Offensive Threat Modeling for Attackers

turning threat modeling on its head

Rafal M. Los – Chief Security Evangelist – HP Software
Shane MacDougall – Principal – Tactical Intelligence

Abstract

Modern *threat modeling* is a defensive response to understanding a threat so as to prepare yourself, your network, and your assets. This talk shows how threat modeling can be used as an *offensive* weapon. While traditional threat modeling looks at the attacker, the asset and the system – offensive threat modeling looks back at the defender to understand his tactics and expose weaknesses.

By adopting the five P's - People, Points, Posture, Pwnage, Poll – an attacker can understand where best to strike to inflict the most optimal result.

This talk focuses heavily (but not exclusively) on the human side of the defensive equation to *get inside the mind of the defender*. Combining expertise in intelligence gathering through social reconnaissance and various other methods of social engineering with expertise in traditional threat modeling and penetration testing – this talk yields a powerful new weapon in the attacker's toolbox.

Much like a spy movie plot, this talk will provide the attacker with the necessary tools to know their target, control the situation more effectively, and have a greater chance at successfully reaching their goal. This talk is meant to be used to understand how the other side (the attackers) sees you (the defenders) in any scenario and what the defenders should expect … to formulate a solid defensive posture.

Threat Modeling Primer

what is threat modeling?

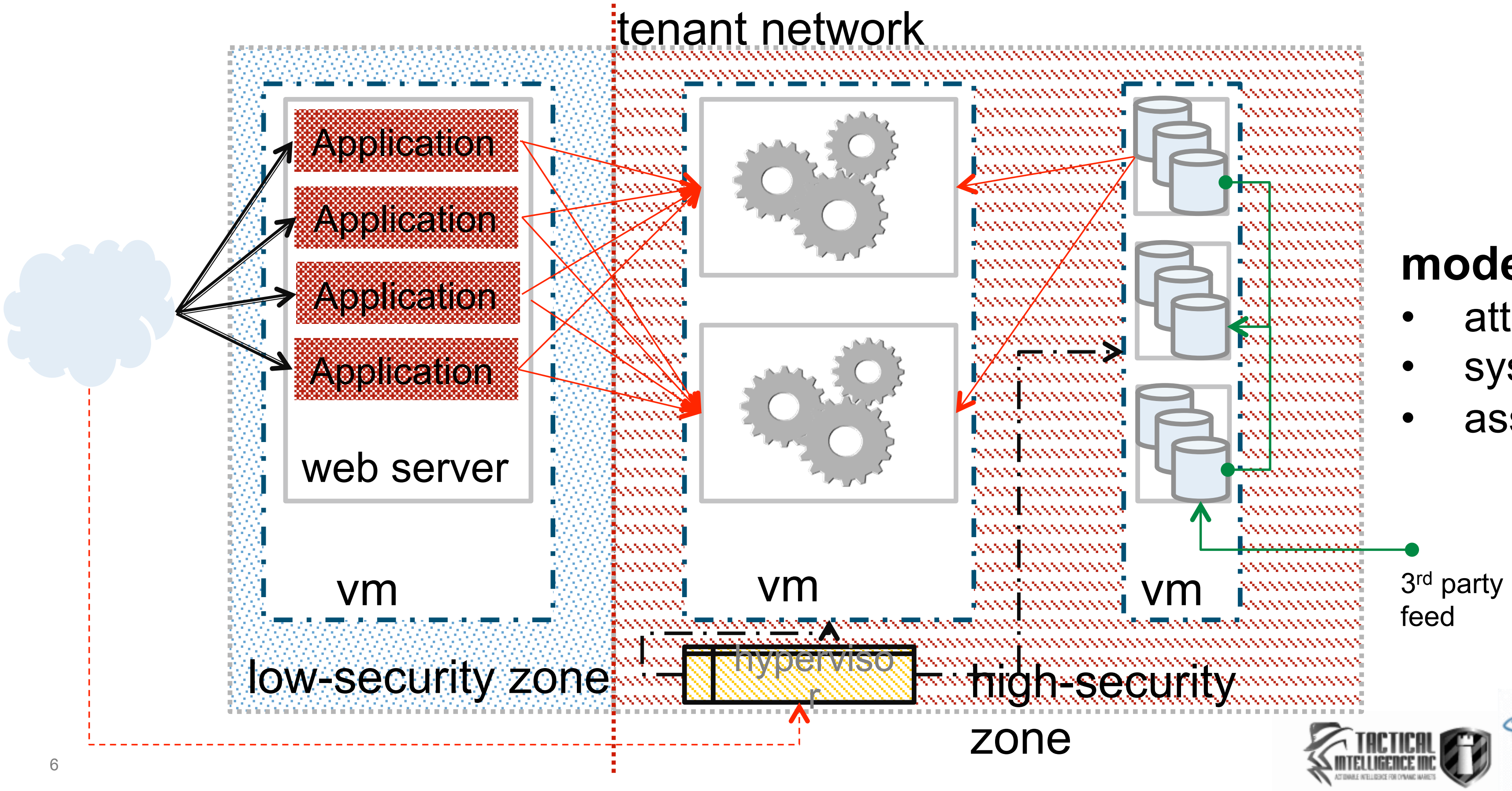
- **analysis** which exposes *possible threat vectors*, leading to better understanding of a system, asset, or attacker for **defensive** purposes
- primary used as a tool to develop defensive countermeasures
- currently focuses on analysis of system, asset or attacker
- “understand the attack” > “design a compensating defense”
- “how will this be attacked?” “where should we fortify defenses?”

