device acting as the CA?

COMMERCIAL TOOLS FOR DPI IN SSL (WE MAY COME ACROSS)

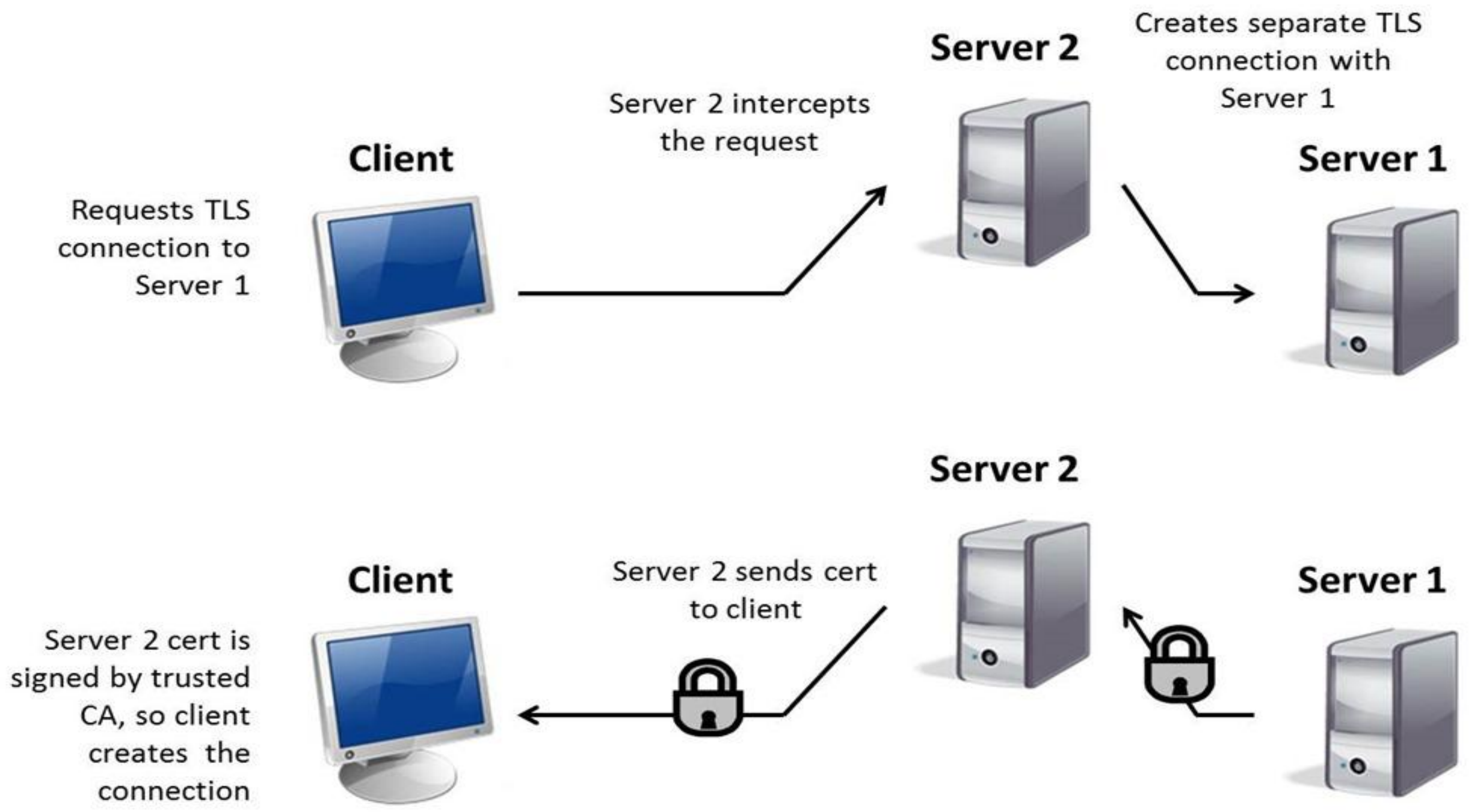
- Netronome
  (Several products for different size networks)
  - Will find SSL traffic on any port and encrypt it
  - Sonic Wall Firewalls can also do DPI on SSL but with very limited scope
- Solar Winds has a DPI on SSL solution
- Procera Networks has a DPI on SSL Solution
- There are lots more and the list is growing!
- How does the government do this?

