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:

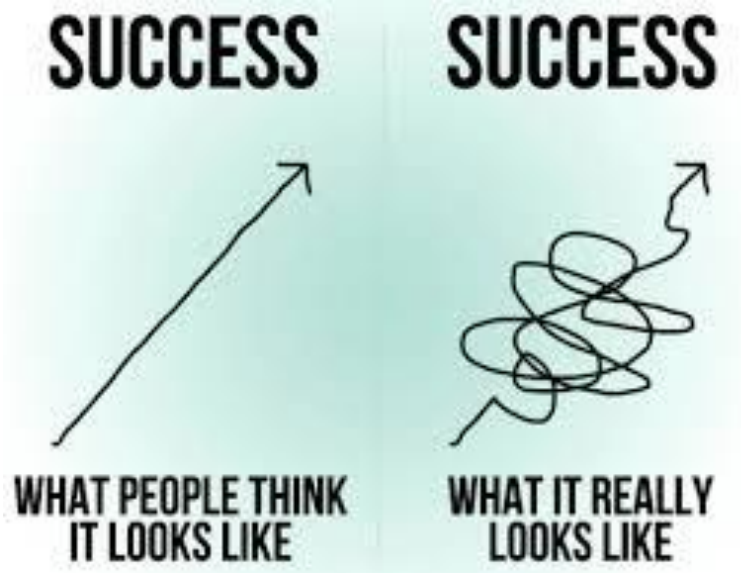
- Show a path an attacker might take.
- Measure effectiveness
- Help you discover where you have gaps.

>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!



>What is it really?

A pentesting framework ≠ 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	VA
Narrative based	Metric Based
Uses creativity	Uses a scanner
Not metric driven	Not narrative driven
Show risk with proof	Completely repeatable
Findings are verifiable	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

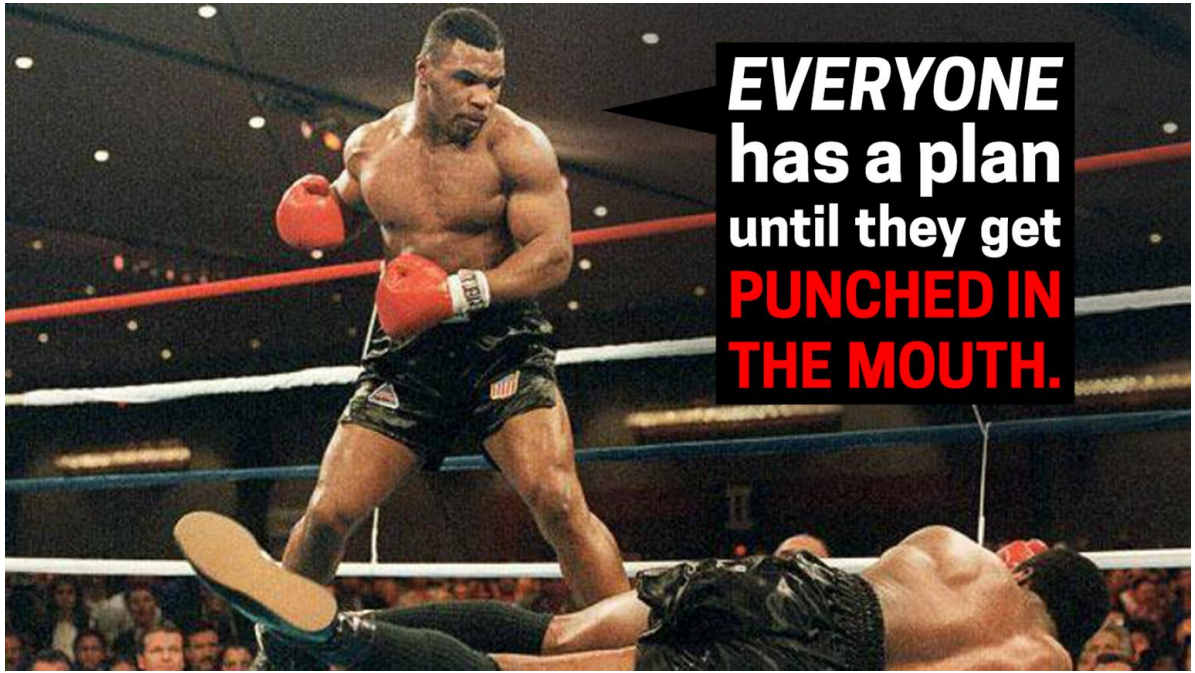
- If you haven’t cleared/mitigated the criticals from your internal vulnerability scans.
    - You will likely not learn anything new in a pentest
    - Good testers will hack all the things
    - This may still be useful to you.
        - An outside consultant can demonstrate **impact**

>Why Test?

