Course 3: Selecting Your Attacks, Part 1

Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001)

Remote Social Engineering

Episode 1

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

PENTEST+ EXAM OBJECTIVES

DOMAIN	PERCENTAGE OF EXAM
1.0 Planning and Scoping	15%
2.0 Information Gathering and Vulnerability Identification	22%
3.0 Attacks and Exploits	30%
4.0 Penetration Testing Tools	17%
5.0 Reporting and Communication	16%
TOTAL	**100%**

SOCIAL ENGINEERING

- Tricking or coercing people into violating security policy
- Depends on willingness to be helpful
- Human weaknesses can be leveraged
- May rely on technical aspects
- Bypasses access controls and most detection controls

3.1 Compare and contrast social engineering attacks.

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

PHISHING

- Phishing – people are contacted by a seemingly legitimate imposter in an attempt to extract sensitive information
  - Spear phishing
  - SMS phishing
  - Voice phishing
  - Whaling

3.1.1 Phishing
3.1.1.1 Spear phishing
3.1.1.2 SMS phishing
3.1.1.3 Voice phishing
3.1.1.4 Whaling
3.1.2 Elicitation
3.1.2.1 Business email compromise

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

Spear Phishing Demo

Episode 2

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

In-Person Social Engineering

Episode 3

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

MORE ATTACKS AND EXPLOITS

- Elicitation – Gathering information about a system or environment from authorized users
  - Business email compromise – Collecting information as if the attacker were an insider
- Interrogation – Conducting informal (mostly) interviews with specifically crafted questions to extract as much information as possible
- Impersonation – Pretending to be someone with authority, such as technical support
- Shoulder surfing – watching as someone enters a username, password, PIN, or other secret to satisfy access controls

3.1.2 Elicitation
3.1.2.1 Business email compromise
3.1.3 Interrogation
3.1.4 Impersonation
3.1.5 Shoulder surfing

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

MOTIVATION TECHNIQUES

- Motivation techniques – why social engineering works
  - Authority
  - Scarcity
  - Social proof
  - Urgency
  - Likeness
  - Fear
- The bottom line
  - People want to be accepted and valued by others

3.1.7 Motivation techniques
3.1.7.1 Authority
3.1.7.2 Scarcity
3.1.7.3 Social proof
3.1.7.4 Urgency
3.1.7.5 Likeness
3.1.7.6 Fear

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

Network-Based Exploits

Episode 4

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

USB KEYS AND SOCIAL ENGINEERING

- USB key drop
  - Weaponized USB keys placed where users might pick them up and insert them into their own computers
  - https://null-byte.wonderhowto.com/how-to/hack-wpa2-wi-fi-passwords-using-jedi-mind-tricks-usb-dead-drops-0185290/

3.1.6 USB key drop

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

NETWORK-BASED EXPLOITS

- Name resolution exploits
  - NETBIOS name service (NBNS)
    - Part of NetBIOS-over-TCP
    - Similar functionality to DNS – translate host name to IP address
  - LLMNR (Link-local Multicast Name Resolution)
    - Protocol based on DNS packet format
    - Allows IPv4 and IPv6 name resolution on the same local link
  - DNS and ARP poisoning could be in this category as well

3.2 Given a scenario, exploit network-based vulnerabilities.
3.2.1 Name resolution exploits
3.2.1.1 NETBIOS name service
3.2.1.2 LLMNR
3.2.2 SMB exploits
3.2.3 SNMP exploits
3.2.4 SMTP exploits
3.2.5 FTP exploits

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

MORE NETWORK EXPLOITS

- SMB (Server Message Block) exploits
  - Protocol used in Windows to provide file and printer access, and remote service access
  - Uses TCP ports 139 and 445
  - Some ransomware (EternalBlue, WannaCry) use SMB to propogate
- SNMP (Simple Network Management Protocol) exploits
  - Used to query and manage IP devices
  - Multiple versions - SNMPv1 is not secure
    - cleartext passwords (default “community string” is “public”)

