THE SAD TALE OF ETAOIN SHRDLU AND THE DANGER OF AUTOMATED PEN TESTS

Doug White
Chair, Cybersecurity and Networking
Roger Williams University
Bristol, RI
dwhite@rwu.edu
The Sad Tale of Etaoin Shrdlu*

- It’s pronounced Ethan Allen, my Mother was Welsh.
  - float dougsBankAccount;
  - dougsBankAccount = urPayck-(long)urPayck; //short change salami attack

- But how can the payload be delivered?

- *whitehat
The Dream...

- ...Caused by the Flight of a Bee around a Pomegranate a Second before Awakening – Reality
- ☒ Pen Test – (the dream)
Since the Dawn of Time...

- Human beings like to check boxes
- I mean, they really do
- A sense of accomplishment
- A job...well...done
- A sense of....Compliance!
But not too many boxes!

- Compliance can be overwhelming
- How many subparts of COBIT are there?
Also, since the dawn of time...

- Humans hate having their shortcomings and weaknesses pointed out by hackers and con men.
also, also, since the dawn of time...

- and, we really like having someone tell us: “Everything is going to be ok. You can trust me, I’m a doctor.”

![Image of vintage advertisement for Luckies cigarettes]
Enter the Automated Pen Test

- These kids today...
- Can you click F4?
- Yay!
- ☒ Pen Test
- Here is your PDF, that
  - will be 5,000$
But, what if it’s Console ports?

- “Our server rack has a lock.”
- “That door is ‘hardened’ against entry.”
- “Well, normally, that window is locked.”
- “The guards don’t have tasers.”
What if it’s “Taco Truck Tuesday”? 

- What if I get you to deliver the payload? 
- Spearphishing is the number one type of attack? 
- Spearphishing circumvents everything because it relies on human behavior rather than open ports and vulnerabilities. 
- Spearphishing is not going to be seen in automated pen tests
The Sad Tale of L. B. Jeffries*

- I know, I know, you won’t get Spearphished!
- How about a little Van Eck Phreaking (well, not really)?
- Is the network key really written on that post it note? Really?
- Oh, and was the password for the admin on that post it note too?
- That automated test didn’t detect...
- I also called this “Rear Window”
- *whitehat
So, what’s the point Doug?

- All too often, we see mid size and even large organizations relying on
  - “The Cheapest”
  - “The Fastest”
  - “The Easiest”
  - “The Most Efficient”
- methods for checking that box
As the Security environment continues to mature (well, that’s relative), we increasingly see the involvement/request of “fully automated pen tests” and “discount pen testers” and pretty soon...

Come on down to Crazy Eddie’s Pen Test Discount Warehouse, where prices are INSAAAANE!

All industries go through this type of movement from:
- whacky inventors – “weird science”
- startups – “should I be wearing a tie?”
- Reputable and disreputable – “We are not like those other guys?” and “We’re wearing ties.”
- Maturation – “Safe, reliable, efficient, cost effective”
- Underwriting
- Crazy Eddie
The reality is?

- All of us seek the Banker but we also secretly crave Crazy Eddie!
So, we shouldn’t do automated Pen Tests?

- Absolutely, you should but it should be the first thing you, not the last.
- APT can be the trigger which causes audit but even then, it shouldn’t be the only trigger.
- The Triangle Shirtwaist Factory Fire.
  - Are we locking doors that need to be unlocked?
  - Are we locking doors that need to be unlocked?
  - Are we locking doors that need to be unlocked?
How do you find the balance?

- That is where you have to take a serious step
  - (serious) Evaluation of threats
  - Risk Acceptance
  - Risk Avoidance
  - Risk Limitation (reduction)
  - Risk Transference

- Die Rückkehr von Etoain
  - The bank did NOT want to document exposure
  - Instead, security through obscurity was assumed and this reinforced the idea of simple, checkbox pen tests. All is well, nothing to see here.
  - This is, of course, Risk Acceptance or Risk Denial
The failure facet fulcrum

- The Facet of Oversimplification
- The Facet of Budgetary Pressure
- The Facet of Ego
- The Facet of Complacency
- The Facet of Failure
- The Facet of Ignorance
Apply: What to do?

- You must have a full understanding of the Risk Structure YOU wish to adopt that suits your risk profile
  - This means budget must be applied accordingly, even when it hurts!
  - This means you can’t just push that button and check that box
  - You can live in the wild west but remember there is always a new gun in town
- You must remember that humans will find a way and that humans are involved, not just automated attacks (although those are getting better too)
- You must avoid assumption of risk scenarios unless you truly understand them and the cost of this assumption
- Start with Automated Pen Tests, but don’t end with them.
Apply: What to do?

- Always be asking yourself: “Am I just ticking a box or do I understand the risk?”
- Always be asking yourself: “What else can happen? Not just what I want to see?”
- Always be asking yourself: “What are the consequences if I assume this risk?”
- Always be telling yourself: “I am not invulnerable.”
- Always be telling yourself: “We are a target.”
- ABD: “Always be deposing.”
Questions?

- dwhite@rwu.edu
- @dougwhitephd
- securedigitallife.com
- securityweekly.com
- Doug White, PhD, CCE, CCNA, CISSP, PI(RI)