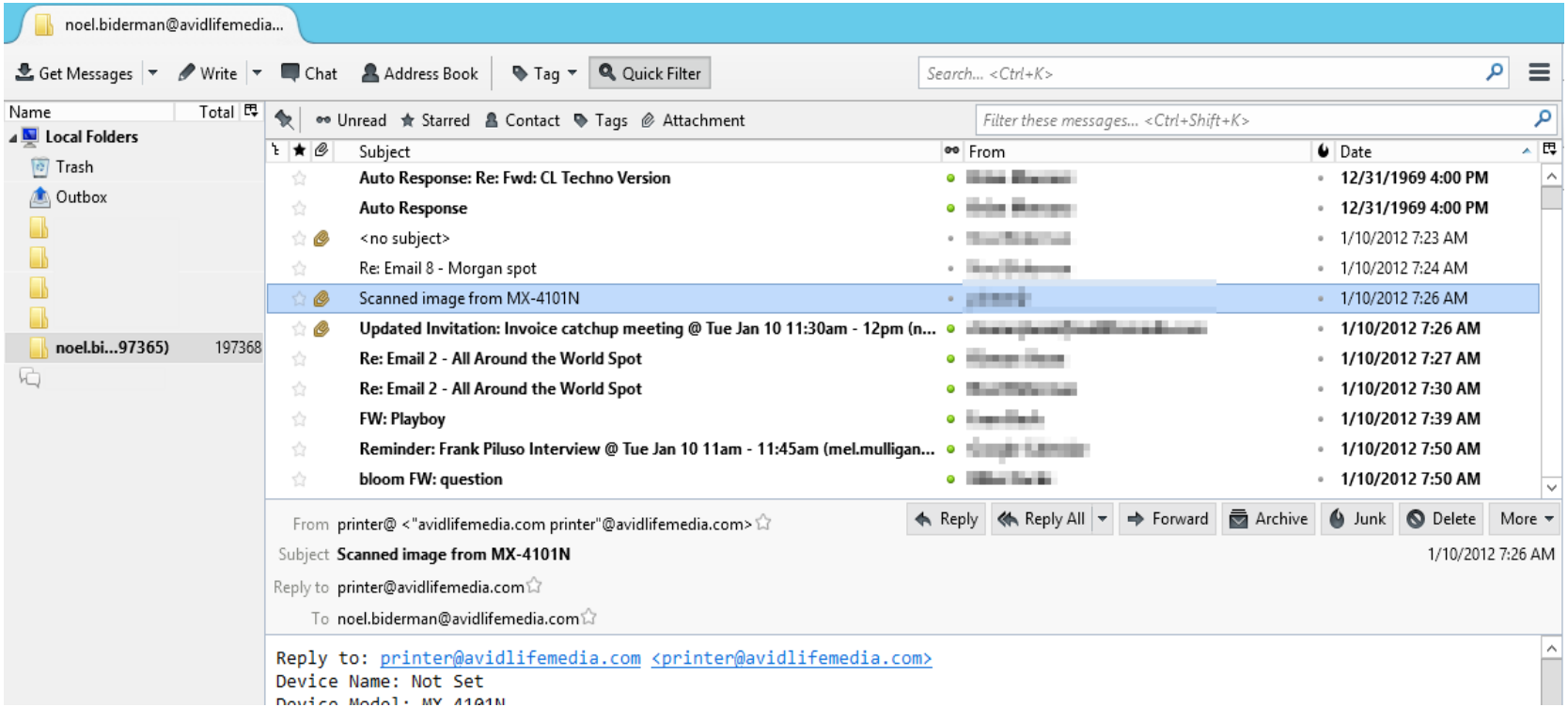
A pentest can:

- 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



> The proof



Credit: Ashley Madison.

