SANS
Pen Test Austin

MARCH 27 – APRIL 1, 2017 | AUSTIN, TX

Courses offered:			3 Nights of SANS NetWars Experience	I Night of CyberCity Missions	Coin-A-Palooza: Your chance to earn up to 5 SANS Pen Test Challenge Coins
• SEC401	• SEC550	• SEC617			
• SEC504	• SEC560	• SEC642			
• SEC542	• SEC562	• SEC660			

sans.org/event/pentest2017

SANS HackFest
Information Security Summit & Training — November 2017

For more information: www.sans.org/hackfest

SUMMIT
2-DAYS
20+ SPEAKERS
PANELS

DIGITAL BADGES

TRAINING
6-DAYS
PEN TEST COURSES

EVENING BONUS SESSIONS:
Three Nights of
NETWARS EXPERIENCE with Coin-A-Palooza

www.sans.org/netwars

EVENING BONUS SESSION:
One Night of
CyberCity
1:87 SCALE - ICS/SCADA-ENABLED PHYSICAL MODEL CITY
Offensive & Defensive Missions

www.sans.org/netwars/cybercity

"This is my favorite event each year. We throw everything we have into it to make it special, and I do hope you decide to attend." – Ed Skoudis, SANS

SANS

PENETRATION TESTING

Attack Surfaces, Tools, and Techniques

POSTER

This poster presents:

- Tools and techniques that every security professional should know to maximize the value of your pen testing and vulnerability assessment work

- In-depth network diagrams with various attack surfaces every enterprise must defend, as well as world-class pen test techniques to assess each vector

- A detailed mind map of sites and distributions you can use to practice your skills and keep them sharp

- A list of awesome resources for keeping your skills current

- A description of the SANS Pen Test Challenge Coins for our Capture the Flag winners

- An overview of the in-depth, hands-on, skill-driven courses in the SANS Pen Test Curriculum

