Pentesting
Red Teaming

Open Source Offerings Document

Latest version of this document can be found here:
https://bit.ly/OpenSourcePentest

Original Document Authors

This document was created with input from individuals I (Rob Fuller) worked with/for in multiple jobs. If you see your input in here, feel free to message me and make sure I add you to the list.

Leave a comment / suggest a change, be added to this list.

The purpose of these slides are to ensure that this document stays freely available to enhance levels of service and allow those new to the community have a baseline to start from.

In no particular order:

- Rob Fuller
- Craig Balding
- Dale Pearson
- Adam Uccello
- Joshua Gauthier
- Dorota Kulas
- Blazej K.
- Matt Sabourin
- John Cooper
- Jirka V.

- Chris Gates
- Chris Nickerson
- Eric Smith
-

<u>Name listed does not imply endorsement of document</u>

Terminology

What is Penetration Testing?

Engagement that centers around a computer, network or web application infrastructure of an enterprise. This type of engagement focuses on the prevention security layer, finding, testing, classifying and verifying vulnerabilities in the enterprise’s environment.

This type of engagement is usually performed specifically for PCI and other compliance needs.

What is Red Teaming?

Team based engagements that includes the IT, social, and physical vertices. This type of engagements focus on all three layers of security defense, prevention, detection, and response. Findings focus on systemic, broad spectrum vulnerabilities in narrative format.

For the rest of the document, Pentesting, and Red Teaming will simply be referred to as “engagements”

customers / clients == partners

We are not adversaries.

Mindset

Communication Documentation

- Non-Disclosure Agreement (NDA)
- Statement of Work (SoW)
- Rules of Engagement (RoE)
- Deliverables Request (DR)
- During Engagement Communications Agreement (DECA)
- Results Rubric (RR)
- End of Engagement Report (EER)

Why? Prevent, Detect, Respond

In many of the scenarios listed prevention, detection, and response play a major role. Open and two way dialogue between the engagement team and the defensive team creates a learning opportunity for both sides and enables a positive environment for both teams to grow. Company security becomes organic instead of forced.

This type of two way communication has been known to reduce job stress , increase job satisfaction, retention rate, and team culture as a bi-product. (“failing a pentest looks poorly on our reviews” turns into “the engagement team showed us how to tweak our rules to reduce the noise and catch new things”)

What? Setting goals for the engagement (Examples)

- Senior or core developer of company product / service
- Core company products or services and / or the software, machines or date that they encompass
- Domain Administrator (DA)
    - This is a common goal, but should be coupled with a goal that matters to the business outside of general IT. (“I don’t have to be a DA to access Jane The Coder’s laptop”)

Communication Timeline

Communication Timeline: Default (3w Example)

SUN	MON	TUE	WED	THU	FRI	SAT
1	2 🟨	3	4	5	6	7
8	9 🟩	10	11	12	13	14 ⚡
15	16	17	18 ⊗	19	20	21
22	23	24 ⊕	25	26	27 🟥	28
29	30	31				

🟨 Pre-engagement deliverables are due

🟩 Start of engagement

⚡ Unscheduled outage

⊗ Non-engagement related intrusion detected

⊕ Engagement related intrusion detected

🟥 End of engagement

Communication Timeline: Default (3w Example)

- Pre-Engagement due date
- Start of Engagement
- Unscheduled outage
  - Any time there are outages that may cause a disruption to testing, or may have been caused by testing.
  - If the engagement team causes an outage then <u>**immediate**</u> communication to the partner PoC
- Non-engagement related intrusion detected
  - If at any time the engagement team identifies evidence of an intrusion to the partner's network
  - <u>**Immediate**</u> communication to the partner PoC to verify detection and discuss next steps.
- Engagement related intrusion detected
- PoC to reach out to the engagement team to discuss next steps
- End of Engagement

Communication
Documentation

Communications Documentation: NDA

- Includes:
  - Agreement by both parties not to disclose the contents or context of the test
- Template Link:
  - http://bit.ly/OpenSourceNDA

Communications Documentation: SoW

- Includes:
  - Cost
  - Scenarios included for the engagement
- Template Link:
  - https://bit.ly/OpenSourceSoW