>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

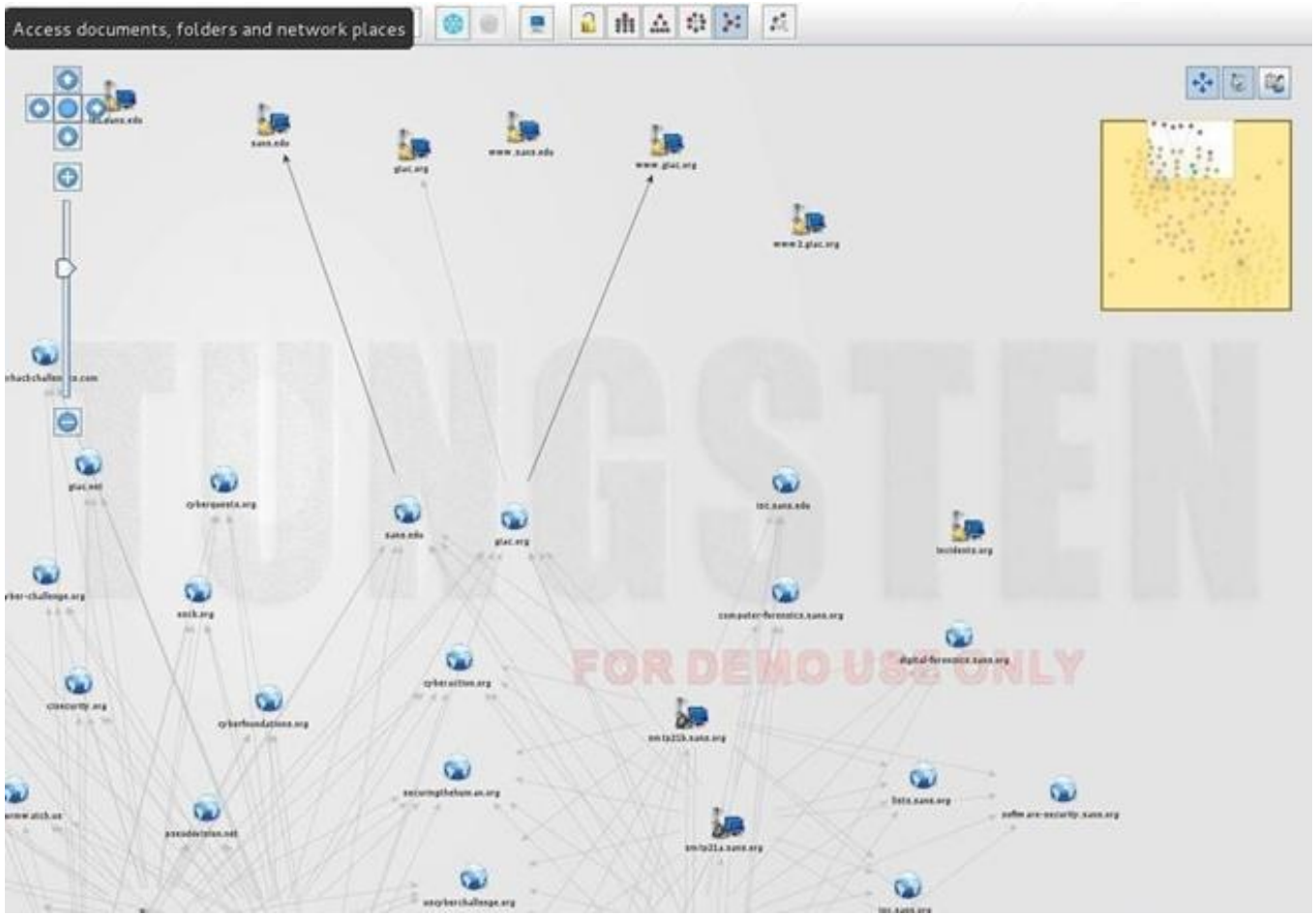
Maltego - https://www.paterva.com/web7/