WE CANNOT ALWAYS SEE EVERYTHING:

- **SPEDY**
  - Relatively new protocol often transmitted over SSL
  - Created by google for chrome
  - http://www.chromium.org/spdy/spdy-whitepaper
  - We need a carver for it, if your DPI engine does not understand the protocol nothing will be carved out.

- **Prevention (used self signed certs) http://www.zytrax.com/tech/survival/ssl.html**
- **d**
- **D**

SSL MITM PROCESS


Requests TLS connection to Server 1
Client
Server 2 intercepts the request
Server 2
Creates separate TLS connection with Server 1
Server 1
Server 2 cert is signed by trusted CA, so client creates the connection
Client
Server 2 sends cert to client
Server 2
Server 1

MISC. INFORMATION TO FLUSH OUT AND BE AWARE OF

Temporary Email Services

- 10minutemail.com
- 20minutemail.com
- Air mail
- Dead address
- Email sensei
- Email the
- Filzmail (24 Hours?) ← Yes!!!
- Guerrillamail
- Incognito email
- Koszmail
- Mailcatch
- Mailnesia
- Mint email
- My trashmail
- http://www.ghacks.net/2012/05/31/the-ultimate-disposable-email-provider-list-2012/

BUT – WE DO NOT EVEN USE DNS IN INDUSTRIAL ENVIRONMENTS!

- Can be used to identify misconfigurations
- Re-Use of gear from one process to another
- Incomplete configurations
- Rogue equipment
- Equipment booting off of the wrong partition on startup (common) (Elaborate here)

BANNER GRABBING ON THE LAN

- Python Scripting for LAN version of SHODAN
  - Banner Grabbing
  - Vulnerability Lookups
  - Default credential testing (automated)
- Intro to Python?
- Conflicker Worm (de-fanged)
  - Can be used to add other exploits for hunting (especially customized one)
  - She wont spread on her own (downside is she wont cross router barriers)

GRE TUNNELING

- Note TTLs (learn this!)
- Why is it used?
  - Honeypots
  - Moving IP to another location (Plant, SKID, Process, Network, Overseas)
- D
- D
- d

BASELINES

- Need to know your Aps
- Industrial Environments do not change like an enterprise environment.
- PBNJ (Lab Time?) (Page 106)
- Capture some LAN traffic for further analysis (MOLOCH/Netwitness/TARDIS)
- D
- D

USE A HONEYPOT ON THE LAN IF ALLOWED

- Will sound the alarm to scanning
  (may not have real IDS on an industrial network)
- Help find noisy devices that should be muted
- May reveal a hacker, BOT, Rogue or malfunctioning device
- Select strategic locations (networks are segmented)
- May require a GRE Tunnel back to other networks
- May require a Darknet on the LAN (requires some infrastructure)
- Can be used to validate your scanning skills and coverage
  (when the scans were performed, was the honeypot touched?) This is important for the customer and the Penetration Testing contractor.

CYBRARY.IT

GOOGLE HACKS (REFER BACK TO GHDB, GOOGLE HACKING DATABASE)

- Do they have a google appliance in house? (on the LAN)
- Inurl:ftp “password” filetype:xls
- Site:example.com inurl:ftp “password” filetype:xls
- Etc…

STORAGE CONCEPTS AND HOW TO'S

- Rosewill NAS Storage Chassis
- NAS HDDs/WD Black Label (Know the engineering!)
  - Vibration Damping and harmonic destruction of HDDs
  - Speed
  - Reliability
- SAS Arrays / JBODs
- Try to keep it portable
- Scrubbing (make it part of the agreement, what the expectations are)
- D
- d

PROFESSIONAL TOOL KITS

- Armitage: http://www.fastandeasyhacking.com/
- Cobalt Strike: http://www.advancedpentest.com/
- Metasploit: http://www.metasploit.com/
- Exploit-DB: http://www.exploit-db.com/

- Nexpose: http://www.rapid7.com/products/nexpose/
- OpenVAS Vulnerability Scanner: http://www.openvas.org/

Programmers

This section is for programmers only

Exploit-DB Compilation Examples

- Why are they not pre-compiled? (some believe by obfuscating the code kiddies wont be able to compile it (script kiddie aversion)
- Not all of them are obfuscated
- Compilers will need to be installed as well as any supporting libraries

SHELL CODE ANALYSIS

- **Find a couple of examples on exploit-db**
- **http://www.ollydbg.de/**
- **Lets take a look at what it does**
- **We can take any malware (virusshare.com) and make shellcode from it and build our own exploits**
- **This is where honeypots also come in for unknown malware and exploits they are using! Woohoo!**