3.2.2 SMB exploits
3.2.3 SNMP exploits
3.2.4 SMTP exploits
3.2.5 FTP exploits

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

EVEN MORE NETWORK EXPLOITS

- SMTP (Simple Mail Transport Protocol) exploits
  - Standard protocol for transmitting email
  - Open relay, local relay, phishing, spam, etc.
- FTP (File Transfer Protocol) exploits
  - Overall insecure protocol for transferring files
  - No encryption for transfers and credentials (i.e. in the clear)
  - Easy for attackers to use for data exfiltration if FTP is available

3.2.4 SMTP exploits
3.2.5 FTP exploits

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

FTP Exploit Demo

Episode 5

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

Man-in-the Middle Exploits

Episode 6

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

ADDITIONAL NETWORK EXPLOITS

- Man-in-the-middle picture
  - Family of attacks where the attack intercepts messages between a sender and receiver
  - Attack may modify, regenerate, or forward intercepted messages

3.2.8 Man-in-the-middle

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

MAN-IN-THE-MIDDLE EXPLOITS

- ARP spoofing
  - Similar to DNS poisoning, but with local MAC addresses
- Pass the hash
  - Attacker intercepts an NTLM hash (user credential) and reuses it to appear as an authenticated user to Windows

3.2.8.1 ARP spoofing
3.2.7 Pass the hash

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

MAN-IN-THE-MIDDLE EXPLOITS

- Replay
- Relay
- SSL (Secure Sockets Layer) stripping
- Downgrade

3.2.8.2 Replay
3.2.8.3 Relay
3.2.8.4 SSL stripping
3.2.8.5 Downgrade

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

MAN-IN-THE-MIDDLE EXPLOITS

- DoS (Denial of Service)/stress test
- NAC (Network Access Control) bypass
- VLAN (Virtual Local Area Network) hopping

3.2.9 DoS/stress test
3.2.10 NAC bypass
3.2.11 VLAN hopping

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

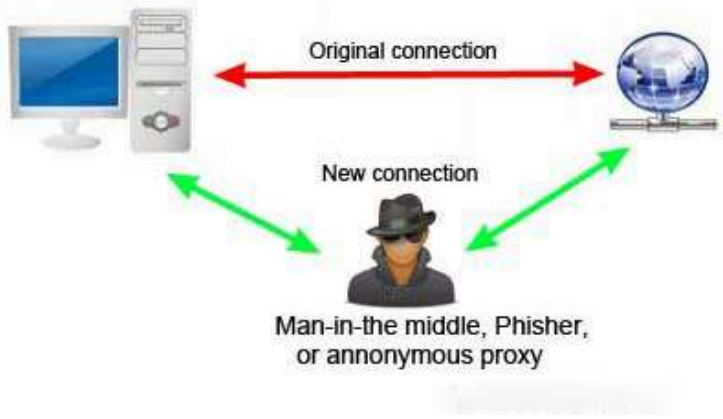
Wireless Exploits

Episode 7

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

MAN-IN-THE-MIDDLE ATTACK

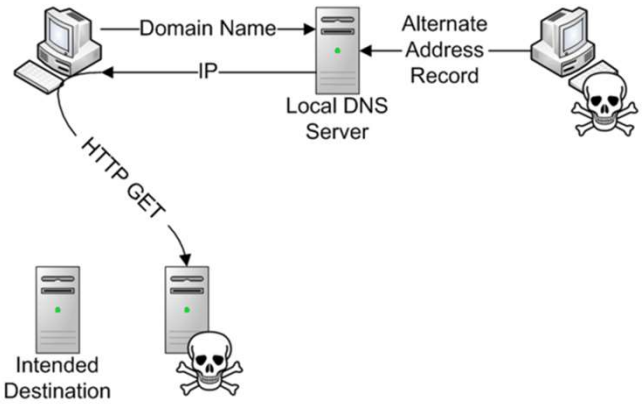


Source: https://www.computerhope.com/jargon/m/mitma.htm

3.2.6 DNS cache poisoning

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

DNS CACHE POISONING



Source: https://www.greycampus.com/opencampus/ethical-hacking/web-services-attacks