COIN-A-PALOOZA

Each SANS Pen Test Course includes a final full day (Day 6) of hands-on computer security challenges that hammer home the lessons taught throughout the entire course. The top winners in each course of this full-day Capture-the-Flag event receive the much-coveted challenge coin associated with the course. Each coin is unique for its associated course, with a custom logo, a special tag line, and a theme. Coins are available for SANS SEC504, SEC542, SEC560, SEC561, SEC573, SEC575, SEC617, SEC642, SEC660, and SEC760 courses, as well as the SANS NetWars Challenge. The prize coin congratulates the victors on their accomplishment and challenges them to further use their award-winning skills to make a positive difference in their workplace and career.
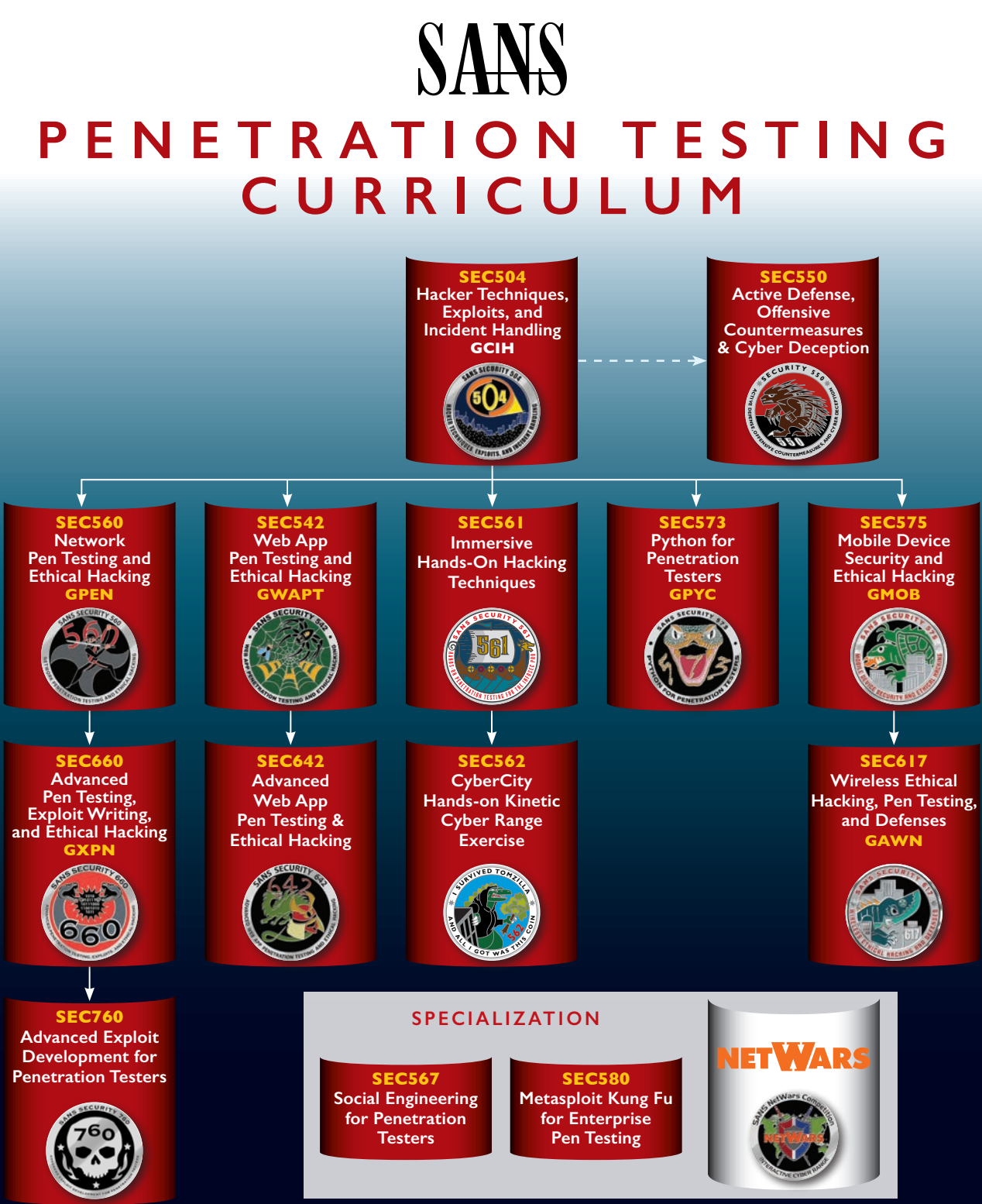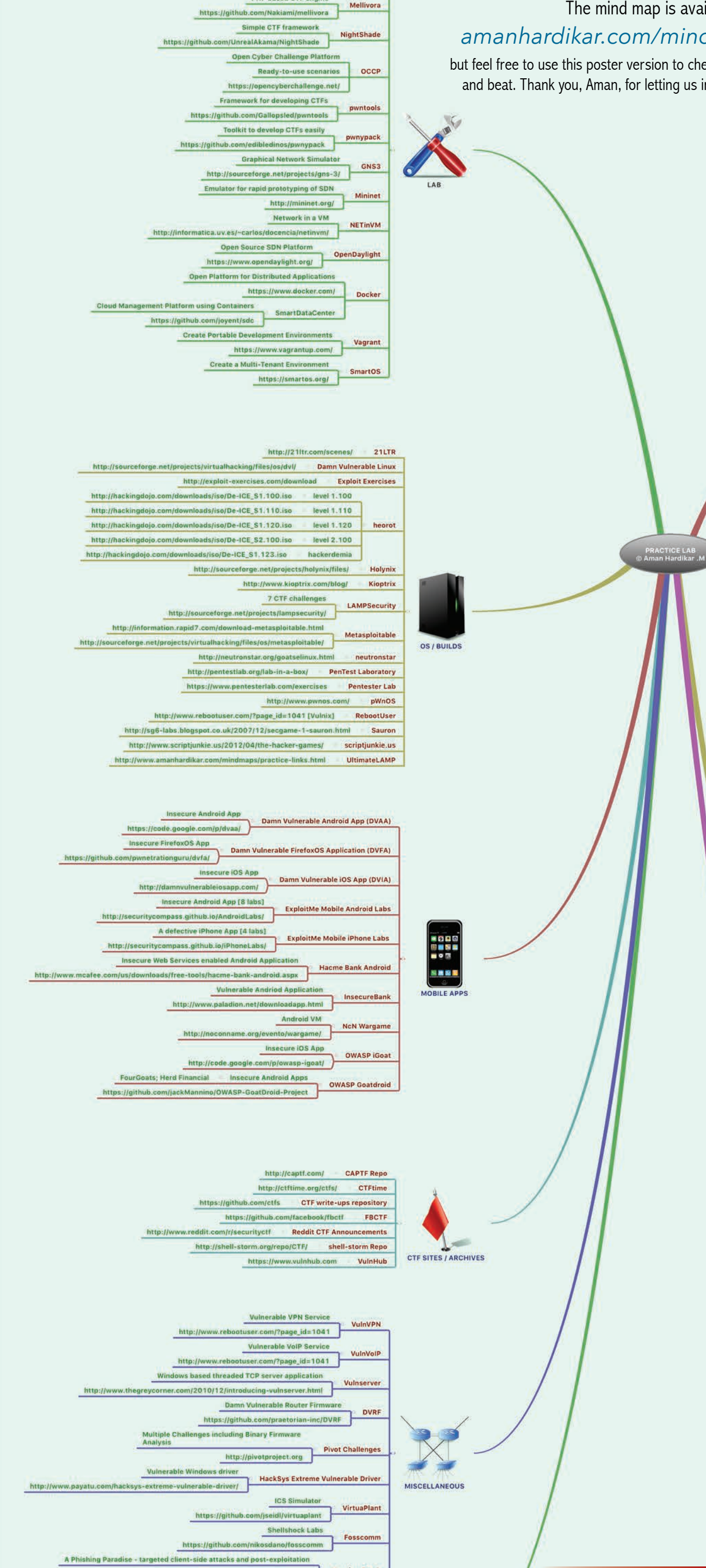
And, best of all, each coin includes a special cipher that encodes or encrypts a part of a hidden message. (Note: We have purposefully omitted the ciphers from the coin images on this poster.) The coins include all kinds of ancient, modern, and custom-created ciphers ready to challenge and delight Capture the Flag winners. Each coin encodes a single word, so you can analyze your prize and determine its secret right away. Then, as you earn multiple coins, you can crack the larger message and achieve the ultimate SANS Pen Test coin victory.

