YOUR FLY IS OPEN

PERSPECTIVES ON PENTESTING FROM A PROFESSIONAL VICTIM

TOM LISTON
SENIOR SECURITY CONSULTANT
DARKMATTER - UAE
I AM A PROFESSIONAL VICTIM

• Don’t shed a tear…
• I’ve run a honeypot for the better part of the last six years
• It tweets when attacked. Follow @netmenaces on twitter
• It is getting close to sending its 325,000th tweet
AT YOUR SERVICE

- HTTP (80/TCP)
- MSSQL (1433/TCP, 1434/UDP)
- MYSQL (3306/TCP)
- FTP (21/TCP)
- Terminal Services (3389/TCP)
- SSH (22/TCP)
- VNC (5900/TCP)
- RADMIND (4899/TCP)
- SIP (5060/UDP)
- TELNET (23/TCP)*
I ALSO WRITE A BLOG...
BUT REALLY, WHO DOESN’T?

• I WRITE UP INTERESTING (TO ME) STORIES ABOUT SECURITY AND RUNNING A HONEYPOT IN A HUMOROUS (TO ME) AND DELIGHTFULLY (TO ME) IRREVERENT STYLE

• IF YOU READ MY BLOG – THANK YOU
OTHER INTERESTING FACTS

- I’ve never been groped by Donald Trump
- I DO NOT run my own private email server
- No, I am not Jim Gaffigan
- No, I don’t know if Jim Gaffigan has been been groped by Donald Trump or if he runs his own private email server.
I NEED A "VOLUNTEER"

- Ed Skoudis
- Josh Wright
- Tim Medin
A “VISCERAL” DEMONSTRATION

• I WANTED TO CREATE A DEMONSTRATION OF WHAT BEING AN INTERNET VICTIM WAS LIKE
• I BOUGHT THIS LITTLE INTERNET-CONNECTED BLINKY LIGHT “CUBE THINGIE”
• REVERSE-ENGINEERED DEEPLY RESEARCHED THE API AND GOT IT TO LIGHT UP DIFFERENT COLORS WHENEVER MY HONEYPOT TWEETED
• IT ANNOYED MY WIFE AND KIDS, BUT JUST DIDN’T SEEM TO BE A “VISCERAL” ENOUGH DEMONSTRATION
SO I CAME UP WITH SOMETHING ELSE...
“THE TAKE-AWAY”

- SANS CONFERENCES AND SANS SUMMITS ARE ALL ABOUT “THE TAKEAWAY”
- THE IDEA IS TO GIVE YOU INFORMATION THAT YOU CAN TAKE BACK AND PUT TO USE RIGHT AWAY
STUFF I’VE LEARNED:
THREE “TAKE-AWAYS”

• The “Big Picture” Take-Away
• The “Current Events” Take-Away
• The “Philosophical” Take-Away
TAKE-AWAY #1 – "BIG PICTURE"
WE’RE JUST PLAYING WITH OURSELVES

- As security professionals, we spend a great deal of our time within a "self-selected echo chamber"
  - Our clients and our colleagues are all "security conscious"
- It’s an incredibly bad idea to make generalizations about the state of the internet as a whole based off that experience
THE SETUP...

• **When was the last time you found something really interesting doing an external network pentest?**

• **As pentesters, we all are walking around having internalized the notion that we’re really not going to find much “on the outside” anymore**

• **We’ve even changed tactics to the point where an “external pentest” is now likely focused on client-side attacks**
The Conclusion...

- Things have gotten better on the Internet...
THE REALITY...

• Things are WAY worse on the Internet than you think they are

• Your clients make up a very small, very insular subset of the actual Internet
THANK YOU, “INTERNET OF THINGS”

- **The great bulk of that traffic is from internet connected video cameras and DVR devices that were manufactured with difficult to change, default passwords**

- **Attached to the ‘net by clueless folks who are now part of the biggest, baddest botnet ever**
WHO ARE THESE PEOPLE?

- The bulk of systems connected to the internet are owned and operated by people who don’t hire pentesters.
- Individuals & small businesses who have been sold the idea that the internet is “easy”.
- They’re dropping like flies.
THE UPSHOT...

- Yes, our orgs (or our client orgs) are getting more secure
- Unfortunately, those folks make up a smaller and smaller portion of the actual Internet
TAKE-AWAY #2 – "CURRENT EVENTS"
ONLY THE SHADOW KNOWS...

• "Shadow IT" is a real, and dangerous thing
• Over the past three months, I’ve notified four separate large orgs about cloud deployments they didn’t know they had
• They all argued with me
• They all ended up being wrong
• None of them apologized… (Just sayin’…)
Example:

“BIG-COMPANY-THAT-REALLY-SHOULD-KNOW-BETTER”

- Microsoft "partner"
- Attacks sourcing from Amazon's EC2
  - Wait... wut?!? Not Azure
- First indicator: inbound RDP
- I "knocked" back...
  - Real, SSL cert for "$COMPANY_NAME.ME"
  - NOT a self-signed cert
EXAMPLE (CONTINUED):
“BIG-COMPANY-THAT-REALLY-SHOULD-KNOW-BETTER”

- **Communication #1:**
  - "Hey guys, is this yours? Seems like it might be..."