Communications Documentation: RoE

- Includes:
  - Stopping points or limits to the engagement and the specified scenarios
  - Exclusion Lists / Fragile systems
  - Emergency contact information for both parties
- Template Link:
  - https://bit.ly/OpenSourceROE

Communications Documentation: DR

- Includes:
  - List of partner and engagement team deliverables
  - Timeline for deliverables
  - Template and examples for deliverables
- Template Link:
  - https://bit.ly/OpenSourceDR

Communications Documentation: DECA

- Includes:
  - Timeline of all pre-engagement, engagement, and reporting communications
  - Contact information tree for all communications and in case of escalation
  - Any vacation or unavailability periods on either side
  - Time zones for all parties (if differing)
- Template Link:
  - https://bit.ly/OpenSourceDECA

Communications Documentation: RR

- Includes:
  - Rubric scoring from partner
  - Rubric scoring from assessment
- Template Link:
  - http://bit.ly/OpenSourceRR

Provided as a deliverable that both the sides fill out

Communications Documentation: EER

- Includes:
  - Attack Narrative / Diagram
  - Findings
  - Remediation Steps
  - Prevention / Detection Opportunities
  - Clean-up Items
- Template Link:
  - https://bit.ly/OpenSourceEER

Common Fears

Common Fears: Outages

All possible precautions will be taken in order to ensure the engagement team does not cause outages or undue added work to the partner organization. This includes the clean up of all engagement binaries, files, and changes to the best of the ability of the engagement team.

A list of any “clean up” items that the team was unable to restore or remove will be provided within the End of Engagement Report (EER)

Common Fears: Physical Damages

All possible precautions will be taken in order to ensure the engagement team does not cause damages to the partner organization. This includes the clean up of all engagement binaries, files, and changes to the best of the ability of the engagement team.

A list of any “clean up” items that the team was unable to restore or remove will be provided within the End of Engagement Report (EER)

Methodology

PTES Methodology is the gold standard. No reason to reiterate here.
(Not all methodologies apply to every scenario / engagement.

Pentest Execution Standard

http://www.pentest-standard.org/index.php/Main_Page

Scenarios

Opportunistic Attacker

1 week

Opportunistic Attacker: Methodology

- Loud (no attempts to perform testing in a stealthy manner)
- Techniques
  - Login brute forcing
  - Fast / Large port range Nmap scanning
  - Vuln scanning / Web vuln scanning
  - SPAM style phishing
- Separating attack techniques by day for ease of identification

Opportunistic Attacker: Goals

- Identify IT security maturity level
- Test prevention security layer
  - Antivirus
  - Host Intrusion Prevention Systems
  - Proxy services
  - Web Application Firewalls
  - SPAM / Phishing filters
- Active or Post-Engagement Detection just to see if capabilities are working and can see “loud” attacks

Opportunistic Attacker: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

- ❑ List of in-scope IP addresses
- ❑ List of scope exclusions

TO CLIENT

- ❑ List of “attack” IP addresses

(POST-ENGAGEMENT)

FROM CLIENT

- ❑ N/A

TO CLIENT (OUTSIDE OF EER)

- ❑ List of attacks categories performed based on MITRE ATT&CK

External with Credentials

1 week

External w/ Credentials: Methodology

- Login Attempts
  - Company web login interfaces
  - VPN / Remote Access interfaces
  - Email interfaces
  - External / Cloud interfaces (Office365, Dropbox, Box, etc)
  - External / Cloud infrastructure (AWS, Azure)
- Attempts to obtain code execution
  - If obtained, post-exploitation is in-scope to better identify risk of scenario

External w/ Credentials: Goals

- Identify authentication leak risk to the enterprise via stolen, backdoored, or disgruntled employee
- Identify previously unknown authentication interfaces
- Test <u>prevention</u> security layer
  - 2-Factor Authentication / Multi-Factor Authentication
- Test <u>detection</u> security layer
  - Foreign / suspicious login identification / alerting