Look for our Coin-A-Palooza events at SANS Pen Test Austin and the SANS Pen Test HackFest for the chance to earn multiple coins at a single event!

SANS

PENETRATION TESTING CURRICULUM

SEC504 Hacker Techniques, Exploits, and Incident Handling — GCIH

SEC550 Active Defense, Offensive Countermeasures & Cyber Deception

SEC560 Network Pen Testing and Ethical Hacking — GPEN

SEC542 Web App Pen Testing and Ethical Hacking — GWAPT

SEC561 Immersive Hands-On Hacking Techniques

SEC573 Python for Penetration Testers — GPYC

SEC575 Mobile Device Security and Ethical Hacking — GMOB

SEC660 Advanced Pen Testing, Exploit Writing, and Ethical Hacking — GXPN

SEC642 Advanced Web App Pen Testing & Ethical Hacking

SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise

SEC617 Wireless Ethical Hacking, Pen Testing, and Defenses — GAWN

SEC760 Advanced Exploit Development for Penetration Testers

SPECIALIZATION

SEC567 Social Engineering for Penetration Testers

SEC580 Metasploit Kung Fu for Enterprise Pen Testing

NETWARS

RESOURCES

Website
pen-testing.sans.org

Pen Test Blog
pen-testing.sans.org/blog

GPWN Mailing List
lists.sans.org/mailman/listinfo/gpwn-list

Webcasts
pen-testing.sans.org/resources/webcasts

Twitter
@SANSPenTest

Poster & Cheat Sheets
pen-testing.sans.org/resources/downloads

PENETRATION TESTING PRACTICE LABS

Vulnerable Apps/Systems

Created by Aman Hardikar .M

Building your skills through hands-on lab experimentation is vital in the life of a penetration tester. Aman Hardikar .M built a hugely useful mind map showing various free, publicly available distributions, challenges, and other resources for practicing your skills.

