


# Pentesting for fun and profit

An overview for aspiring testers and those that hire them.



## >Whoami – William Reyor

- Security Enthusiast
- Former Redteam, Current Blueteam
- Security BSidesCT Co-Founder
- LGBT supporter 
- Twitter: @OpticOpticfiber
- Blog: <http://www.topsight.net>
- NESIT hackerspace co-founder – <http://www.nesit.org>



Fairfield  
UNIVERSITY

The views expressed are my own and do not reflect those of my employer.

For those hiring a pentesting firm.

(Part 1 of 2)

>What is a pentest?

## >What is?

A pentest is live attack simulation.

Designed to:

Show a path an attacker might take.

Measure effectiveness

Help you discover where you have gaps.

# >What is?

On Paper:



## >What is it really?

- A pentest is a live attacker simulation.
- Becoming the attacker requires creativity.
- A pentest should be adaptive.
- Always try new things!



**SUCCESS**



**WHAT PEOPLE THINK  
IT LOOKS LIKE**

**SUCCESS**



**WHAT IT REALLY  
LOOKS LIKE**

>What is it really?

A pentesting framework  $\neq$  Checklist

If your pentesters are using a checklist, it's not a pentest, it's a vulnscan with verification (Hint: you can do this yourself).



## >Pentest Vs Vulnerability Assessment

Pentest

Narrative based

Uses creativity

Not metric driven

Show risk with proof

Findings are verifiable

VA

Metric Based

Uses a scanner

Not narrative driven

Completely repeatable

No creativity

## > Suggested Pre-requirements

Find answers to these questions:

- What do you have?
- Who has access?
- How do you patch it?
- When was your last vulnerability scan?

## > Suggested Pre-requirements

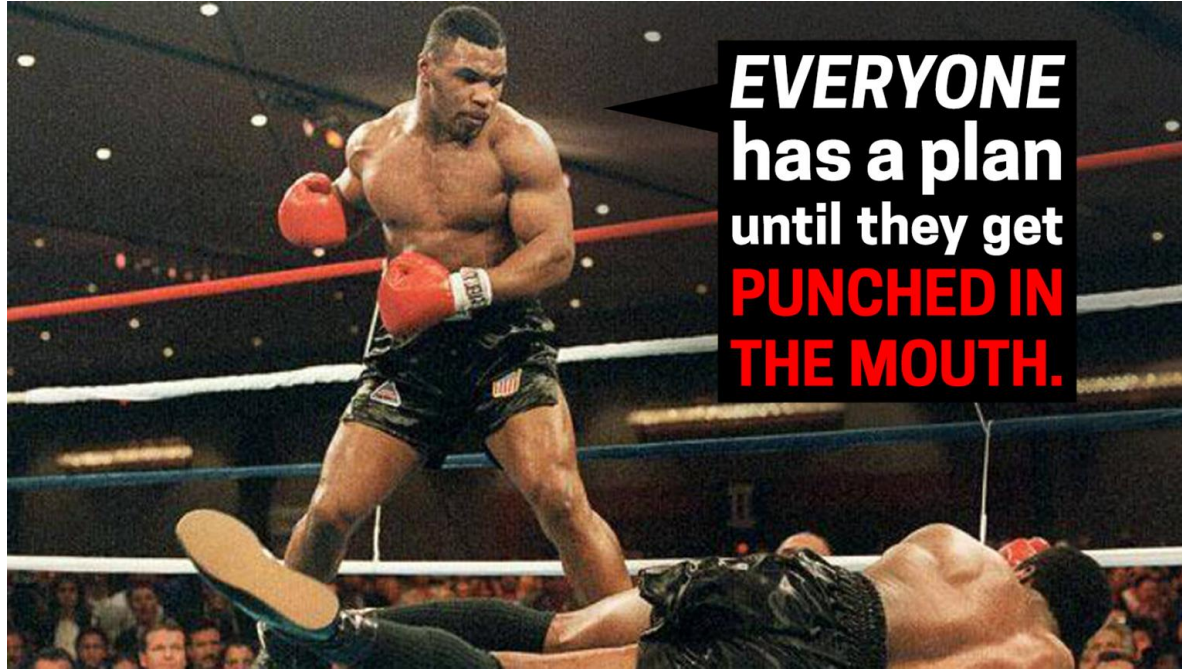
- If you haven't cleared/mitigated the criticals from your internal vulnerability scans.
  - You will likely not learn anything new in a pentest
  - Good testers will hack all the things
  - This may still be useful to you.
    - An outside consultant can demonstrate **impact**

