Steps of a Vulnerability Assessment Assignment

Peter Kasza @ 2018

$ whoami

- I've worked in IT Security for 8+ years
  - Security Auditor @ PRAudit
  - Testing CPEs @ Vodafone
  - Currently doing APPSEC @ Umbrella Bank
- Developer background
  - Design and implementation of a commercial log analysis framework
  - Fond of functional languages; Clojure, Haskell ♥
- Cryptography
  - Training series based on CryptoPals
  - Cryptocourse held @ ELTE

Who is a Hacker?

Who is a Hacker?

Who is a Hacker?

Who is a Hacker?

hacker: n.
[originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities
2. One who programs enthusiastically (even obsessively) or who enjoys programming
3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'.
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around.

Who is an Ethical Hacker?

ethical hacker: n.
[originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities
2. One who programs enthusiastically (even obsessively) or who enjoys programming
3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'.
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. [deprecated] ~~A malicious meddler~~ An ethical professional who tries to discover sensitive information and evaluates the security posture of a client by ~~poking around~~ mimicking a real attacker.

Security personnel in an Organization

- Red Team
  - IT Security Analyst
    - Application Testing
    - Infrastructure Testing
    - Red Teaming
- Blue Team
  - Information Security Officer (ISO)
  - Security Engineer
  - Security Architect
  - Security Operations Centre
  - Vulnerability Monitoring

Hackers by hat color

- Ethical, performs only authorized tests
- Helps businesses to protect themselves
- Tries to minimize harm

- Performs unauthorized actions, breaks the law
- Often profit oriented
- Doesn't care about collateral damage

Hackers by hat color

- Handles matters in an opportunistic fashion
- Takes traits from both sides, but to lesser extremes

Why do you need Ethical Hackers?

It's a **requirement** for doing **business**

- It can be a **regulatory** requirement (financial institutions, healthcare, etc..)
- It can be **required** by **business partners** depending on their profile

It's **needed** to **limit** operational **risk**

- Your business **depends** on **trade secrets**, **sensitive information** that you want to **protect** (confidentiality)
- Your business **depends** on the **accuracy** of certain **information** (integrity)
- Your business **depends** highly on **access** to online **services** (availability)
- Your business **depends** highly on **reputation** (technology companies, financial institutions)

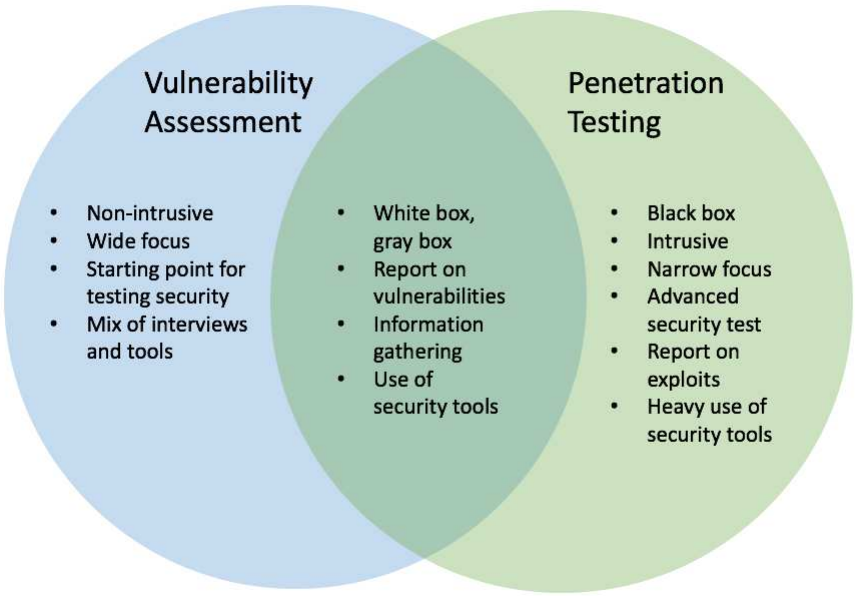
Legal trouble due to unauthorized access

Unauthorized access is a felony

- Bypassing any technical control or written restriction is punishable by law
- Defined under the Hungarian BTK. as 300/C.

What is Vulnerability Assessment (VA)?

