From Salmon to Scarlet
Getting The Most Out of The Many Shades of Red

Ed Skoudis
@edskoudis
#SANSHackFest
November 16, 2015

Welcome to the SANS HackFest
• Thank you for joining us!
• We’ve been planning and building this for a year
• We’ve got an awesome event for you
What’s On Tap?

- 2 Days of In-Depth Summit Talks
- 3 Nights of NetWars
- Coin-a-palooza during NetWars
- Special Surprise “HackFest Hits the Road” Session
  -- Featuring JoMama’s Sooper Sekret Cookies!
- 6 In-Depth Courses
- Hacking the “Internet of Things” Thing
- A Night of CyberCity Missions
- Special Closing Ceremony on Monday, Nov 23

SANS Pen Test HackFest Agenda

<table>
<thead>
<tr>
<th>Mon Nov 16</th>
<th>Tues Nov 17</th>
<th>Wed Nov 18</th>
<th>Thurs Nov 19</th>
<th>Fri Nov 20</th>
<th>Sat Nov 21</th>
<th>Sun Nov 22</th>
<th>Mon Nov 23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summit 9 AM to 5:30 PM</td>
<td>Summit 9 AM to 4:30 PM</td>
<td>Classes 9 AM to 5:30 PM</td>
<td>Classes 9 AM to 5:30 PM</td>
<td>Classes 9 AM to 5:30 PM</td>
<td>Classes 9 AM to 5:30 PM</td>
<td>Classes 9 AM to 5:30 PM</td>
<td>Classes 9 AM to 3 PM</td>
</tr>
<tr>
<td>NetWars w/ Coin-a-Palooza 6:30 PM to 9:30 PM</td>
<td>Hackfest Hits the Road 5:00 PM to 10 PM</td>
<td>Hacking The Internet of Things Thing 7:15 PM to 9:15 PM</td>
<td>NetWars w/ Coin-a-Palooza 6:30 PM to 9:30 PM</td>
<td>CyberCity 6:30 PM to 9:30 PM</td>
<td>CyberCity 6:30 PM to 9:30 PM</td>
<td>CyberCity 6:30 PM to 9:30 PM</td>
<td>Brief Closing Session 3 PM</td>
</tr>
</tbody>
</table>
Thank You to Our Sponsors!

Pen Test HackFest Themes

• Offense helps cyber defenders & DFIR professionals
• The continuing evolution of offensive capabilities
• Multi-faceted offensive skills
• We must strive to provide technical excellence with great business value
Please Help Make This Special

• We’re a community of friends & colleagues
• We want you to get as much value out of this as you can
• Interact with speakers, instructors, staff
• Introduce yourself to others... make friends
• Please take advantage of our evening sessions
  – Lots of learning, but also a lot of FUN!

The Many Shades of Red

Auditors
Vuln Assessors
Pen Testers
Red Teamers

Width:
Approx # of Jobs

Depth:
Relative Technical Complexity

Where do you fit?
Where do you want to fit?

Security
Researchers
Pen Testing Rut

- Pen testing, as it is commonly understood, has a fixed time span, narrow scope, and a focus on finding vulnerabilities
  - And exploiting them only as time is available
- In doing this, we sacrifice realism, stealth, depth, and understanding deep business implications
  - And most importantly, determining whether Blue is ready to detect and respond to real-world attackers

The Move Toward Red Teaming

- Engagements tend to be longer (instead of 1-2 week pen test)
  - Months or even continuously
- Often done without a fixed starting date / time
- Internal red teams tend to know the “lay of the land”
- Useful in determining changes of security stance over time
Adversary Simulation

• Applying the Red Team deeply
  – Face the Red Team against the Blue/Hunt Team
  – Apply techniques used by real-world attackers
  – Include surprise, stealth, lateral movement
• Focus on measuring detection and response
  – Very useful... but can feel a bit “messy”

The Foundations of Red vs. Blue

• Considering the evolution from Vuln Assessment → Red Team / Adversary Simulation, what’s the real purpose of Red?
  – To help prioritize resources and heighten defenses
  – To make Blue better
  – This will help us provide more business value
Metrics and Continuous Improvement

• To provide some structure, consider this process:
• Red discusses with Blue the general techniques they’ll use
  – Spear phishing... something that nearly guarantees access
  – Or, just assume compromise & pivot mercilessly
• Establish time metric for Blue to detect
  – 2 weeks of active infiltration & exfil sim
    as a first blush for an inexperienced Blue
• Establish a scope (fairly widespread)
• GO!

Did Blue Detect Red in Time?

• No...
  – Red helps explain to Blue what they did, and they brainstorm how to
detect it better, faster, and in a more distributed fashion
  – Red sharpens Blue
• No! But they detected a real bad guy – WIN!
• Yes!
  – Blue then shows how it detected Red
  – Tweak scope, enhance allowed Red techniques, lower timeframe (1 day)!
  – Blue sharpens Red
Conclusions

• It used to be OUTLANDISH to say “I’m going to pay people to hack my stuff.”
  – Now, unless you do get a pen test or red team assessment, you aren’t exercising your due diligence

• As you participate in the HackFest, think about how Red and Blue can sharpen each other

References

• Raphael Mudge Blog, “Models for Red Team Operations”

• Ed Skoudis presentation, “How to Give the Best Pen Test of Your Life”
  – http://is.gd/8OAXRN

• Robin Mejia article, “Red Team Versus Blue Team: How to Run an Effective Simulation”, CSO Online
  – http://www.csoonline.com/article/2122440

• Raphael Mudge Blog, “Red Team Tradecraft”