## >Why Test?

A pentest can:

- Verify controls you have in place are working
- Create political capital to improve security
- Determine how responsive your responders are.
- Find unknown unknowns.
- Check a compliance checkbox

> Pentests offer proof





## >Choosing a firm

- Look for published research (Disclosed findings)
- Look for OSCP certification
- Review a sample of the firms report.
  - Does it look like parsed nessus results?
  - Is everything pie charts and tables?
  - Are there few if any verified findings?
  - Is the report plagiarized or an obvious copy/paste job?
  - Run!

## So you have a report (now what?)

1. Carefully review the report
2. Schedule a follow up call with the testing team
3. Challenge anything that isn't clear.
4. Use the report to plan and drive remediation.
5. Schedule follow-up verification, after things are fixed.

Repeat yearly



Questions?

(Fin. Part 1)

For those seeking to become Pentesters  
(Part 2)

## >Ethics

- Don't copy paste
- Always try and exceed expectations (try harder)
- Do no harm
  - Don't test in production
  - Treat anything you find as confidential (ie STFU)
  - Store results and supporting evidence with due care.
- Don't compromise on or water down report results

## >Quick tips for starting (Getting a job)

Plan a Security BSides (or help plan one)

Publish research (Hack stuff!)

Participate in CTF's

Bug bounties (See: hackerOne, BugCrowd)

Mentor or find a mentor

## >Some existing knowledge is helpful

Public speaking	Powershell, Shell scripting, VB
Patch management	Python / Ruby / C++
Linux	Pentesting tools (OSCP)
Windows Desktop	Security frameworks (NIST CSF)
Windows Server	Webapp testing (See OWASP)
Networking, ACLS, and routing	Electronics and RF (WiFi)
	Acting (thinking like a phish)

# >Major Phases

KICKOFF

RECON

EXPLOIT

EXFILTRATE

REPORT

# >THE KICKOFF

Establish ROE

Proof of IP ownership?

Do the guards have guns? Silent alarms? Cams?

If webapp testing, can we fuzz?

Combined attacks?

3rd party vendors and/or Cloud?

## >THE KICKOFF

Set expectations:

- For communication

- For the report you're delivering

- How involved you'll be with remediation

- How often updates will be sent, and to whom.



## >Before we start

You need to log all the things:

Time stamp all notes - (Sublime2 makes this easy)

Pipe all output from tools to text and preserve.

Make sure you get log output from everything.

Part of your deliverables should be turning over this info.

## >RECON - Passive

Seek to understand:

What is critical to the client's business?

How mature is the client's security posture?

What information is leaking?

- Social media (Facebook, LinkedIn, twitter)
- DNS, SSL, IP block ownership information?

## >RECON - Passive

Use a single piece of information and pivot!

Just listen! – wireshark - <https://www.wireshark.org>

Maltego - <https://www.paterva.com/web7/>

Spiderfoot - <http://www.spiderfoot.net>

Discovery scripts - <https://github.com/leeбайд/discover>

Shodan – <http://shodan.io>



# Spiderfoot



SpiderFoot

New Scan

Scans

Settings

About



Status Browse Graph Scan Settings Log



Search...