- **Vulnerability assessment** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
- Vulnerability assessment is a well (well, better) defined process, but often confused with **penetration testing**, which is goal oriented, i.e., a pen tester makes an effort to control critical systems and acquire access to sensitive data.



Penetration test strategies

- **Targeted testing**
  Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.
- **External testing**
  This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.
- **Internal testing**
  This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.
- **Blind testing**
  A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.
- **Double blind testing**
  Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

How to perform a VA?

- Preliminary tasks
  - Presales (marketing, demo services)
  - Sales (contracts, framework contracts)
- Testing tasks
  - Scoping, project kick-off
  - Testing, vulnerability detection
  - Reporting, risk prioritization
  - Retests, ongoing support

How to perform a VA? (Preliminary Tasks)

- Presales
  - The marketing of the service to clients
  - Demo reports, previous partners
- Sales
  - Formalizing relationship, contracts
  - Frame contracts are preferred

How to perform a VA? (Preliminary Tasks)

- Scoping, project kick-off
  - What part of the infrastructure, software is in scope?
  - Are there any special requirements from the client?
  - Where is the test traffic emanating from?
  - What is the timeframe for the test?
  - When is testing permitted?
  - What types of checks are permitted?

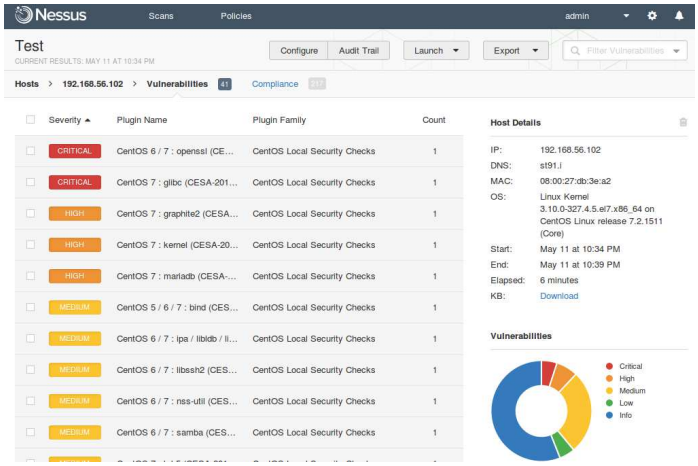
How to perform a VA? (Testing Tasks)

- Testing
  - Running the automated scanner (can be fed manually with discovery data)
  - Evaluating the results, checking for false positives
  - Testing vulnerabilities not covered by the scanner
- Reporting
  - Creating the deliverable (report) which contains verified vulnerabilities ranked by risk
- Retests
  - Consulting the client on how to fix certain vulnerabilities
  - Testing of the implemented fixes

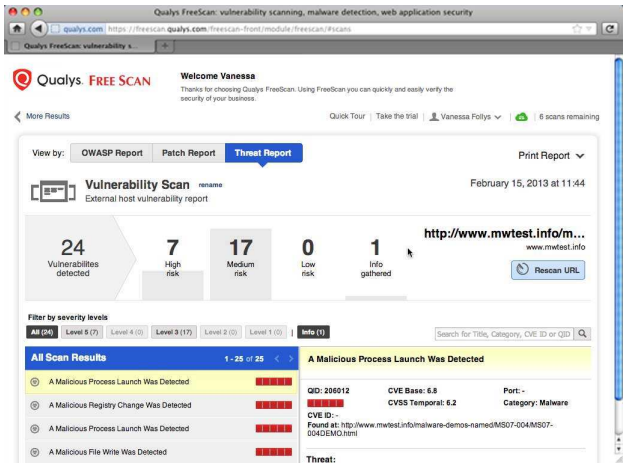
The vulnerability discovery process

- Automated Tools
  - Qualys
  - Nessus
  - OpenVAS
- Manual
  - Vendor publications, CVEs
  - Service discovery (Nmap)