The mind map is available online at:
amanhardikar.com/mindmaps/Practice.html
but feel free to use this poster version to check off the practice labs you've visited and beat. Thank you, Aman, for letting us include the mind map on this poster.
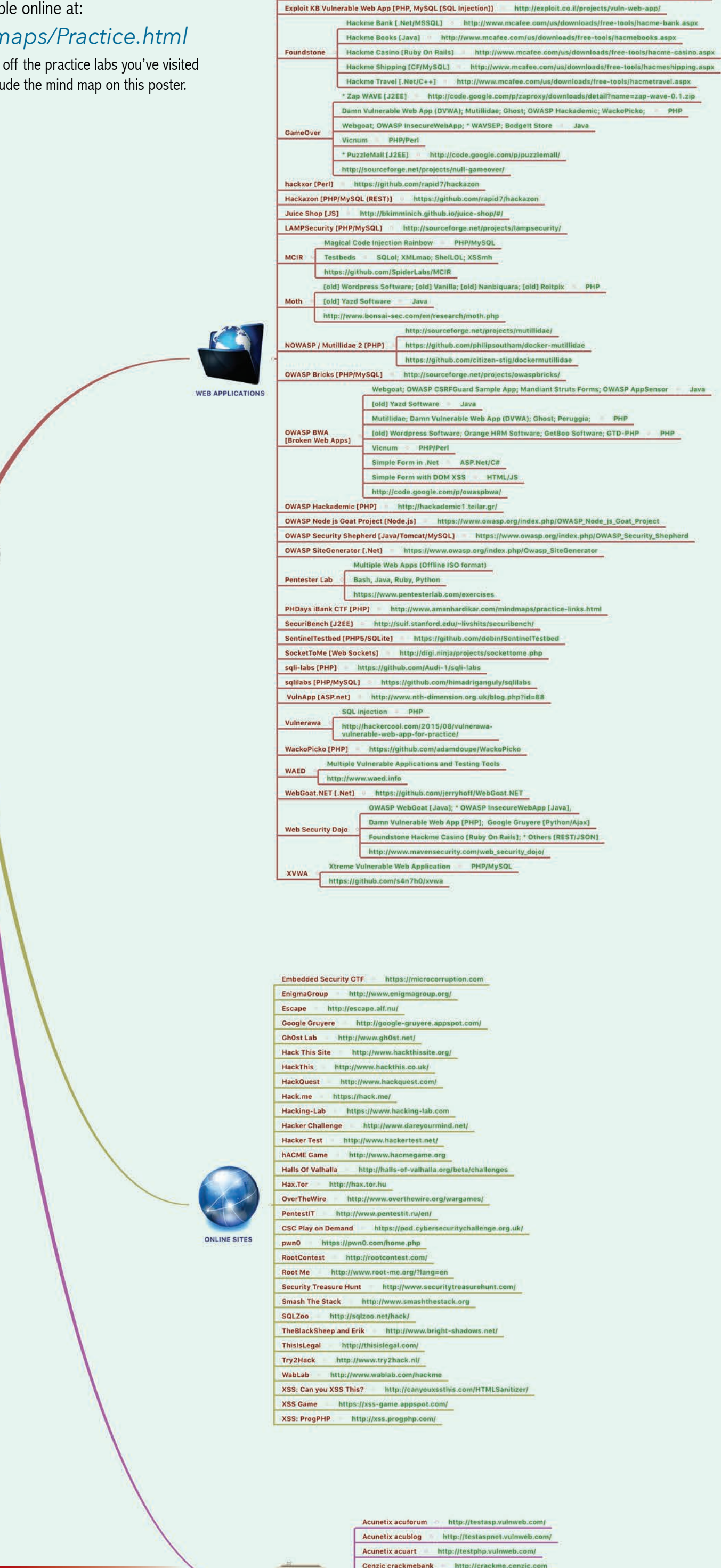

Mind map: PRACTICE LABS © Aman Hardikar .M

Please make sure you have explicit permission before analyzing or attacking any site in the list above. Always review the site's policies to ensure that you have explicit permission for any planned activities before proceeding.

NETWORK PENETRATION TESTING
by Ed Skoudis

GOAL
Determine whether sensitive data on the intranet could be compromised

TOOLS AND TECHNIQUES APPLIED
- Recon-ng (Step 1)
- Social Engineering Toolkit (Steps 2 and 3)
- Metasploit (Step 5)
- Meterpreter (Step 6)
- Mimikatz (Step 6)
- Lateral movement and pass-the-hash (Steps 6, 7, and 8)
- Detailed post-exploitation analysis (Step 8)

RELATED SANS COURSES
SEC504 SEC562
SEC560 SEC580
SEC561

1. Pen tester performs recon on the Internet to locate email addresses
2. As a first phase of a phishing attack, pen tester sends emails to all in-scope email addresses to measure clicks on links
3. For the second phase of phishing, the pen tester uses a specific email address of a given user to test client-side exploitation
4. User clicks on link, causing system to surf to pen tester's machine
5. Browser downloads client-side exploit, which runs payload on target client
6. Pen tester escalates privileges, gathers credentials, and seizes tokens
7. Pen tester uses credentials to attack administrative workstations, gaining domain admin privileges
8. Pen tester leverages privileges to show potential for accessing sensitive data on database server (without actually accessing the data)