Type	Unique Data Elements	Total Data Elements	Last Data Element
<a href="#">Affiliate - Internet Name</a>	3	5	2015-11-08 03:00:18
<a href="#">Affiliate - Web Content</a>	3	5	2015-11-08 03:00:50
<a href="#">Affiliate Description - Abstract</a>	2	2	2015-11-08 03:00:19
<a href="#">Affiliate Description - Category</a>	34	41	2015-11-08 03:00:20
<a href="#">HTTP Headers</a>	1	1	2015-11-08 02:43:45
<a href="#">HTTP Status Code</a>	1	1	2015-11-08 02:43:45
<a href="#">Human Name</a>	1	1	2015-11-08 02:41:35
<a href="#">Internet Name</a>	1	1	2015-11-08 02:40:39
<a href="#">Junk File</a>	9	9	2015-11-08 02:54:17
<a href="#">Linked URL - External</a>	14	14	2015-11-08 03:00:16
<a href="#">Linked URL - Internal</a>	53	54	2015-11-08 03:00:51
<a href="#">Malicious Affiliate</a>	3	3	2015-11-08 03:00:48
<a href="#">Non-Standard HTTP Header</a>	1	1	2015-11-08 02:43:45
<a href="#">Raw File Meta Data</a>	1	1	2015-11-08 02:52:02
<a href="#">SSL Certificate - Issued by</a>	1	1	2015-11-08 02:44:09

# Discover.sh

By Lee Baird

## RECON

1. Domain
2. Person
3. Parse salesforce

## SCANNING

4. Generate target list
5. CIDR
6. List
7. IP, Range or URL

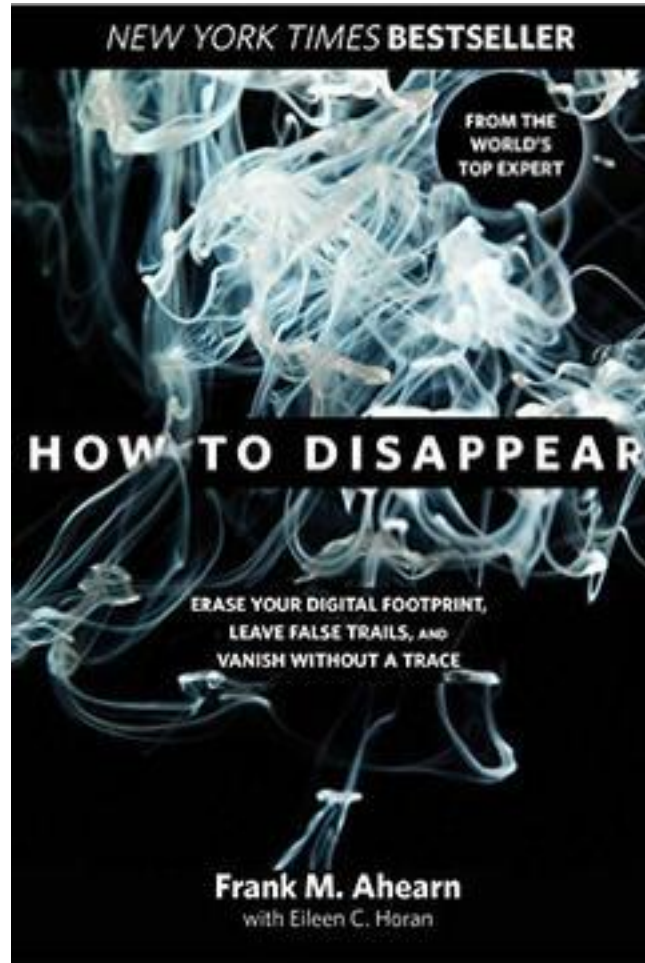
## WEB

8. Open multiple tabs in Firefox
9. Nikto
10. SSL

## MISC

11. Crack WiFi
12. Parse XML
13. Generate a malicious payload
14. Start a Metasploit listener
15. Update

# How to Disappear



## >RECON - Active

Pivot from passive recon

NMAP - <https://nmap.org>

NESSUS - <http://www.tenable.com/>

NIKTO - <https://cirt.net/Nikto2>

NETCAT - <http://nc110.sourceforge.net>

Identify critical systems, software, and vulnerable versions.