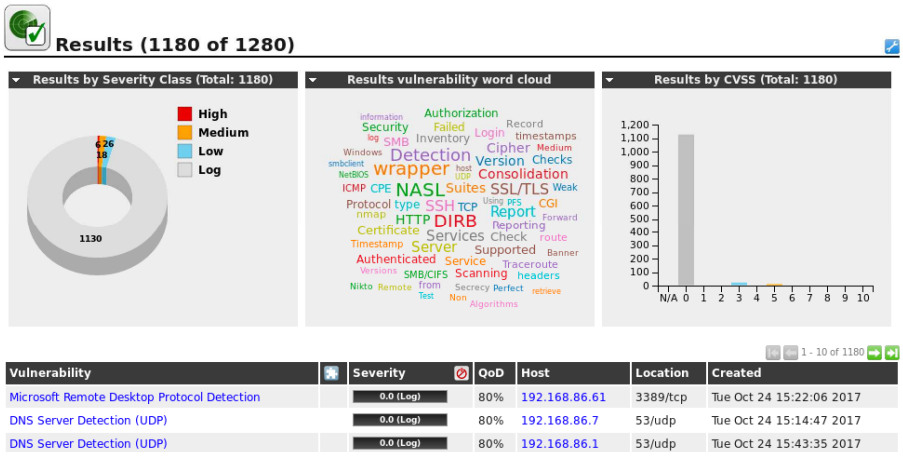
The vulnerability discovery process (Nessus)



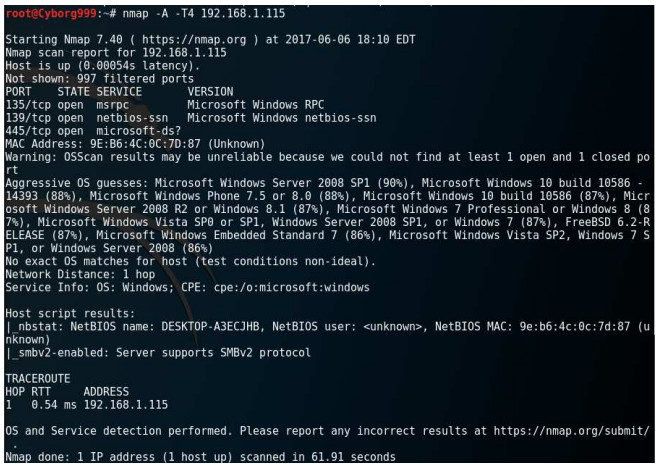
The vulnerability discovery process (Qualys)



The vulnerability discovery process (OpenVAS)

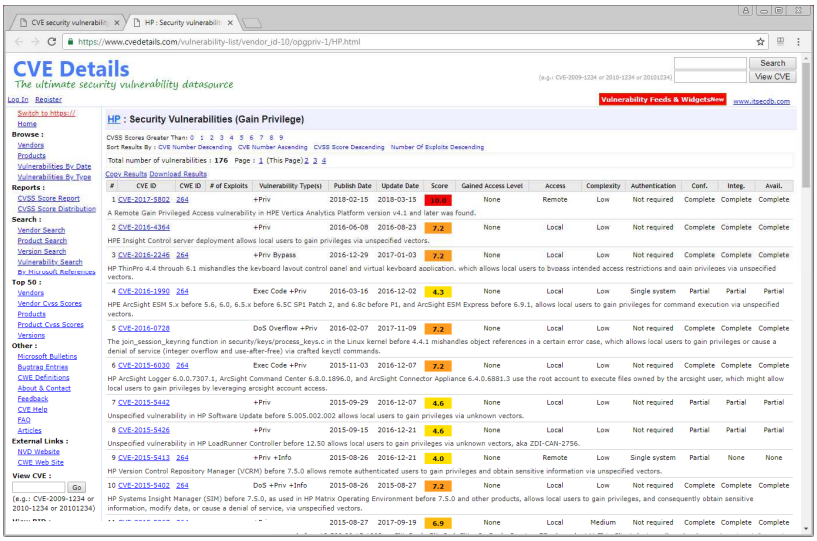


The vulnerability discovery process (NMAP)