Spiderfoot - http://www.spiderfoot.net

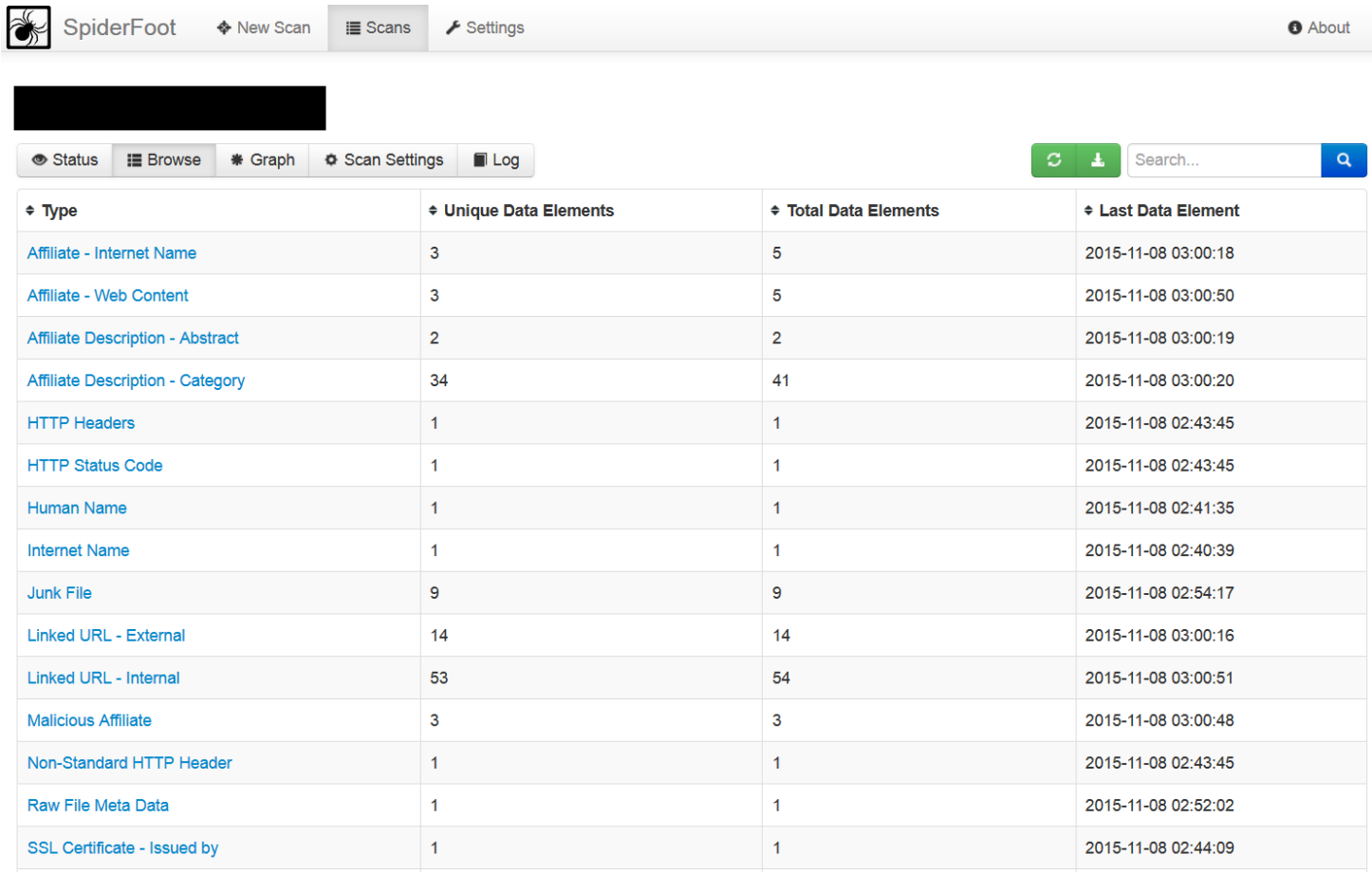
Discovery scripts - https://github.com/leebaird/discover