## >EXPLOIT Shortcuts (for soft environments)

OPEN FILE SHARES

DEFAULT PASSWORDS - [www.defaultpassword.com](http://www.defaultpassword.com)

COMPLETELY UNPATCHED SYSTEMS

RESPONDER <https://github.com/SpiderLabs/Responder>

IPMI - <http://fish2.com/ipmi/remote-pw-cracking.html>

# OPEN FILESHARES

Metasploit spool output to a log ie:

```
spool /root/consolelog.txt
```

use auxiliary/scanner/smb/smb\_enumshares

(Result will log to /root/.ms4/loot/)

[https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb\\_enumshares](https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_enumshares)

# >EXPLOIT

Pivot from recon, research, step, pivot.

WEBAPP - OWASP TOP 10 - <https://www.owasp.org/>

Layer 2 MITM Framework – <https://goo.gl/d9RLGn>

Google – Search for specific attack methods

Phish - <http://www.social-engineer.org>

Observe ->Form a hypothesis -> Test

# >EXPLOIT

Pivot from previous exploits

Pivot from exploited systems with “malware” / Meterpreter

Create Fully UnDetectable Samples

VEIL Evasion - <https://www.veil-framework.com/>

SprayWMI - <https://github.com/trustedsec/spraywmi>

# >EXFILTRATE

Show what's important!

Examples:

user accounts / masked passwords

Masked transaction details

Confidential documentation

Anything else the org would want to protect

# >EXFILTRATE - Examples

Show what's important!

```
epixoip@butters: ~/oci/Hashcat-plus-0.13
c164bc1e4e1aa249aa8800c779213171:www zoosk com
4e17daa83b273a8db302af87871db656:my zoosk
e6264e0b9065c4d14ed2308b6b9d2d16:zoosk password
4aa73f63e392399c5764a6d0d33475ac:zoosk pass
ce43ea398e295b89f66a9dc8654048dc:wwwzoosk com
f9976e166466d6583db1f76368d947d4:my87zoosk
f8096e2ef900e593b3fd4c0ca8f7562:ZooskpassworD
f31adf021078e2bfffdf7bcb42cba75:myZoosk2010
f1b0cac05fa05a476196ddfcb0890c2:Zooskpass123
f1540b51d93401bca292b6dcfa4e3923:4myZoosk!
f0ede158ea87f21e360bee0cca05d4f:passwordzoosk
efe8aa378322d433a055128ae686163a:myzooskx22
ef0c06008a3d2b0f96e5e19eca714f2a:310myzoosk
e7367aa59ca07128cefd61edc3f2348:myzoosk585
e31de91888e4505622d49f2ffe07b1f6:motdepasszoosk
dbc57b31aeddl4cbcd51c37429a03bcl:yi darayzoosk
d6ab272d57d61754af200efc63672lcc:myzooskpc
d4f1cb649c67cc86d866f72ba847d2d5:my58zoosk
d1629272b185035d5b396ec7bf4d4b0:jdcmyzoosk
ccd3f6732b02b904a7c413e02772128:myzooske
cc7f96582e59139ecb78b53d85729695:jimmyat zoosk
c9f1f1452bf42279c737f735e8e1b047:myZooskpass
```

```
[*] Meterpreter session 1 opened (192.168.81.128:443 -> 192
500

msf exploit(handler) > sessions -l

Active sessions
=====

Id Type Information
---
1 meterpreter x86/win32 HACKINGWIN7\malware_win7x86 @
1.129:49279 (192.168.81.129)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer : HACKINGWIN7
```

