You’re Probably Not Red Teaming
...and Often, I’m Not Either
My Job is Fun
We Don’t Belong in Here!
I Get Inside Quickly and Quietly
I Get Inside Quickly and Quietly
I Get Inside Quickly and Quietly
I Bet Many People Here Believe That What You Just Saw is “Red Teaming”
I Bet Many People Here Believe That What You Just Saw is “Red Teaming”

... It’s Not.
Where The Red Team Fits Has Been Discussed Previously...
by Folk Way Smarter, Cooler, and More Attractive Than Me
Talk of Purple Teaming is Becoming Popular
Talk of Purple Teaming is Becoming Popular

“That's when the Red Team sends an extra person to sit in the SOC with the Blue Team... and then they get to charge the client double.”

- Chris Gates
There Are Three Elements To Security
There Are Three Elements To Security
There Are Three Elements To Security
1. Digital
2. Physical
3. Human
And There’s Crossover
And There’s Crossover

EP Convergence
- Attacks on physical systems that are network enabled

Electronic
- Network Penetration Testing
- Surveillance & Implants

ES Convergence
- Phishing
- Pretexting
- Creating moles
- Blackmail

Physical
- Direct attack on facilities and systems

Social
- In person Social Engineering
- Phone conversations
- Social profiling
- Baiting

PS Convergence
- Targeting
- Impersonation
Attacking via the Physical Vector
Covert Methods of Entry
Covert Methods of Entry
Covert Methods of Entry
Covert Methods of Entry
Covert Methods of Entry
Covert Methods of Entry
Covert Methods of Entry
Attacking via the Digital Vector
Network Security & Access Control Systems
Network Security & Access Control Systems
Network Security & Access Control Systems
Attacking via the Human Vector
Look Like You Belong There
Look Like You Belong There
Look Like You Belong There
Look Like You Belong There
Look Like You Belong There
Some Stories... and Some Questions
Story Number One: Elevator Repair
Elevator Technician is a Great Cover Story
Elevator Technician is a Great Cover Story
Elevator Technician is a Great Cover Story

1. This is a test.
Elevator Technician is a Great Cover Story

1. This is a test.
2. Can you hear me?
Elevator Technician is a Great Cover Story

1. This is a test.
2. Can you hear me?
3. Can you identify my location?
A Metal Contractor Clipboard is Awesome
A Metal Contractor Clipboard is Awesome
So I’m in the Building...
...Teammate Had to Go Back to the Hotel
I’ve Got Nothing But Time
I’ve Got Nothing But Time
Things at the Hotel Were Going Slowly
Things at the Hotel Were Going Slowly
Then I Nearly had a Heart Attack
I Figured it Must Be The Cleaners
It Wasn’t
It Wasn't
Fortunately, I’m a Friendly Elevator Technician
“I’ll Have to Check the Elevator Controller in Here”
Everyone Wants to Keep the Elevators Working
Story Number Two: The Cable Technicians
Preliminary Recon
“Look Like You Belong There”
“Look Like You Belong There”
The Cable Technicians
The Cable Technicians
Make a New Friend!
We’re Totally Legit... Trust Us.
Do You Think He Verified Our Story?
How Did We Get In?
How Did We Get In?
Later, Inside the Office
Later, Inside the Office
The Client Actually Pulled the Dispatch Tickets
The Client Actually Pulled the Dispatch Tickets
The Client Actually Pulled the Dispatch Tickets
The Client Actually Pulled the Dispatch Tickets
The Client Actually Pulled the Dispatch Tickets

<table>
<thead>
<tr>
<th>TIME:</th>
<th>2:49</th>
<th>DATE:</th>
<th>2017/08/01</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDRESS:</td>
<td>200 S Mathilde Ave</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CITY:</td>
<td>Sunnyvale, CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUITE:</td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLOOR:</td>
<td>ground</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZONE OR ALERT:</td>
<td>Door 5-21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS THIS COUNTED AS A SITE CHECK?</td>
<td>[ ] YES [x] NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARRIVAL TIME:</td>
<td>3:03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLEAR TIME:</td>
<td>3:22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DISPOSITION OF CALL:</td>
<td>Can’t find any signs of forced entry. Verizon is working in the building and may have propped door open.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMO NOTES:</td>
<td>Instructed Verizon field technician to keep all doors closed for first 30 seconds, they will alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIGNATURE:</td>
<td>[Signature]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

redteamalliance.com
Who Wouldn’t Trust Us?
A Lot of the Time, Guards are Rather Untrained
A Lot of the Time, Guards are Rather Untrained
Armed Guards are Usually More On the Ball
We Wanted to Grab Credentials
We Wanted to Grab Credentials
We Wanted to Grab Credentials
We Wanted to Grab Credentials
We Wanted to Grab Credentials
What Do Many Armed Guards Want To Be?
What Do Many Armed Guards Want To Be?
Send in a Cop!
Meanwhile, Babak is Still Out in the Car
Rob Keeps Trying, The Guards Keep Blading
Time to Wrap it Up and Say Goodbye
 Surprise Hug!
Robert Comes Back to the Car
We Checked the Logs
Now Whose Permissions Did We Have?
We Came Back on Their Next Shift
We Overrode an Elevator Restriction
We Picked Open a Door Lock
We Picked Open a Door Lock
And We Laid Hands Upon Their Server Racks
Which Scenario Was Red Teaming?
Some People Apply the “All Surfaces” Litmus Test