SANS
Penetration Testing

Attack Surfaces, Tools, and Techniques

Effective penetration testing involves modeling the activities of real-world attackers with the goal of better understanding and managing business risk to improve an organization's security stance. Real-world attackers undermine modern organizations in a variety of ways, so penetration testers need to be prepared to draw from a variety of different attack types, tools, and techniques to simulate the activities of real-world attackers. Skilled penetration testers are familiar with numerous different attack types, and strive to build and reinforce their capabilities in each of these areas. Each diagram on this poster shows how different penetration testing techniques and tools can be applied to assessing the security stance of the same organization's infrastructure.
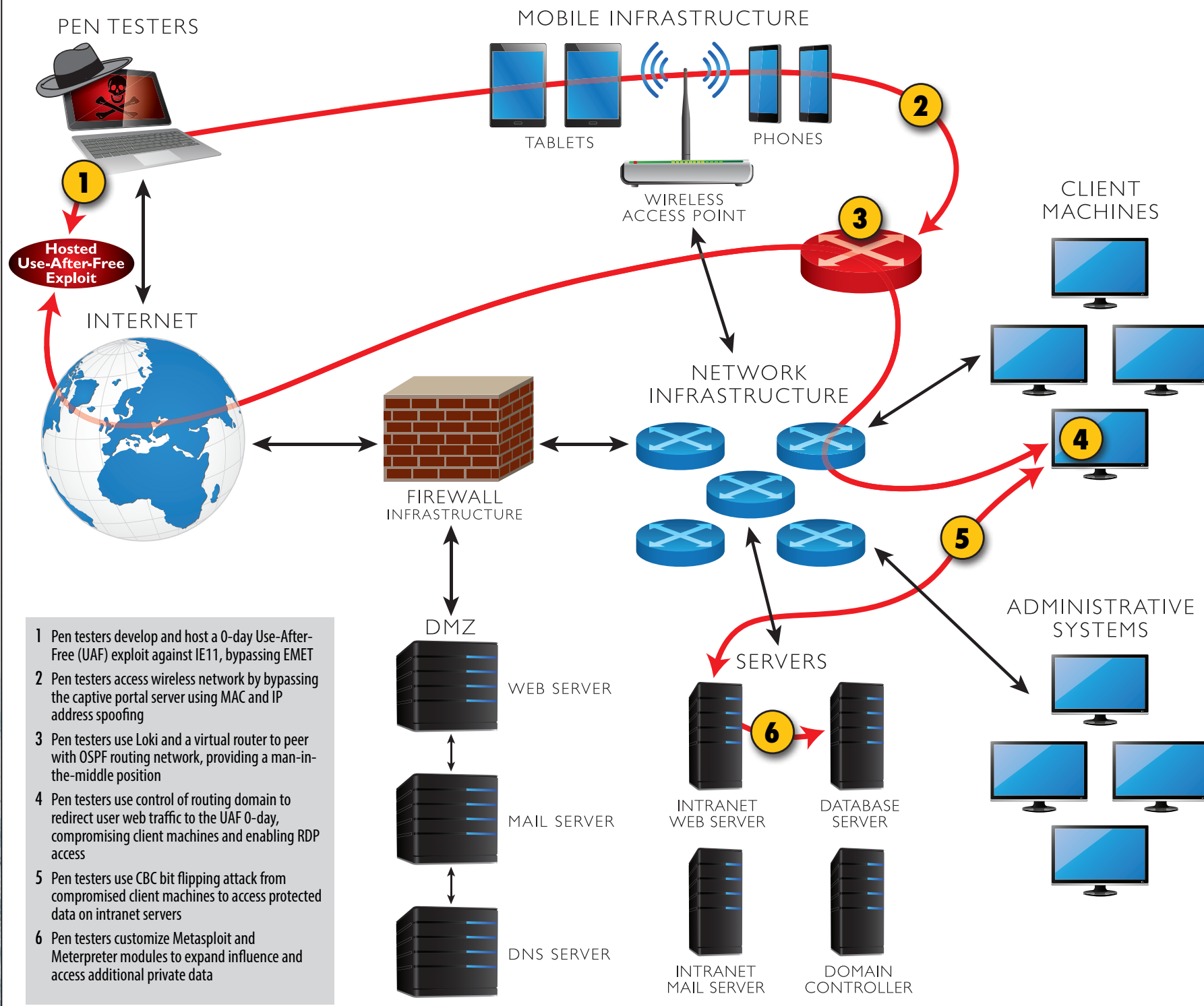
pen-testing.sans.org


ADVANCED NETWORK PEN TESTING
by Steve Sims

GOAL
Demonstrate multiple weaknesses in an organization's defense-in-depth architecture