how offensive threat modeling differs

- turns focus on the *defenders*
- attempts to understand **defenses**, or **defenders**
- provides analysis of the *weaknesses*
- seeks to develop an **offensive** strategy based on analysis
- primarily useful for stealth-mode attackers
- useful for penetration testing, assessments

yes … this is how an APT will attack you

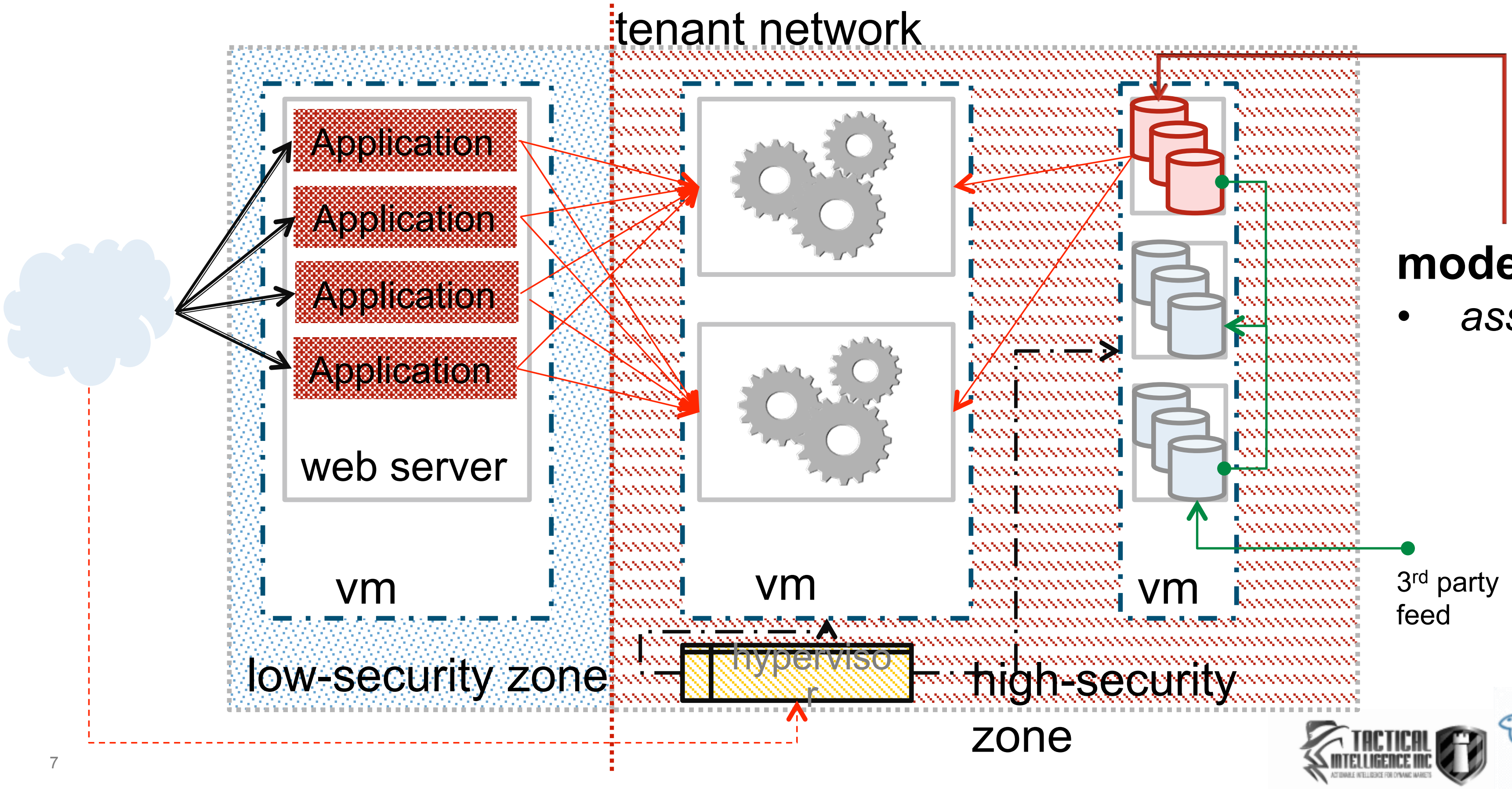
example – a cloud-based application



model:

- attacker
- system
- asset

example – a cloud-based application



model:

- *asset*

introducing ‘offensive’ threat modeling

Perspective

- approach as an attacker
- learn how defenders operate, where defenses are fortified

Objective

- exploit defenses or defender to attack target
- minimal risk of attack failure

“get into the defender’s head”

exploiting -

- human behavior