EP Convergence
Attacks on physical systems that are network enabled

Electronic
- Exploitation
- Lateral Movements
- Implants

ES Convergence
- Phishing
- Profiling
- Creating moles
- Blackmail

Physical
- Direct attack on facilities and systems
- Surveillance / Bugging

Social
- In person Social Engineering
- Phone conversations
- Social profiling
- Baiting

PS Convergence
- Tailgating
- Impersonation

redteamalliance.com
Story Number One: Elevator Repair
I Walked Into A Building and Hid

[ ] Physical
[ ] Digital
[ ] Human
I Encountered Security

[ ] Physical
[ ] Digital
[ ] Human
I Offered My Cover Identity and Showcased Skills

[  ] Physical
[  ] Digital
[✓] Human
I Was Granted Escorted Access Everywhere

[ ] Physical
[ ] Digital
[✓] Human
I’d Call This Social Engineering

[ ] Physical
[ ] Digital
[✓] Human
Was This a Red Team Engagement?

[   ] Physical
[   ] Digital
[✓] Human
Noooooo,
Nooooooonn...
Story Number Two: The Cable Technicians
We Spotted a Guard

[ ] Physical
[ ] Digital
[ ] Human
We Befriended a Guard

[ ] Physical
[ ] Digital
[✓] Human
We Bypassed a Door Lock

- Physical
- Digital
- Human
We Bypassed Another Door

- Physical ✓
- Digital [ ]
- Human ✓
A Blended Attack... On Two Surfaces

[✓] Physical
[ ] Digital
[✓] Human
Was This a Red Team Engagement?

- Physical [✓]
- Digital [ ]
- Human [✓]
HOW ABOUT NO?
Story Number Three: The Armed Guards
We Prepared a HuntPad

[ ] Physical
[ ] Digital
[ ] Human
We Established Rapport

[ ] Physical
[ ] Digital
[✓] Human
We Grabbed RFID Card Data

[ ] Physical
[✓] Digital
[✓] Human
We Wrote New Badge Data

- [ ] Physical
- [x] Digital
- [x] Human
We Bluffed Past More Guards

[ ] Physical
✓ Digital
✓ Human
We Overrode an Elevator

[ ] Physical
✔️ Digital
✔️ Human
We Picked Locks

- Physical
- Digital
- Human
We Entered the Server Room

[✓] Physical
[✓] Digital
[✓] Human
We Feigned Network Attacks

- Physical
- Digital
- Human
Was This a Red Team Engagement?

[✓] Physical
[✓] Digital
[✓] Human
YEAH THAT'S GONNA BE A NO FOR ME DOG
Ahhhh... The Question of How Much Scope
Ahhhh... The Question of How Much Scope

Is *That* What Makes Something a Red Team Engagement?
Ahhhh... The Question of How Much Scope

for all you "you can apply scope to a red team gigs types", the TL;DR here was 'spearphish wife, get creds' - motherboard.vice.com/read/teens-who ...

2:46 PM - 20 Jan 2016

I always felt varied Red Team pentesting with capable attackers and an open scope is the only way to prove effectiveness against current real world threats...

10:35 AM - 28 Jan 2018

“Today’s adversaries don’t play by any rules. They constantly adapt and the complexity of their tactics and thinking is ever increasing”

7:30 AM - 17 Oct 2017
Scope Absolutely Has a Place in Red Teaming
Scope Absolutely Has a Place in Red Teaming
Stop Thinking You Know More Than The Client
What Threat Are You Being Hired To Model?
What Do Clients Ultimately Care About?
What Do Clients Ultimately Care About?

Is a Given Vulnerability Going To...

1. Cost Me Money
2. Make Me Look Bad
“Cost Me Money”
“Make Me Look Bad”
(Many Times the Two are Related)
Your Job as a Red Teamer...
Your Job as a Red Teamer...

1. Think Unconventionally
Your Job as a Red Teamer...

1. Think Unconventionally
2. Attack Across All Surfaces
Your Job as a Red Teamer...

1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
Your Job as a Red Teamer...

1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact
Your Job as a Red Teamer...

1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact
5. ...
What Else is Missing?
Your Job as a Red Teamer...