TOOLS AND TECHNIQUES APPLIED
- WinDbg & Fuzzing (Step 1)
- cpscam (Step 2)
- Loki & Dynamips (Step 3)
- Custom-developed 0-day exploit & RDP (Step 4)
- Browser & Python (Step 5)
- Ruby, Metasploit & Meterpreter (6)

RELATED SANS COURSES
SEC660 SEC760

Hosted Use-After-Free Exploit

1. Pen testers develop and host a 0-day Use-After-Free (UAF) exploit against IE11, bypassing EMET
2. Pen testers access wireless network by bypassing the captive portal server using MAC and IP address spoofing
3. Pen testers use Loki and a virtual router to peer with OSPF routing network, providing a man-in-the-middle position
4. Pen testers use control of routing domain to redirect user web traffic to the UAF 0-day, compromising client machines and enabling RDP access
5. Pen testers use CBC bit flipping attack from compromised client machines to access protected data on intranet servers
6. Pen testers customize Metasploit and Meterpreter modules to expand influence and access additional private data

---

WIRELESS PENETRATION TESTING
by Larry Pesce

GOAL
Evaluate access to internal network via corporate Wi-Fi leveraging all manner of wireless client systems

TOOLS AND TECHNIQUES APPLIED
- Kismet (Step 1)
- Wireshark (Step 3)
- Airmon-ng & aireplay-ng (Step 4 & 6)
- Wi-Fi Pineapple (Step 4)
- Metasploit & Ettercap (Step 5)
- HostAP-WPE (Step 7)
- Hashcat, Asleap & Pass the Hash (Step 8)
- Authenticate to corporate AP (Step 9)
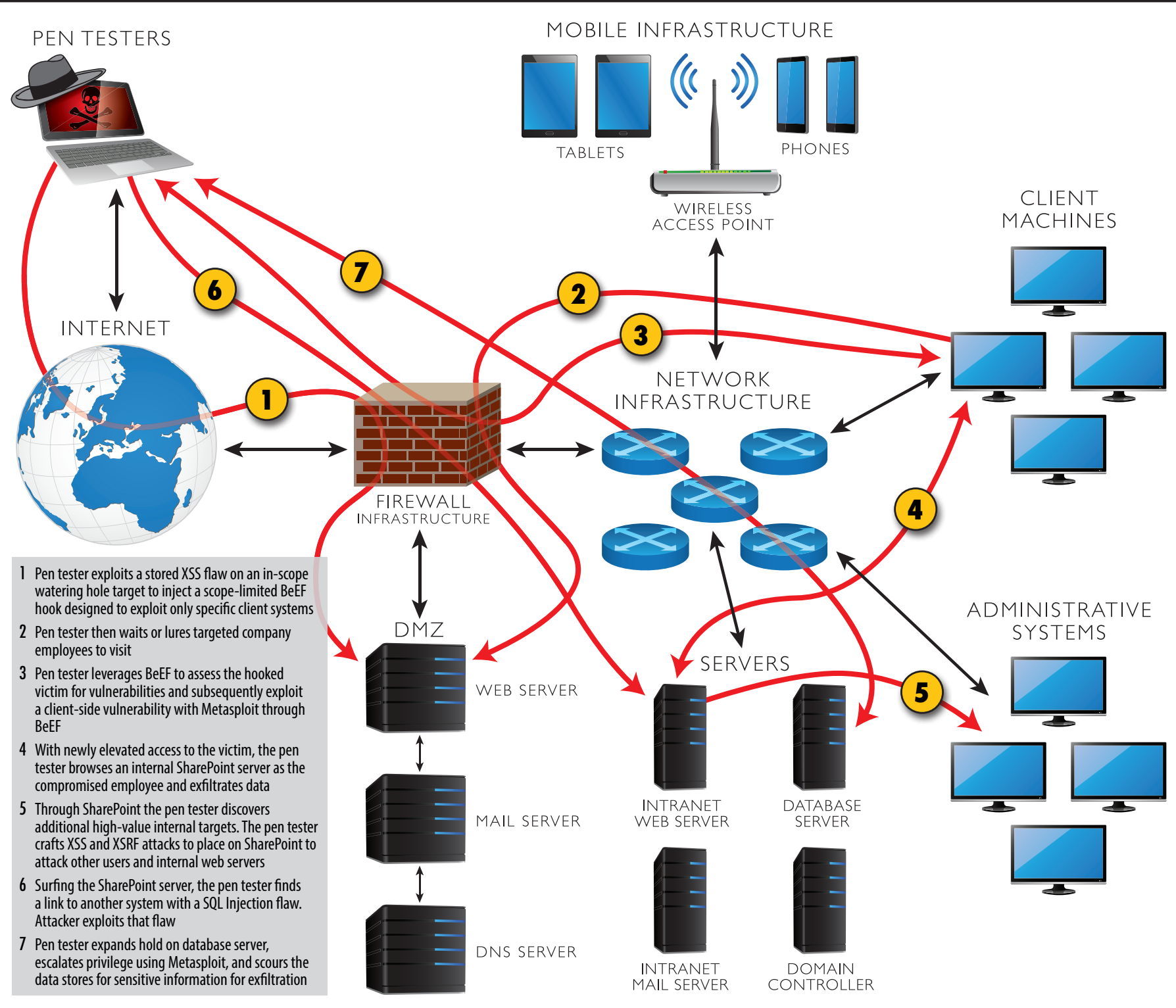
RELATED SANS COURSES
SEC575 SEC617
SEC560
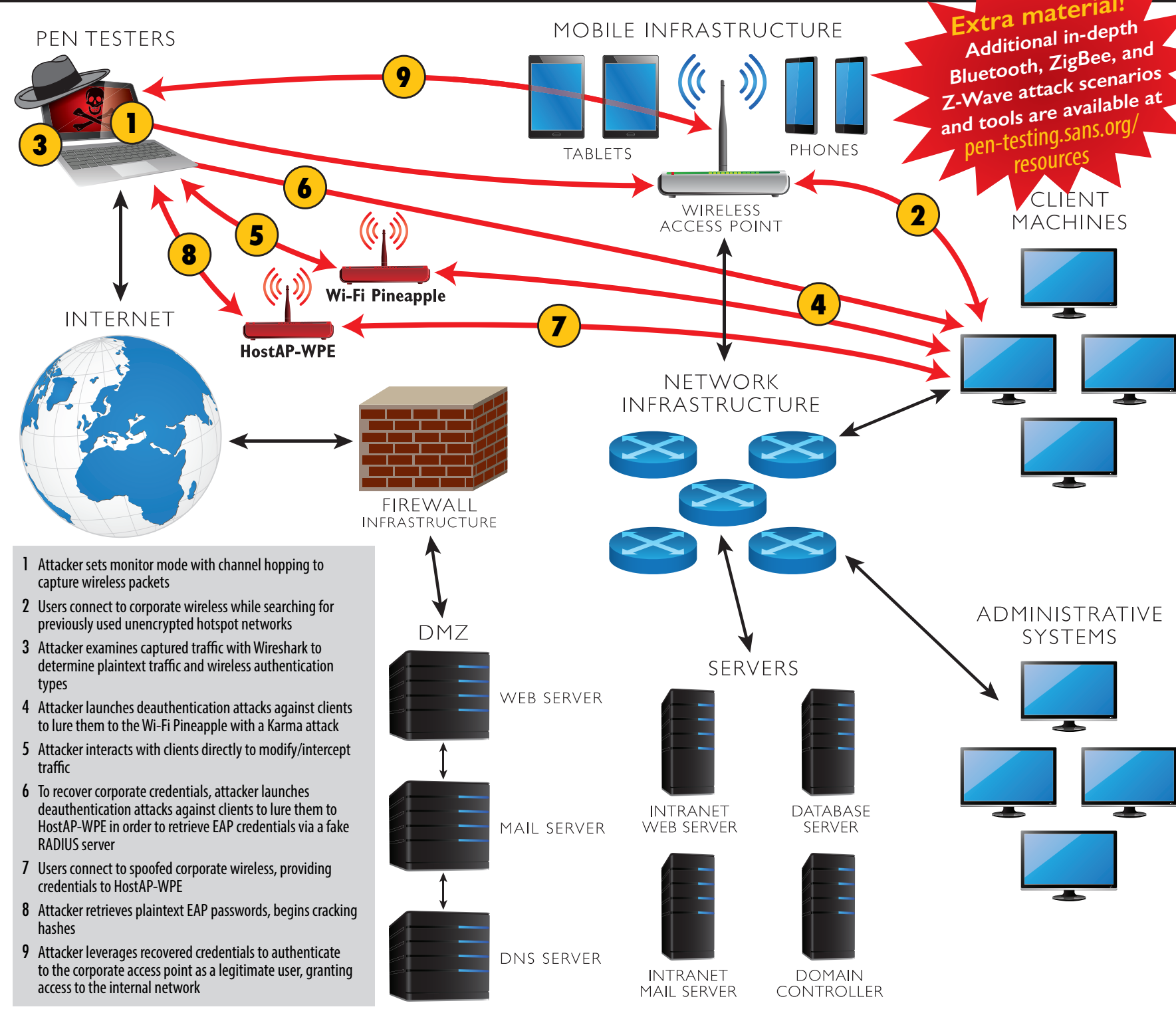
Extra material!
Additional in-depth Bluetooth, ZigBee, and Z-Wave attack scenarios and tools are available at pen-testing.sans.org/resources