- defensive imperfection

✓ figure out defensive modus operandi

✓ exploit weaknesses in defenders

✓ exploit weaknesses in defenses

Threat Modeling as a Weapon

"To lack intelligence is to be in the ring blindfolded."

-Former Commandant of the Marine Corps, General David M. Shoup

turning modeling into a weapon

a battle is won by the side that has better intelligence

- gather intelligence (passive or active)
  - intelligence gathering is critical to a strategic infiltration
- modeling intelligence gathered
  - modeling concentrates intelligence into a usable format
- plan an attack strategy
  - "weaponized" intelligence comes from *intent*

Warner Bros.

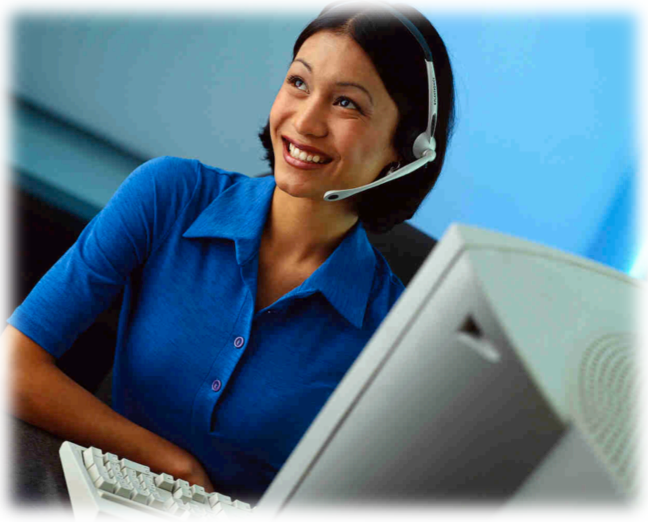
know the adversary

a successful attack requires as much advance knowledge about the target and adversaries as possible