3.2.6 DNS cache poisoning

WIRELESS AND RF VULNERABILITIES

- Wireless and RF vulnerabilities
  - Broadcast is wide open - anyone with receiver can intercept traffic
  - Common tool is aircrack-ng (lots of Wf-Fi scanners for all OSs)
- Evil twin – rogue Wireless Access Point (WAP) used to eavesdrop
  - Karma attack (Karma Attacks Radio Machines Automatically)
    - Device that listen for SSID requests and pretends to be valid WAP
  - Downgrade attack – attempt to negotiate (force) a more insecure protocol
- Deauthentication attacks
  - DoS attacks that disrupt communication between a user and WAP

3.3 Given a scenario, exploit wireless and RF-based vulnerabilities.
3.3.1 Evil twin
3.3.1.1 Karma attack
3.3.1.2 Downgrade attack
3.3.2 Deauthentication attacks

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

WIRELESS AND RF VULNERABILITIES

- Fragmentation attacks
  - DoS attack that floods a network with datagram fragments (someone has to reassemble)
- Credential harvesting
  - Process of capturing or discovering valid login credentials
  - Social engineering or other means
- WPS implementation weaknesses
  - Several consumer grade WAPs could allow an attacker to learn the WPS PIN
- https://github.com/exploitagency/ESPortalV2

3.3.3 Fragmentation attacks
3.3.4 Credential harvesting
3.3.5 WPS implementation weakness

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

OTHER WIRELESS VULNERABILITIES

- Bluejacking – sending unsolicited messages to a Bluetooth-enabled device
- Bluesnarfing – stealing information from a Bluetooth-enabled device
- RFID Cloning – unauthorized copy of a device's RF signal
- Jamming – DoS attack that disables communication among devices
- Repeating – receiving and retransmitting a signal to increase range
  - Can provide easier access for an attacker

3.3.6 Bluejacking
3.3.7 Bluesnarfing
3.3.8 RFID cloning
3.3.9 Jamming
3.3.10 Repeating

Some Tools:

Aircrack-ng is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security:

Monitoring
Attacking
Testing
Cracking

Various wifi scanners and related tools can be found on many platforms including Android.

Fake cell phone towers (also called ISMI (International mobile subscriber identity) catchers or Stingrays)

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

Application Exploits, Part 1

Episode 8

SAGEFOX

APPLICATION-BASED VULNERABILITIES

- Injections – inserting additional input data beyond what is expected
  - SQL (Standard Query Language)
    - Adding specially crafted SQL in input to extract/modify data or execute commands
  - HTML (HyperText Markup Language)
    - Adding HTML code when rendering web pages or submitting data to change the way a page works or how the data is handled
  - Command
    - Adding command line options that change the way commands operate
  - Code
    - A generalization of SQL injection – adding code in any language to change a program's behavior

3.4 Given a scenario, exploit application-based vulnerabilities.
3.4.1 Injections
3.4.1.1 SQL
3.4.1.2 HTML
3.4.1.3 Command
3.4.1.4 Code

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

APPLICATION-BASED

- Injection attack
  - Inserting additional data into application beyond what is expected
  - SQL (Structured Query Language)
    - Adding specially crafted SQL input to extract/modify data or execute commands
  - HTML
    - Adding HTML code/ submitting data to change how a page works or the data is handled

3.4 Given a scenario, exploit application-based vulnerabilities.
3.4.1 Injections
3.4.1.1 SQL
3.4.1.2 HTML
3.4.1.3 Command
3.4.1.4 Code

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

INJECTIONS, cont'd

- Command
  - Adding command line options that change the way commands operate
- Code
  - A generalization of SQL injection – adding code in any language to change a program's behavior

3.4 Given a scenario, exploit application-based vulnerabilities.
3.4.1 Injections
3.4.1.1 SQL
3.4.1.2 HTML
3.4.1.3 Command
3.4.1.4 Code

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

SQL Injection Demo

Episode 9

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

Application Exploits, Part 2

Episode 10

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

AUTHENTICATION EXPLOITS

- Credential brute forcing
  - Offline cracking (Hydra)
- Session hijacking
  - Intercepting and using a session token (generally) to take over a valid distributed (web) session
- Redirect
  - Sending the user to a different site from what they expected (phishing)