- **Response #1:**
  - "Nope, not ours..."
EXAMPLE (CONTINUED):
“BIG-COMPANY-THAT-REALLY-SHOULD-KNOW-BETTER”

• Communication #2:
  • "Uh... It’s got a real root-signed SSL cert that kinda looks like it might belong to you”

• Response #2:
  • “Nope, not ours...”
EXAMPLE (CONTINUED):
“BIG-COMPANY-THAT-REALLY-SHOULD-KNOW-BETTER”

- I “KNOCK” A LITTLE HARDER
- I FIND AN HTTPS WEBSERVER RUNNING ON AN ODDBALL PORT
  - SITE ABSOLUTELY LOOKS TO BE ASSOCIATED WITH THEM
  - IT HAS THEIR LOGO
- USES SAME SSL CERT
- CHECK PASSIVE DNS ASSOCIATED W/ THE .ME DOMAIN AND FIND A WHOLE BUNCH OF DNS NAMES
  - EITHER ITS THEIRS, OR SOMEONE’S GOT AN AMAZING SCAM GOIN’ ON
EXAMPLE (CONTINUED):
“BIG-COMPANY-THAT-REALLY-SHOULD-KNOW-BETTER”

- **Communication #3:**
  - “**Sorry to beat a dead horse, but either this is yours, or you’ve got a HUGE problem**”
  - “**Here’s why...**”

- **Response #3:**
  - “**Why do you keep bothering us about this?**”
  - “**It **ISN’T** OURS**”
EXAMPLE (CONTINUED):
“BIG-COMPANY-THAT-REALLY-SHOULD-KNOW-BETTER”

• SEVERAL DAYS PASS...

• UNSOLICITED RESPONSE #1:
  • “HOLY CRAP! PLEASE SEND US EVERYTHING YOU KNOW ABOUT THIS SYSTEM…”
EXAMPLE (CONTINUED):
“BIG-GO-THAT-REALLY-SHOULD-KNOW-BETTER”

• WHAT THEY DIDN’T KNOW:
  1. THEIR DEVS USED A COMPANY CREDIT CARD TO STAND UP EC2 INFRASTRUCTURE
  2. THEY PURCHASED A DOMAIN AND SSL CERTS
  3. THEY USED IT TO DEMO CUSTOMIZED PRODUCT TO CLIENTS
  4. THEY ADMINISTERED THE WHOLE THING VIA RDP WITH CRAPPY PASSWORDS AND IT GOT OWNED
THE TAKE-AWAY

• How do you help your org or your clients to **find** something like this?

• This is a HUGE and GROWING problem

• It’s **WAY** too easy for anyone in an org to stand up this kind of shadow **IT**
TAKE-AWAY #3 – "PHILOSOPHY"

GOOD GUYS WEAR BLACK...
(…T-SHIRTS WITH WITTY SAYINGS ABOUT BINARY THAT NORMAL PEOPLE SIMPLY DON’T UNDERSTAND)

• I notify LOTS of people that they’ve been hacked
• It’s rarely pretty
• I also end up crossing paths with the bad guys a lot
  • The non-targeted, non-nation state, non-APT type
• Most of the bad guys turn out to be self-entitled jerks with badly broken ethical compasses
SPEEDY PAPER

• "TERM PAPER ASSISTANCE"
• HUNDREDS OF SITES HACKED
  • THE U.S. CAPITOL, THE NAVY LEAGUE, AND (GASP!) SKYLINE CHILI
  • ADDED LINKS TO THE SPEEDY PAPER SITE – SEO!
• THEY HAVE AN ACTIVE TWITTER ACCOUNT
  • I... WELL... I KINDA’, SORTA’ PUBLICLY CALLED THEM OUT
“IT WAS OUR COMPETITORS”

- They responded!
  - Annoyingly smugly...
  - But they responded
- “We believe our competitors did it to make us look bad”
  - Sure they did...
  - ‘Cause that’s what competitors do...
OPERATING WITH ABANDON...

- The bad guys aren’t afraid of being caught
- They operate with — literally — no fear of consequences
- We are all that stand in their way
FIGHTING THE GOOD FIGHT

• **It isn’t hyperbole to state that in this Internet age, we’re the ones fighting the good fight**

• **There are bad, morally bankrupt people out there and we — literally — are the only check on their activities**

• **You are “the good guys”**

• **The fact that you’re here, wanting to get better at what you do is proof of your commitment to that fight**

  • **Remember: If you’re coasting, you’re going downhill**...
SLEEP SOUNDLY, MY FRIENDS...

• **AFTER RUN-INS WITH THE BAD GUYS I ALWAYS HAVE TWO QUESTIONS**
  - “HOW DO THEY SLEEP AT NIGHT?”
  - “WHAT DO THEY TELL THEIR KIDS THEY DO FOR A LIVING?”
WHEN YOU GET HOME FROM THE CONFERENCE, DO ME A FAVOR...

• TALK TO YOUR KIDS ABOUT WHAT YOU DO
• TELL THEM YOU’RE ONE OF THE GOOD GUYS
BONUS TAKE-AWAY – "DON’T DESPAIR"
THERE’S ALWAYS A WAY IN...
(YOU JUST HAVEN’T THOUGHT OF IT YET)

• Performing a test against the network infrastructure of THE telephony/internet provider for an entire eastern European country
• I spent the whole 16-hour flight worrying
  • "How the hell will we get anywhere? This is a telephone company - and we’re testing INFRASTRUCTURE!"
IT Turns OUT...

• You COULD Own the network Infrastructure for an Entire Country FROM the Network USED by a Cable-TV Set-Top Box USING DEFAULT Password FOR TACACS
• There’s always a way in... and it’s often easier than you think.
• No matter how good you may think they are...
• No matter how good they may think they are...
• To quote Leonard Cohen (and fraVia+): “there’s a crack, a crack in everything: that’s how the light gets in...”

yourliftisonopen.com
QUESTIONS? COMMENTS?

- **Tom Liston**
  - tom.liston@darkmatter.ae
  - tliston.phone@gmail.com
  - @tliston
  - @netmenaces
  - http://www.yourflyisopen.com