Shodan – http://shodan.io

Maltego


Access documents, folders and network places
FOR DEMO USE ONLY

Spiderfoot

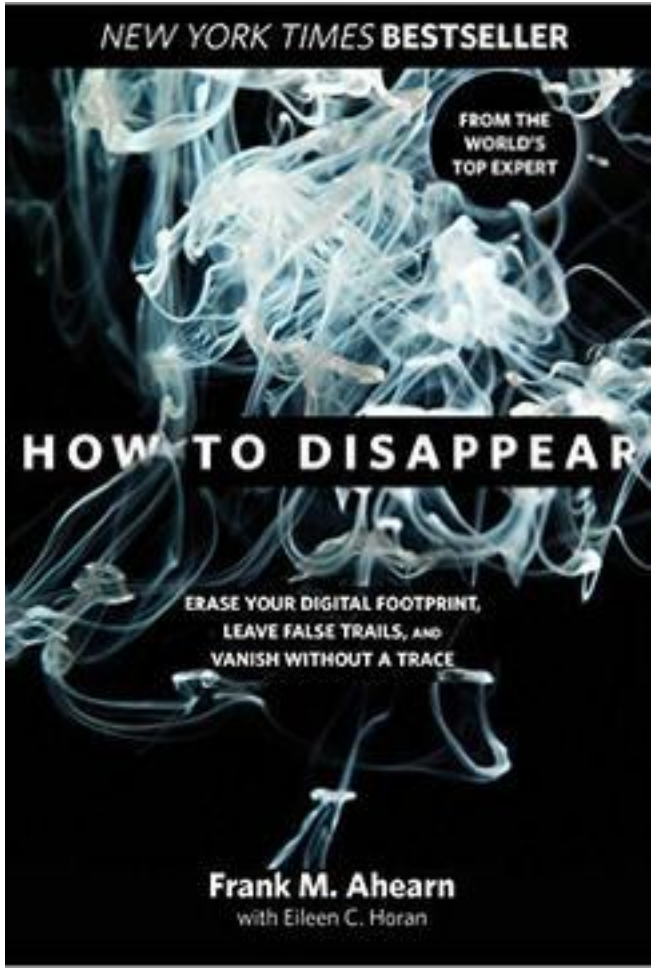


Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Internet Name	3	5	2015-11-08 03:00:18
Affiliate - Web Content	3	5	2015-11-08 03:00:50
Affiliate Description - Abstract	2	2	2015-11-08 03:00:19
Affiliate Description - Category	34	41	2015-11-08 03:00:20
HTTP Headers	1	1	2015-11-08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

Discover.sh


DISCOVER
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

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

>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

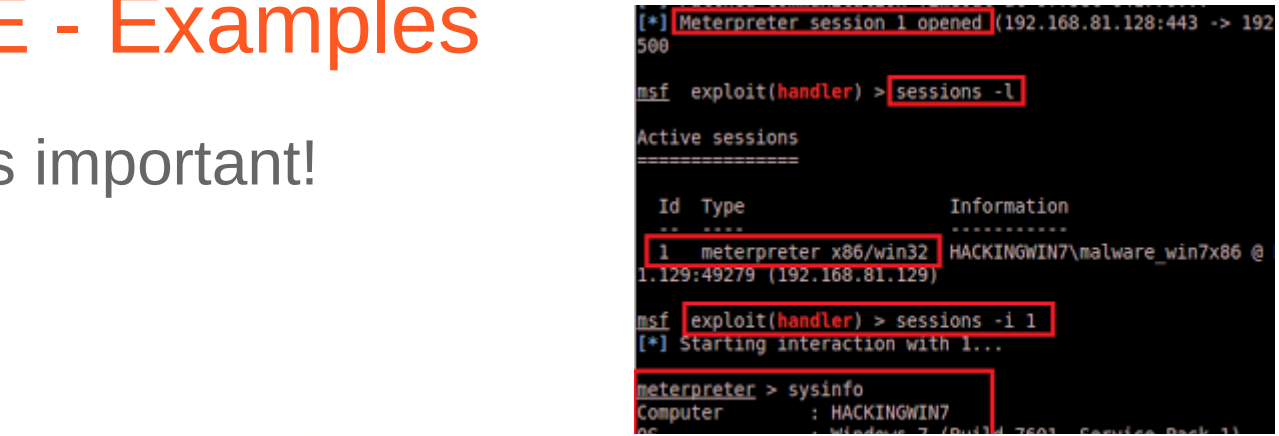
Show what's important!