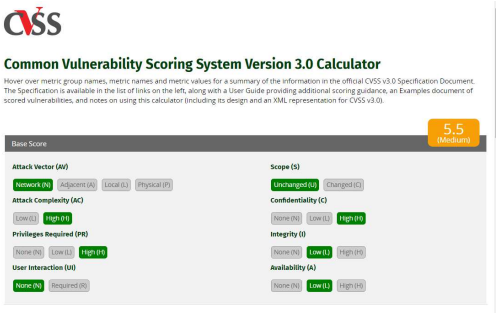
```
root@Cyborg999:~# nmap -A -T4 192.168.1.115

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-06 18:10 EDT
Nmap scan report for 192.168.1.115
Host is up (0.00054s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 9E:B6:4C:0C:7D:87 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Aggressive OS guesses: Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 build 10586 -
14393 (88%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows 10 build 10586 (87%), Micr
osoft Windows Server 2008 R2 or Windows 8.1 (87%), Microsoft Windows 7 Professional or Windows 8 (8
7%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (87%), FreeBSD 6.2-R
ELEASE (87%), Microsoft Windows Embedded Standard 7 (86%), Microsoft Windows Vista SP2, Windows 7 S
P1, or Windows Server 2008 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: DESKTOP-A3ECJHB, NetBIOS user: <unknown>, NetBIOS MAC: 9e:b6:4c:0c:7d:87 (u
nknown)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.54 ms 192.168.1.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 61.91 seconds
```

The vulnerability discovery process



Issue prioritization methods

- Qualitative
  - CVSSv3
  - DREAD
  - STRIDE
- Quantitative
  - Estimated costs for a vulnerability
  - Assigned monetary ($) values

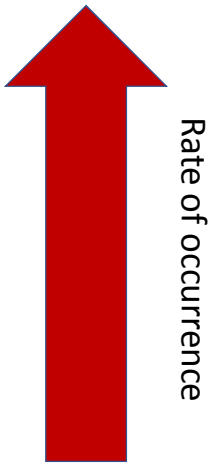


Remediation of issues

- Usually a cyclic process
  - Tester describes the issue and the remediation steps
  - The developers, vendor, sysadmin implements a fix
  - The tester retests the issue in the patched environment
- Repeated until the issue is fixed

Common types of security issues

- Configuration issues
  - Default username and password
  - Exposed admin interface
  - Forgotten features
- Implementation errors
  - High-level errors
    - Improper authorization
    - Race conditions
    - Logic bugs
  - Low level implementation issues
    - Buffer overflow
    - Heap overflow



Combining different methods

	Infrastructure	Application		
		Black	Grey	White
External				
Internal				

External infrastructure: nmap, whois, google, Nessus, ikescan, hydra, snmpwalk stb.

Internal infrastructure: nmap, metasploit, Nessus, Cain&Abel, aircrack-ng stb.

External black-box application: nikto, wikto, DirBuster, Hydra, BurpSuite, Firefox extensions, WebScarab stb.

Common protocols – (FTP, FTPS)

- Plaintext protocol (FTP) TCP/21
  - Used for file transfer (file transfer protocol)
- Complicated data flow
  - Control port, data port
  - Scanning the intranet!
- Default passwords
  - Including anonymous access
- No bruteforce protection
  - Credentials are sometimes tied into another system
    - Grants access to further resources!

Common protocols – (FTP, FTPS)

- Implementation Errors
- Path handling issues "../"
- Excessive Read, Write permissions
- FTPS – SSL related issues

Common protocols – (NFS)

- TCP/2049
- Used for file transfer (Network File System)
- Uses DNS based ACLs (showmount command)
  - If you have a DHCP server chances are you can gain access!
- No "root_squash" option is set for exports
- The "privileged ports" option is not set
- Client machines mount shares without nosuid, nodev

Common protocols – (DNS)

- UDP/53, TCP/53
- Recursive protocol for resolving domain names
- Open Recursive DNS Servers Denial-of-Service (DoS)
  - Requesting queries with source IP spoofing
  - Large response leads to amplification
- Cache poisoning attack
  - Additional information section is cached by DNS server
    - Redirecting the name server
    - Redirecting the NS record

Common protocols – (NTP)

- UDP/123
- NTP amplification attack (DoS)
  - Spoofed source IP requests
  - ~20-500X traffic amplification

Common protocols – (DHCP)

- DDNS hostname stealing
- Rouge DHCP servers

Common protocols – (SNMP)

- TCP/161, UDP/161
- Default credentials, community string
  - Modification of system parameters
- Vendor specific MIBs
  - Even code execution may be possible

Common protocols – (SSL)

- Weak Encryption Issues
  - Weak Ciphers are used by the server
    - No Cipher order is forced by the server
  - Weak protocol versions are allowed (SSLv1, SSLv2, SSLv3, TLS/1.0)
- Weak, bad certificate issues
  - Incomplete Chain of Trust
  - Weak hashing algorithm
- Weak parameters
  - Small encryption keys
  - Small DH parameters