- map the attack surface
  - map the target system or object
  - identify complete profile of exposures and externa
- profile the defenses
  - profile the human defenders
  - profile the automated fortifications

gaining an advantage

taking an upper-hand against the defense



- attack the defenders directly
  - attack those protecting the target
  - use a defender to unknowingly attack target
  - use a defender to knowingly attack target
- attack the target, using information about defenders
  - gleam weaknesses in defenses through defender profiling
  - use weaknesses in defenses, defenders against them

attacking the defenders

directly

directly attack the defender (the asset) using their weaknesses against them

- very bold attack
- requires advanced intelligence on asset
- requires advance preparation, time
- likelihood of success heavily depends on asset
- foresake the element of stealth
- burn the asset, attack tactic during attack
- generally a short-term (one-time) attack

attacking the defenders

indirectly

exploit a defender (the asset) without their knowledge to gain access to the target

- assumes asset has access to attack target
- requires preparation, time, intelligence
- attack hinges on being stealth
- “embedded” attack can be long-term
- possibility of burning asset, attack method varies depending on method

attacking the target

exploitation

learning the weaknesses of the defenders (and defenses) to plan the most strategic strike against the target

- exploit intelligence gathered about defenders
- exploit intelligence gathered about defenses
- perform reconnaissance against target
- perform false attacks to gather intelligence on response
- may require attacker to burn multiple attacks
- exploit complexity of attack surface
- exploit complexity of organizational response

Offensive Threat Modeling Tactics

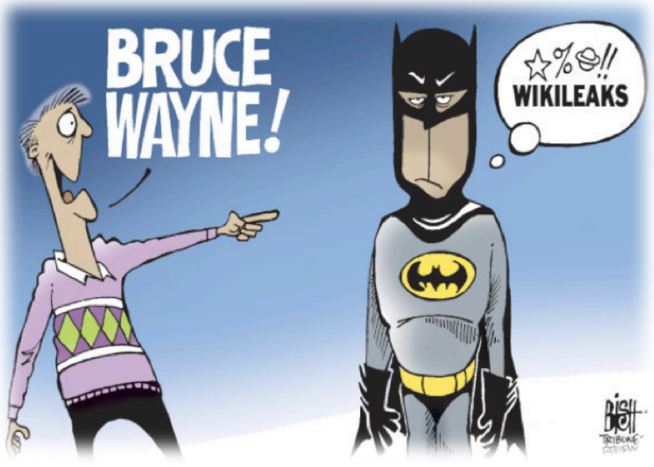
the 5 P's

silent P: "Purpose"

- identify the **objective**
- understand the full objective of the incursion
  - define whether objective is to infiltrate the organization, or a component thereof
- seek to infiltrate the enterprise from many diverse avenues
  - be pervasive, persistent
  - if one compromise is discovered other compromised assets will not be affected
- this step is critical if goal is to target a specific application or asset
  - assists in identifying when other "P's" begin to move away from the end goal

first P: “Pinpoint”

- create a HPTL (High Payoff Target List)
  - assets that give the biggest bang for the buck when compromised
  - example: security personnel, senior executives
- secondary targets
  - targets which can be used as an *indirect* attack vector
  - sales personnel, support staff, and vendors
- create a list of targets of opportunity
  - the “low hanging fruit” of the enterprise
- map out defensive capabilities
  - infrastructure like IDS, firewalls, physical plant defenses (CCTV, proxcards, guards)



second P: “points of attack”

- decompose target assets into **points of attack**
- break down each asset into base components
  - identify what parts can be readily compromised
- physical vs. human assets
  - family affiliations, hobbies
  - behavioral analysis, psych profiling
  - sentiment analysis
  - target fingerprinting, mapping
  - port scans, vulnerability inventories
  - system maps, application analysis

third P: “Posture”