1. Attacker sets monitor mode with channel hopping to capture wireless packets
2. Users connect to corporate wireless while searching for previously used unencrypted hotspot networks
3. Attacker examines captured traffic with Wireshark to determine plaintext traffic and wireless authentication types
4. Attacker launches deauthentication attacks against clients to lure them to the Wi-Fi Pineapple with a Karma attack
5. Attacker interacts with clients directly to modify/intercept traffic
6. To recover corporate credentials, attacker launches deauthentication attacks against clients to lure them to HostAP-WPE in order to retrieve EAP credentials via a fake RADIUS server
7. Users connect to spoofed corporate wireless, providing credentials to HostAP-WPE
8. Attacker retrieves plaintext EAP passwords, begins cracking hashes
9. Attacker uses recovered credentials to authenticate to the corporate access point as a legitimate user, granting access to the internal network

---

WEB APP PENETRATION TESTING
by Seth Misenar and Justin Searle

GOAL
Determine whether sensitive data on the intranet could be compromised

TOOLS AND TECHNIQUES APPLIED
- Burp Suite Pro / Zed Attack Proxy (ZAP) (Steps 1-7)
- Browser Exploitation Framework (BeEF) (Steps 1 & 3)
- Cross-Site Request Forgery (XSRF/CSRF) (Step 5)
- sqlmap (Steps 6 & 7)
- Metasploit (Step 3 & 7)
- Pen Tester written HTML5 code (Steps 1 & 5)
- Cross-Site Scripting (XSS) (Steps 1, 3 & 5)
- SQL Injection (Steps 6 & 7)

RELATED SANS COURSES
SEC542 SEC561
SEC560 SEC642

1. Pen tester exploits a stored XSS flaw on an in-scope watering hole target to inject a scope-limited BeEF hook designed to exploit only specific client systems
2. Pen tester then waits or lures targeted company employees to visit
3. Pen tester leverages BeEF to assess the hooked victim for vulnerabilities and subsequently exploit a client-side vulnerability with Metasploit through BeEF
4. With newly elevated access to the victim, the pen tester browses an internal SharePoint server as the compromised employee and exfiltrates data
5. Through SharePoint the pen tester discovers additional high-value internal targets. The pen tester crafts XSS and XSRF attacks to place on SharePoint to attack other users and internal web servers
6. Surfing the SharePoint server, the pen tester finds a link to another system with a SQL Injection flaw. Attacker exploits that flaw
7. Pen tester expands hold on database server, escalates privilege using Metasploit, and scours the data stores for sensitive information for exfiltration

---

MOBILE PENETRATION TESTING
by Joshua Wright

GOAL
Leverage weaknesses in mobile devices to harvest sensitive data, gain a foothold in corporate systems, and propagate extended access into the network

TOOLS AND TECHNIQUES APPLIED
- HostAP (Step 1)
- Aireplay-ng (Step 2)
- Wireshark & tcpdump (Step 3)
- Iptables & Burp Suite (Step 4)
- Spec.js & Drozer (Step 5)
- Drozer Weasel & Metasploit (Step 6)
- Drozer, Unix utilities, custom exploits (Step 7)
- Elcomsoft Phone Password Breaker & Phone Viewer (Step 8)
- Drozer modules & iPhone Configuration Utility (Step 9)

RELATED SANS COURSES
SEC575 SEC617
SEC561 SEC660

IMPOSTER AP
SMS

1. Attacker establishes imposter AP to lure victims
2. Attacker forces mobile devices to disconnect from corporate Wi-Fi
3. Victim mobile device connects to attacker trap, retrieves web page
4. Attacker dynamically rewrites webpage content being delivered to victim, using iptables and Burp Suite to include custom JavaScript content
5. Attacker uses Spec.js to automatically characterize victim and deliver browser exploit with Drozer
6. Victim mobile device returns shell to attacker
7. Attacker uses Drozer to enumerate files, escalate privileges, and read password manager app contents
8. Attacker uses credentials to access corporate and cloud servers
9. Attacker uses victim mobile device to forge SMS messages to contact book entries to push malicious device control policies to other mobile devices