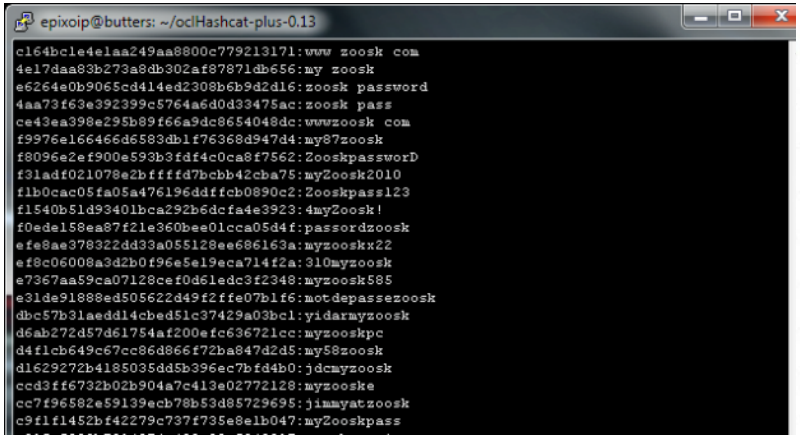
Examples:

- user accounts / masked passwords
- Masked transaction details
- Confidential documentation
- Anything else the org would want to protect

>EXFILTRATE - Examples

Show what's important!





	id	username	hash
Edit Copy Delete	1	caesar	$1$50$GHABNWBNE/o4VL7QjmQ6x0
Edit Copy Delete	2	cs50	$1$50$ceNa7BV5AoVQqilACNLuC1
Edit Copy Delete	3	jharvard	$1$50$RX3wnAMNrGIbgzbRYrxM1/
Edit Copy Delete	4	malan	1HA$azTGIMVlmPi9W9Y12cYSj/
Edit Copy Delete	5	nate	$1$50$sUyTaTbiSKVPZCpjJckan0
Edit Copy Delete	6	rbowden	$1$50$lJS9HiGK6sphej8c4bnbX.
Edit Copy Delete	7	skroob	$1$50$euBi4ugiJmbplbvTTfmfI.
Edit Copy Delete	8	tmacwilliam	$1$50$91ya4AroFPepdLpiX.bdP1
Edit Copy Delete	9	zamyla	$1$50$Suq.MOtQj51maavfKvFsW1

>Report

MAJOR PARTS

EXECUTIVE SUMMARY

ANALYSIS / NARRATIVE / FINDINGS

REMEDIATION 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

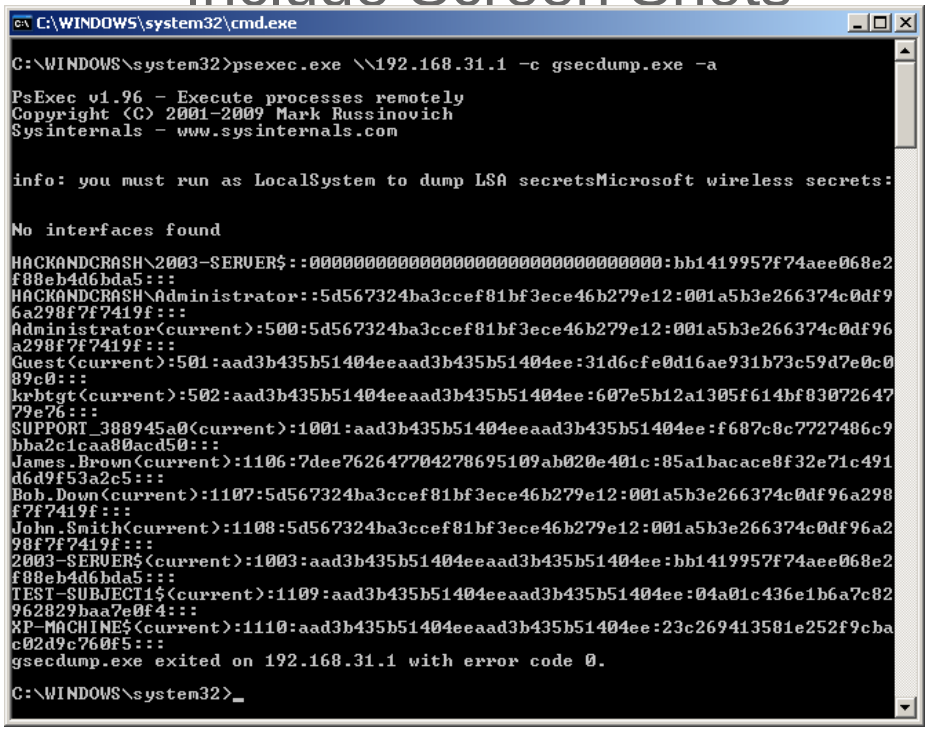
>Report – Narrative

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



>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)