Common protocols – (SSL)

- Protocol Issues
  - Freak (Factoring RSA Export Keys)
  - Logjam (Export DH parameters)
  - BREACH, CRIME (Compression related issues)
  - POODLE (Padding Oracle attack)
  - Heartbleed (Memory leak)

Common protocols – (SSH)

- TCP/22
- Weak Cipher, MACs, or KEX algorithm used

Common protocols – (Telnet)

- TCP/23
- Plaintext (MITM, Sniffing, Session Hijacking!!!)
- No brute force protection

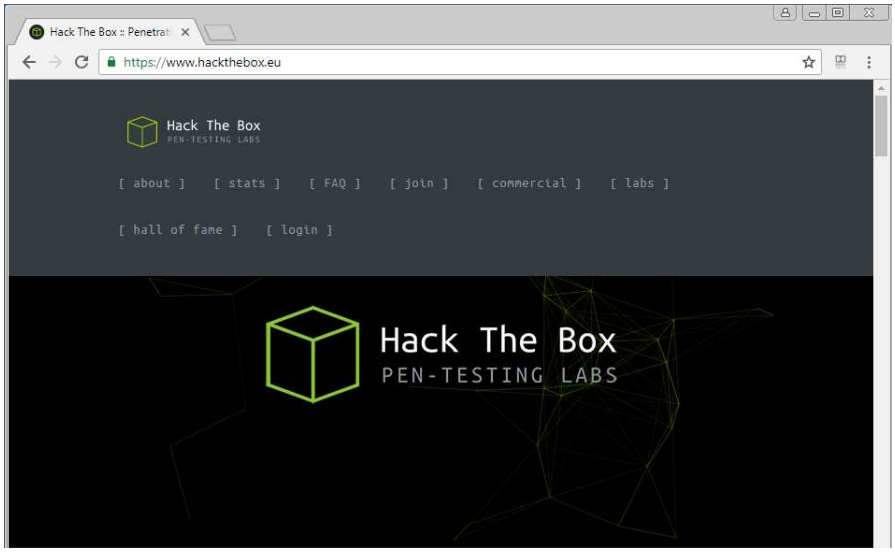
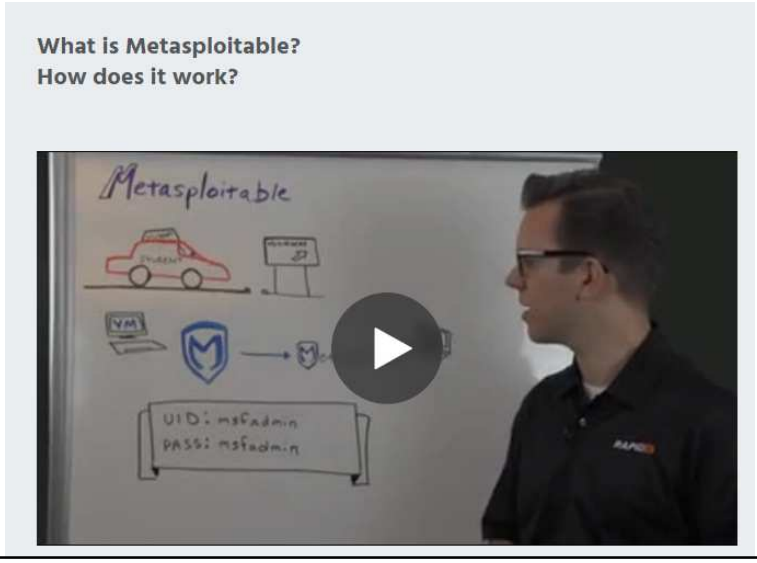
Common protocols – (HTTP, HTTPS)

- TCP/80, TCP/443
- Basic authentication is used
- Directory Traversal issues
- SQL injection
- File Upload
- Administration interface (Tomcat)
- Filename enumeration (IIS)

Common protocols – (HTTP, HTTPS)

- Basic authentication is used
- Directory Traversal issues
- SQL injection
- File Upload
- Administration interface (Tomcat)
- Filename enumeration (IIS)

Practice



Practice