				id	username	hash
<input type="checkbox"/>				1	caesar	\$1\$50\$GHABNWBNE/o4VL7QjmQ6x0
<input type="checkbox"/>				2	cs50	\$1\$50\$ceNa7BV5AoVQqilACNLuC1
<input type="checkbox"/>				3	jharvard	\$1\$50\$RX3wnAMnRGlbgzbRYrxM1/
<input type="checkbox"/>				4	malan	\$1\$HA\$azTGIMVImPi9W9Y12cYSj/
<input type="checkbox"/>				5	nate	\$1\$50\$sUyTaTbiSKVPZCpjJckan0
<input type="checkbox"/>				6	rbowden	\$1\$50\$JJS9HiGK6sphej8c4bnbX.
<input type="checkbox"/>				7	skroob	\$1\$50\$euBi4ugiJmbplbvTTfmfl.
<input type="checkbox"/>				8	tmacwilliam	\$1\$50\$91ya4AroFPepdLpiX.bdP1
<input type="checkbox"/>				9	zamyla	\$1\$50\$Suq.MOtQj51maavfKvFsW1

# >Report

## MAJOR PARTS

EXECUTIVE SUMMARY

ANALYSIS / NARRATIVE / FINDINGS

REMEDICATION GUIDANCE

# >Report – Executive Summary

Summarize:

What you did

What you did it to (what critical systems)

What methods you used

What conclusions you can draw



## >Report – Narrative

### Technical Meat:

Tell your story of exactly what you did

What tools did you use

What systems did you pivot from

What did you recover?

What is the impact?

# >Report – Narrative

## Include Screen Shots

```
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>psexec.exe \192.168.31.1 -c gsecdump.exe -a

PsExec v1.96 - Execute processes remotely
Copyright (C) 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

info: you must run as LocalSystem to dump LSA secretsMicrosoft wireless secrets:

No interfaces found

HACKANDCRASH\2003-SERVER$:0000000000000000000000000000000000000000000000000000000000000000:bb1419957f74ae068e2
f88eb4d6bda5:::
HACKANDCRASH\Administrator$:5d567324ba3cccf81bf3ece46b279e12:001a5b3e266374c0df9
6a298f7f7419f:::
Administrator(current):500:5d567324ba3cccf81bf3ece46b279e12:001a5b3e266374c0df96
a298f7f7419f:::
Guest(current):501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
krhtgt(current):502:aad3b435b51404eeaad3b435b51404ee:607e5b12a1305f614bf83072647
79e76:::
SUPPORT_388945a0(current):1001:aad3b435b51404eeaad3b435b51404ee:f687c8c7727486c9
bba2c1caa80acd50:::
James.Brown(current):1106:7dee762647704278695109ab020e401c:85a1bacace8f32e71c491
d6d9f53a2c5:::
Bob.Down(current):1107:5d567324ba3cccf81bf3ece46b279e12:001a5b3e266374c0df96a298
f7f7419f:::
John.Smith(current):1108:5d567324ba3cccf81bf3ece46b279e12:001a5b3e266374c0df96a2
98f7f7419f:::
2003-SERVER$(current):1003:aad3b435b51404eeaad3b435b51404ee:bb1419957f74ae068e2
f88eb4d6bda5:::
TEST-SUBJECT1$(current):1109:aad3b435b51404eeaad3b435b51404ee:04a01c436e1b6a7c82
962829haa7e0f4:::
XP-MACHINE$(current):1110:aad3b435b51404eeaad3b435b51404ee:23c269413581e252f9cba
c02d9c760f5:::
gsecdump.exe exited on 192.168.31.1 with error code 0.

C:\WINDOWS\system32>
```

## >Report – Remediation Guidance

For every finding:

- Provide actionable remediation guidance

- Do not assume things you find in Vulnerability scans are usable

- Do your own research on how to remediate

The goal is to help your client better secure their systems.

Questions?

(Fin. Part 2)