3.4.2 Authentication
3.4.2.1 Credential brute forcing
3.4.2.2 Session hijacking
3.4.2.3 Redirect
3.4.2.4 Default credentials
3.4.2.5 Weak credentials
3.4.2.6 Kerberos exploits

Golden tickets are forged Kerberos Ticket-Granting Tickets (TGT) and a Silver tickets are forged Kerberos Ticket Granting Service (TGS) tickets, also called service tickets. Golden tickets allow for gaining access to any Kerberos service, while Silver tickets are limited to targeted service.

AUTHENTICATION EXPLOITS

- Default credentials
  - Out of the box artifacts (you have to clean these up!)
- Weak credentials
  - This is why password cracking works
- Kerberos exploits
  - Forged tickets to allow unauthorized access to resources

3.4.2 Authentication
3.4.2.1 Credential brute forcing
3.4.2.2 Session hijacking
3.4.2.3 Redirect
3.4.2.4 Default credentials
3.4.2.5 Weak credentials
3.4.2.6 Kerberos exploits

Golden tickets are forged Kerberos Ticket-Granting Tickets (TGT) and a Silver tickets are forged Kerberos Ticket Granting Service (TGS) tickets, also called service tickets. Golden tickets allow for gaining access to any Kerberos service, while Silver tickets are limited to targeted service.

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

AUTHORIZATION

- Parameter pollution
  - Providing custom input parameters to alter service/API operation
- Insecure direct object reference
  - Programming mistake that can allow an attacker to bypass access controls and access resources or data

3.4.3 Authorization
3.4.3.1 Parameter pollution
3.4.3.2 Insecure direct object reference
3.4.4 Cross-site scripting (XSS)
3.4.4.1 Stored/persistent
3.4.4.2 Reflected
3.4.4.3 DOM

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

Application Exploits, Part 3

Episode 11

SAGEFOX

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

CROSS-SITE SCRIPTING (XSS)

- Injection attack in which an attacker sends malicious code (client-side script) to a web application that a subsequent client runs
  - Stored/persistent
    - Attack data (script) stored discretely on the server
  - Reflected
    - Non-persistent attack in which attack code is sent to another client
  - DOM (Document Object Model)
    - XSS attack that uses XML, not HTML, to transport attack code

3.4.3 Authorization
3.4.3.1 Parameter pollution
3.4.3.2 Insecure direct object reference
3.4.4 Cross-site scripting (XSS)
3.4.4.1 Stored/persistent
3.4.4.2 Reflected
3.4.4.3 DOM

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

CROSS-SITE REQUEST FORGERY (CSRF/XSRF)

- Similar to XSS; occurs within an authenticated session
- XSRF attacks a user
- Attacker can cause authorized user to take some action by clicking a link

3.4.5 Cross-site request forgery (CSRF/XSRF)
3.4.6 Clickjacking

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

CLICKJACKING

- Tricking user into clicking a different link or object that was intended
- Attackers can use transparent or opaque layers to embed attack links

3.4.5 Cross-site request forgery (CSRF/XSRF)
3.4.6 Clickjacking

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

SECURITY MISCONFIGURATION

- Directory traversal
  - Allows users to navigate outside a web server's root directory
- Cookie manipulation
  - Access to cookies can allow an attacker to change the way in which a web application operates in general, or just for a specific user/session

3.4.7 Security misconfiguration
3.4.7.1 Directory traversal
3.4.7.2 Cookie manipulation
3.4.8 File inclusion
3.4.8.1 Local
3.4.8.2 Remote

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon

FILE INCLUSION

- Related to directory traversal
- Attacker is allowed to build path to .exe file or a file to access
- File can be local or remote

3.4.7 Security misconfiguration
3.4.7.1 Directory traversal
3.4.7.2 Cookie manipulation
3.4.8 File inclusion
3.4.8.1 Local
3.4.8.2 Remote

Source: Ethical and CompTIA PenTest+ Exam Prep (PT0-001) Hacking with Michael Solomon