- identify asset’s defensive posture
- assess the state or posture of each component
  - is it ready to be compromised?
- lots of critical time-based components
  - technical schedules – are firewalls rebooted, patches applied at fixed intervals?
  - change management windows & release schedules
  - when are employees least likely to be engaged (off-hours, traveling, conferences, etc)
- does the enterprise understand security?
  - is there a proactive security posture, or simply reactive?
  - is incident response implemented, tested?

fourth P: “Pwn”

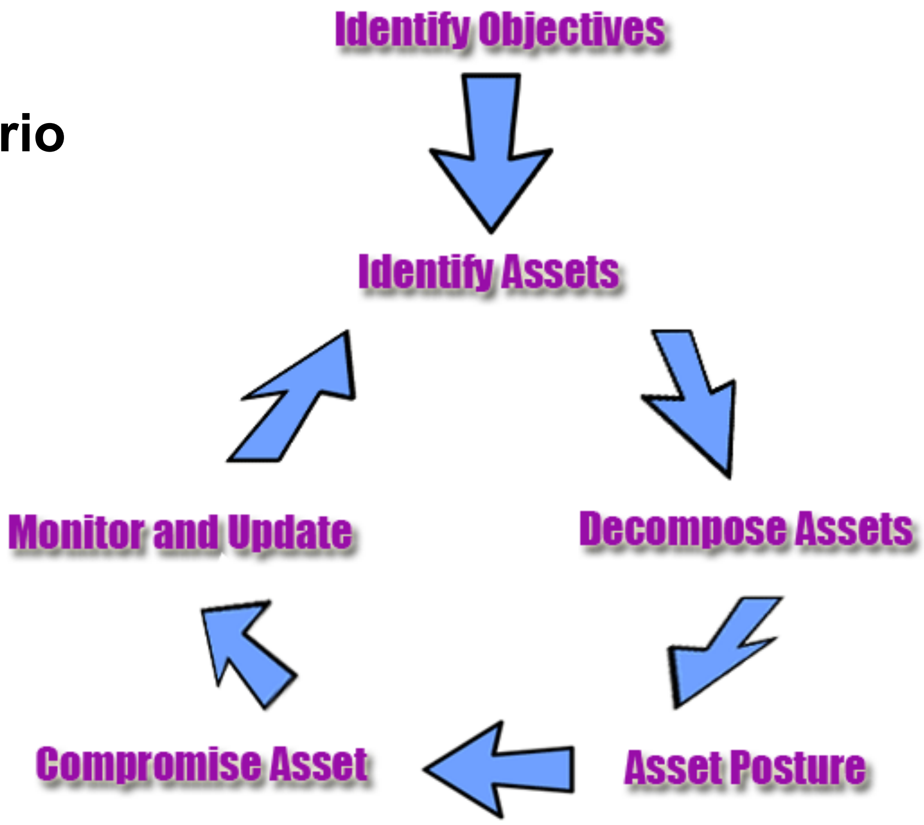
- **execute** the attack (Hax0r those assets)
  - compromise multiple assets using varied attacks
  - logical attacks – attack logic of processes or applications
  - social engineering – attack the *people* element
  - physical attacks – engage on-site (high risk)
  - leverage known weaknesses to compromise assets
  - focus on assets whose posture leaves them exposed
  - stealth is key when executing
- human weaknesses are often the easiest to exploit
  - bribery, blackmail, simple incentives

fifth P: “Poll”

- continuously monitor, maintain compromised assets
- attacker must continuously monitor, update asset list
  - identify if target response has been activated
  - analyze attack & defensive effectiveness
  - perform a cost-benefit analysis on underperforming assets
- perform damage assessment on lost assets
  - ensure no attack leakage has occurred
  - identify possible replacements.