External w/ Credentials: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

- Authentication information to be tested
- New employee packet / information
- List of known authentication interfaces
- List of external IP ranges

(POST-ENGAGEMENT)

FROM CLIENT

- Logins detected and identified

TO CLIENT (OUTSIDE OF EER)

- List of “found” authentication interfaces

Stolen Laptop / Mobile

2 weeks

Stolen Laptop / Mobile: Methodology

- Risk Modes
  - Stolen / Unlocked
  - Stolen / Locked
- Fully provisioned “Employee” laptop and / or mobile device(s)
- Week 1 - 1.5: Used for attempting to gain access to the devices and infrastructure.
- Week 1.5 - 2: Used for testing alerting and response procedures

Stolen Laptop / Mobile: Goals

- Identify potential risk to enterprise if IT devices are lost / infrastructure
- Test prevention security layer
  - 2-Factor Authentication / Multi-Factor Authentication
  - Hard drive encryption
  - Mobile app siloing
- Test detect security layer
  - Identify Lost / Stolen device alerting policies

Stolen Laptop / Mobile: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

- Laptop / Mobile device (fully provisioned)
- New employee packet / information
- Authentication / Pin code login information

TO CLIENT

(POST-ENGAGEMENT)

FROM CLIENT

- Logins detected and identified

TO CLIENT (OUTSIDE OF EER)

Breach Simulation

2 weeks

Breach Simulation: Methodology

- Begins with a **real user** being identified and used for the engagement.
- Engagement team provides partner with binary or link to be pushed to user’s machine or user is asked to run.
- **Goal oriented** actions performed after initial access provided.

Breach Simulation: Goals

- Assesses the actions, policies, and procedures of the enterprise’s detection and response team (CIRT) under breach conditions
- Test prevention security layer
  - Antivirus
  - Host Intrusion Prevention Systems
  - Internal authentication (ACL) controls / Separation of privilege
- Test detect security layer

Breach Simulation: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

- Goals and target data locations
  - Dummy data sitting virtually “next to” risky data is preferable as testing of exfiltration can be accomplished without risk to

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

-

Insider

2 weeks

Insider: Methodology

- Loud
- Full physical or remote access (RDP) access to a enterprise laptop or desktop provided
- Techniques:
  - Large file transfers (Internal shares, download, uploads, Box/Dropbox)
  - Downloading of “hacker” tools
  - AV detections
  - Overt scanning
  - Installation of unauthorized software

Insider: Goals

- Identifies opportunities for improvement of controls around data access and exfiltration
- Identifies opportunities for improvement surrounding "malicious" activity of insiders that deviate from standard enterprise access
- Test prevention security layer
  - Antivirus
  - Host Intrusion Prevention Systems
  - Internal authentication (ACL) controls /

Insider: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

- Access to provisioned workstation with provisioned authentication
- User account provisioned with scenario driven level of acces

TO CLIENT

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

Black Box

4 weeks

Blackbox: Methodology

- Zero knowledge given (other than the company’s name)
- Open Source Intelligence gathering
- Social Engineering
  - Email (can lead to Breach Simulation)
  - Verbal (In person as well as over the phone)
- **<u>Goal oriented</u>**
- Common add-ons:
  - Physical

Blackbox: Goals

- Assesses the actions, policies, and procedures of the Company's detection and response team (CIRT)
- Assesses effectiveness of security products and services purchased or pipelined
- Tests complete **Prevent**, **Detect**, **Respond** stack

Blackbox: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

- Name of the company

TO CLIENT

-

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

-

Add-ons

Addition testing scenarios that are not generally offered without being coupled with another scenario type

What is an “Add-on”

Interchangeable parts of an engagement that are not automatically included, but is available upon request.