GRAY HAT PYTHON

- **Defanged Conflicker Worm**
- **Delivery Mechanism for Penetration Testing**

SYMBOLS

- If you are RE files be sure to install the IDE and debugging symbols for that particular target you are working with
- Install the appropriate debugger as it will make the job easier, be sure to check that before disassembling and decompiling.
- Not all disassemblers come with complete sets of symbols

REGISTER INFO

- http://msdn.microsoft.com/en-us/magazine/cc300794.aspx
- **Registers Reference:** http://en.wikipedia.org/wiki/X86#x86_registers

REGISTER INFO

- **AL/AH/AX/EAX/RAX: Accumulator**
- **BL/BH/BX/EBX/RBX: Base index (for use with arrays)**
- **CL/CH/CX/ECX/RCX: Counter (for use with loops and strings)**
- **DL/DH/DX/EDX/RDX: Extend the precision of the accumulator (e.g. combine 32-bit EAX and EDX for 64-bit integer operations in 32-bit code)**
- **SI/ESI/RSI: *Source index* for string operations.**
- **DI/EDI/RDI: *Destination index* for string operations.**
- **SP/ESP/RSP: Stack pointer for top address of the stack.**
- **BP/EBP/RBP: Stack base pointer for holding the address of the current stack frame.**
- **IP/EIP/RIP: Instruction pointer. Holds the program counter, the current instruction address.**

SEGMENT REGISTERS

- **CS: Code**
- **DS: Data**
- **SS: Stack**
- **ES: Extra data**
- **FS: Extra data #2**
- **GS: Extra data #3**

REFERENCE

- http://en.wikipedia.org/wiki/X86_instruction_listings

Aptana Studio 3 (Python 2.x/3.x IDE)

- IDE for: Python, C/C++, others…
- http://www.aptana.com/

- Unzip Aptana… (will unzip in ./ w/out parameters)

- Now you can have syntax highlighting for python instead of just having the interpreters (2.x, 3.x)

CONCLUSION

The Fun is almost about to Start

IT'S OVER, WE LIVED! WHAT DID WE MISS?

Industrial Gear?

- SCADA Protocol Analysis
- Analyze firmware with findbugs, Fortify,
- Embedded Operating Systems

Mobile?

- Do not forget mobile devices
- Pi's?
- Arduino?
- Stamps?
- Others?
- RF
- WIFI
- Zigbee
- Lots of other wireless

WHAT IS NEXT FOR ME?

- **Programming/Scripting**
- **Crackme.de**
- **Debuggers (Analyzing Apps)**
- **Find some data and dive into it**
- **Honeypotting, start collecting data at home and on penetration tests**
- **Try and find some old SCADA gear (surplus) around some of the environments you are testing in. Often it is free or will cost you a few hours of work.**
- **Adding your own tools to Kali or customizing your own Kali.**

MALWARE SAMPLES

- **Malware Zoo**
- **Virusshare.com**
  ZeuS 2.8 on github.com
- **Malwr.com**
- **Ddecode.com (decoders)**
- **0x88 Wiki (Github)**
- **User Mode Root Kits:**
  - Rooty
  - Azazel

CYBRARY.IT

TEST TIME

TEST TIME 1

- You find you are testing a JOOMLA framework based site, what is the first recommendation you note?
- What is JOOMLA based on?
- If you are penetration testing a website and you find a form for signup that does not have CAPTCHA, what is your recommendation?
- What is CAPTCHA?
- You are analyzing a website, you find they are allowing form submissions with SSL but are NOT using a valid certificate, what do you recommend and why?

TEST TIME 2

- What is the name of an Open Source firewall?
- What is the name of a load balancer?
- What is a WAF and what does it do?

- How do you start a web server?
- How do you start a mail server?
- Where are the mail stores stored in send mail?

- How does DPI on SSL work?
- How do you prevent DPI on SSL?

CYBRARY.IT

TEST TIME 3

- **What is the purpose of honeypot usage?**
- **How can you test a security appliance for outbound C2 server connections?**
- **What is spidering?**
- **What is the difference between static and dynamic analysis?**
- **What are the kinds of penetration tests we can do to give full coverage?**
- **What tool could be used to identify an operating system passively?**

TEST TIME 4

- **What is BeEF?**