Offensive Threat Scenario

- □ identify objectives
- □ identify assets
- □ decompose assets
- □ assess asset posture
- □ compromise assets
- □ monitor & update



The Offensive Threat Model

Applied Offensive Threat Modeling

modeling the defender (pinpoint)

- assessing the *people* component
  - assess footprint of the organization, structure and defensive talent
- assessing an organization’s footprint
  - scanning corporate websites, press releases, conference presentations
  - dialing through voicemail and phone directories
  - social engineering through human assets to extract information
- identify secondary attack vectors
  - suppliers/vendors, customers all useful avenues for attack
  - posing as a frazzled customer is often the path of least resistance
  - vendors routinely have trusted access to physical sites, applications, systems

modeling the defender (pinpoint)

- footprints from social media outlets
  - crawl *all* social media sites not just Twitter, Facebook and LinkedIn
  - less commonly searched sites such as flickr.com can yield tremendous amounts of actionable intelligence
    - ID cards, badges, employee names and numbers, badge and building layouts
    - referenceable events to use in a social engineering attack
- cultivate background information
  - phone numbers, addresses, emails
  - sites such as beenverified.com, spokeo.com, emailfinder.com, and many others
- identify company, departmental, social hierarchy within target env

modeling the defender (pinpoint)

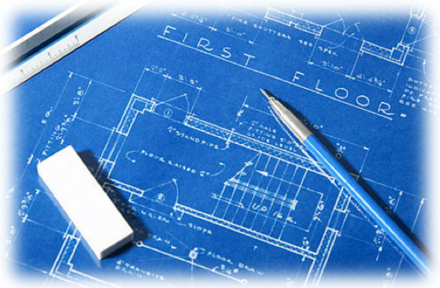
- identifying organizational hierarchy
  - identifying hierarchy within an organization without identifiers is still possible
  - techniques overcome lack of org charts, titles
  - Eric Gilbert at Georgia Institute of Technology identified certain phrases used in electronic messaging have a very high correlation to workplace hierarchy
- identifying hierarchical phrases
  - “thought you would” is strong indicator the recipient outranks the sender
  - “let’s discuss” implies authority, sender outranks recipient
- data set of 7,222 phrases has been released with associated weightings to assist the reader in building own solutions
  - http://comp.social.gatech.edu/hier.phrases.txt

modeling the defender (pinpoint)

prioritizing and categorizing assets

- High Payoff Target List (HPTL): assets that give the biggest ROI
- Tangential Target List (TTL): secondary targets, still have the potential for access
  - if compromised, gets the attacker some proprietary information or access, logical or physical
- Targets of Opportunity (ToL): generally the “low hanging fruit”
  - mainly used for throwaway operations (one-time phishing attacks) or onsite access attacks

modeling the defender (pinpoint)



- electronic (computer-based) asset assessment
  - perform **passive** reconnaissance
    - identify/fingerprint servers, systems, applications to find vulnerable assets
  - perform **active** reconnaissance
    - network mapping using tools like nmap and others
    - vulnerability mapping using nessus or other vulnerability identification tools
- physical asset assessment
  - physical surveillance is critical in identifying a company's security posture
  - lax physical security is usually indicative of poor overall security posture
  - identify surveillance such as CCTV, cameras fixed or PTZ
  - identify employee identification (badges) and access methods (swipe cards, etc)

modeling the “points of attack”

key objectives

- effectiveness predicated on model granularity
  - break every potential asset into as many elements as possible
  - assess each element for weaknesses that can be exploited
- identify and exploit human asset’s familiars
  - family members, friends, room mate, frequent coffee shop
  - shared home network, commonly visited public network
  - indirect targeting of asset via targeted spear phishing, piggy-back hacking
- target via social engineering to elicit information
  - personal information can be leveraged to grant physical access to target

modeling the “points of attack”

modeling and identifying *human behavior*

- personal activities
  - hobbies, routines, favorite hangouts, religious preferences
  - all can be very useful in identifying pretexts to be used in social engineering attacks
  - also used to track an individual physically.
- negative behaviors are key to establishing rapport or control
  - identifying behavioral issues such as substance abuse, gambling, extramarital affairs
  - opens up the possibility for blackmail or extortion
- requires more digging since users rarely sign up under real name

modeling the “points of attack”

psychology and privacy

- psychological profiling from social networking is a growing field
  - sites such as tweetpsych.com, automated user profiling have been established
- correlating psychological profiles and social media
  - recent research from The Online Privacy Foundation has shown some presence, although they argue the correlations are not as strong as previously believed
- psychological profile from social media, proclivity to certain activities and political beliefs are often easy to ascertain
  - if not directly from the target user, then from their common online associates

modeling the “points of attack”