1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact
5. Interface with the Blue Team
I Love the Sparring Analogy
This is What Many Folk Think “Red Teaming” Is
This is What You Want to Eventually See
Build This Into Your Jobs
Build This Into Your Jobs

January

<table>
<thead>
<tr>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Recon</td>
<td>Recon</td>
</tr>
<tr>
<td>Plan &amp; Prep</td>
<td>Wreck Shit</td>
<td>Wreck Shit</td>
<td>Wreck Shit</td>
<td>Gather Findings</td>
<td>Write Report</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Build This Into Your Jobs

<table>
<thead>
<tr>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research the Target While Flying There</td>
<td>Wreck Shit</td>
<td>Wreck Shit</td>
<td>Wreck Shit</td>
<td>Hustle to Next Job</td>
<td>Last Job Ran Long</td>
<td>Laundry &amp; Repack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>21</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>27</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>
# Build This Into Your Jobs

<table>
<thead>
<tr>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Achieve Objectives</td>
<td>Achieve Objectives</td>
<td>Achieve Objectives</td>
<td>Achieve Objectives</td>
<td>Recon</td>
<td>Recon</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>Recon</td>
<td>Recon</td>
<td>Practice w/ Blue Team</td>
</tr>
<tr>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>After-Action Meetings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[redteamalliance.com](http://redteamalliance.com)
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Real-World Examples
Remember... The Best Red Teamers

1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact
5. Interface with the Blue Team
A Bonus Gift For You All
I’ve Talked About Telephony Systems Before...
...Remember: Many Cabinets are Keyed Alike
Keyed-Alike Systems

A126 Linear Key
Availability: In stock
Product Code: KEY LINEAR
Product Price: $5.24

Description
Key for Linear Products

Features
Key for Linear Products
People who viewed this item also viewed

- Door King 16120 Double Sided Key: $11.95, Free shipping
- Manufacturer Original PK625...: $9.99, Free shipping
- Misc. Fire and Security Key Lo...: $21.00, + $2.25
- Misc. Fire and Security Key Lo...: $41.00, + $2.50

Door King 16120 Double Sided Key

- Item condition: New
- Quantity: 1, 3 available / 27 sold
- Price: US $14.95
- Add to cart
- Best Offer: Make Offer
  - 10 watching
  - 27 sold

Seller information
agharezao10 (123 ★)
100% Positive feedback

Follow this seller
See other items

Free shipping
Keyed-Alike Systems
Keyed-Alike Systems
Other Very Useful Keys...
Keyed-Alike Systems

CH751

redteamalliance.com
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
Keyed-Alike Systems
EMKA Industrial Keys
EMKA Industrial Keys

[Image of various lock components and keys]

redteamalliance.com
EMKA Industrial Keys

EK 222

EK 333

2233X
Dev’s Everyday Carry Set
Dev’s Everyday Carry Set

[ ] Physical
[ ] Digital
[ ] Human
Dev’s Everyday Carry Set

[ ] Physical
[ ] Digital
[✓] Human

FEO-K1
Dev’s Everyday Carry Set

- Physical
- Digital
- [ ] Human

FEO-K1
EK333
222343
Dev’s Everyday Carry Set

Physical

Digital

Human

FEO-K1
EK333
222343
C415A
Dev’s Everyday Carry Set

[✓] Physical
[ ] Digital
[ ] Human

FEO-K1
EK333
222343
C415A
CH751
Dev’s Everyday Carry Set

- ✔️ Physical
- ✔️ Digital
- [ ] Human

FEO-K1
EK333
222343
C415A
CH751
16120
Dev’s Everyday Carry Set

[✓] Physical
[ ] Digital
[ ] Human

FEO-K1
EK333
222343
C415A
CH751
16120
Jigglers
Dev’s Everyday Carry Set

[ ] Physical
[ ] Digital
[✓] Human

FEO-K1
EK333
222343
C415A
CH751
16120
Jigglers
1284X
Dev’s Everyday Carry Set

FEO-K1
EK333
222343
C415A
CH751
16120
Jigglers
1284X
Dev’s Everyday Carry Set

then what’s this?

FEO-K1
EK333
222343
C415A
CH751
16120
Jigglers
1284X
Dev’s Everyday Carry Set

that's my wire loop

FEO-K1
EK333
222343
C415A
CH751
16120
Jigglers
1284X
Dev’s Everyday Carry Set
Dev’s Everyday Carry Set
Dev’s Everyday Carry Set
Learning More
SANS Orlando is Around the Corner
SANS Orlando is Around the Corner
In Conclusion
Untangling the Terminology

“I want a pentest”
(can mean so many things)

- Compliance
  - Controls Audit
  - Greybox
  - Blackbox
- Risk Reduction
  - Whitebox
  - Code/Arch Review
- Attacker Simulation
  - Scan
  - Red Team

https://twitter.com/coffeetocode/status/794593057282859008

redteamalliance.com
“On Pentesting, Professionalism, & Chill”

https://coffeetocode.net/2016/09/on-pentesting-professionalism-chill
Work Together to be Better Together
Getting in is Fun... Getting Caught is the Goal
Let’s Keep Making Things Better
Thank You Very Much

deviant@redteamalliance.com at the office

@deviantollam on twitter

“whiskey, neat” at the bar