Wireless

1 week

Wireless: Methodology

- Encryption attacks against any available Company WEP networks
- Brute force attacks against any available Company WPA PSK networks
- Client misdirection and replay attacks
- Enterprise Wireless configuration attacks

Wireless: Goals

- Identifies attack detection capabilities of the enterprise wireless configuration
- Identifies misconfigurations or weak configurations in the enterprise wireless infrastructure
- Test prevention security layer
  - Host separation
  - Wireless Intrusion Prevention Systems
  - Wireless encryption / passwords

Wireless: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

❑

TO CLIENT

❑

(POST-ENGAGEMENT)

FROM CLIENT

❑ Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

❑ Any previously unkown client wireless networks found

Physical

1-2 week(s)

Physical: Methodology

- Testing of single or multiple locations
- Usually coupled with Wireless and other radio assessments strategies:
  - RFID
  - Zigbee
  - etc
-

Physical: Extra Documentation

❑ “Get out of Jail Free” Card

❑ On-site Point of Contact

❑ Local Law Enforcement Communication

Physical: Goals

- Identifies attack detection capabilities of the enterprise wireless configuration
- Identifies misconfigurations or weak configurations in the enterprise wireless infrastructure
- Test prevention security layer
  - Host separation
  - Wireless Intrusion Prevention Systems
  - Wireless encryption / passwords

Physical: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

- Signed Get-Out-Of-Jail-Free
- List of on-site points of contact

TO CLIENT

- Countersigned Get-Out-Of-Jail-Free

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

Egress Testing

1 week

Egress Testing: Methodology

- Encryption attacks against any available Company WEP networks
- Brute force attacks against any available Company WPA PSK networks
- Client misdirection and replay attacks
- Enterprise Wireless configuration attacks

Egress Testing: Goals

- Identifies attack detection capabilities of the enterprise wireless configuration
- Identifies misconfigurations or weak configurations in the enterprise wireless infrastructure
- Test prevention security layer
  - Host separation
  - Wireless Intrusion Prevention Systems
  - Wireless encryption / passwords

Egress Testing: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

-

TO CLIENT

- Link / Binary for engagement

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

-

Detection Collaboration

1 week

Detection Collaboration: Methodology

- Encryption attacks against any available Company WEP networks
- Brute force attacks against any available Company WPA PSK networks
- Client misdirection and replay attacks
- Enterprise Wireless configuration attacks

Detection Collaboration: Goals

- Identifies attack detection capabilities of the enterprise wireless configuration
- Identifies misconfigurations or weak configurations in the enterprise wireless infrastructure
- Test prevention security layer
  - Host separation
  - Wireless Intrusion Prevention Systems
  - Wireless encryption / passwords

Detection Collaboration: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

-

TO CLIENT

- Link / Binary for engagement

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

-

C2 Detection Exercise

1 week

C2 Detection Exercise: Methodology

- Encryption attacks against any available Company WEP networks
- Brute force attacks against any available Company WPA PSK networks
- Client misdirection and replay attacks
- Enterprise Wireless configuration attacks

C2 Detection Exercise: Goals

- Identifies attack detection capabilities of the enterprise wireless configuration
- Identifies misconfigurations or weak configurations in the enterprise wireless infrastructure
- Test prevention security layer
  - Host separation
  - Wireless Intrusion Prevention Systems
  - Wireless encryption / passwords

C2 Detection Exercise: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

-

TO CLIENT

- Link / Binary for engagement

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

-

Rogue Device

1 week

Rogue Device: Methodology

- Devices installed via Physical engagement or client installed
- Network based attacks
- Can be used to enable the following scenarios:
  - Pentest
  - Insider
  - Egress Testing
  - Detection Collaboration
  - C2 Detection

Rogue Device: Goals

- Identifies attack detection capabilities of the enterprise wireless configuration
- Identifies misconfigurations or weak configurations in the enterprise wireless infrastructure
- Test prevention security layer
  - Host separation
  - Wireless Intrusion Prevention Systems
  - Wireless encryption / passwords

Rogue Device: Information Exchange

(PRE-ENGAGEMENT)

FROM CLIENT

TO CLIENT

(POST-ENGAGEMENT)

FROM CLIENT

- Alerts or Response performed, this helps the engagement team identify risk values for findings

TO CLIENT (OUTSIDE OF EER)

Scenarios to add

- CxO Breach Training
- Password Audit scenario
  - Windows (Domain Controller)
  - SSO / Hashing
- Table top scenario (Security Architecture)
- Vendor proving ground

End

Questions?