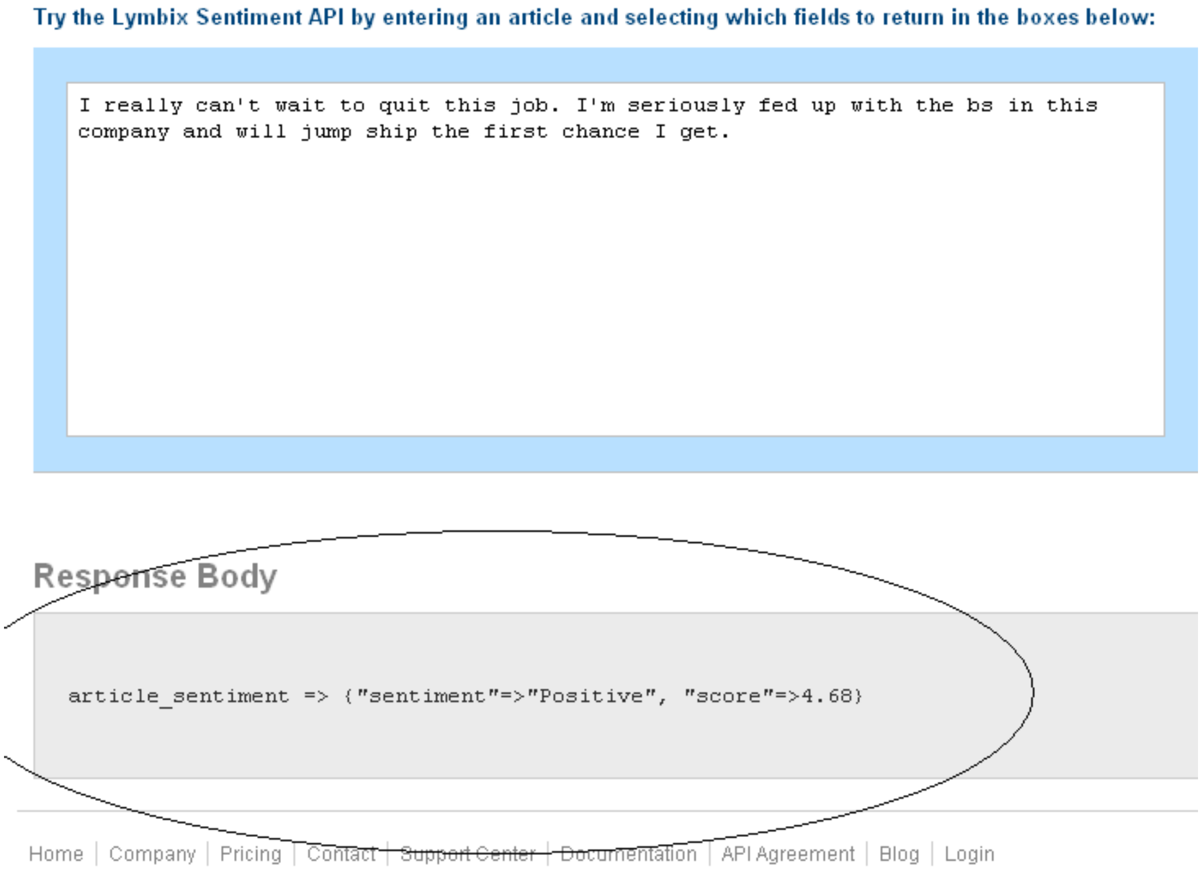
example

- user with a Guy Fawkes mask as their Twitter avatar
- follows command and control accounts from Anonymous
- can be profiled as a follower of Anonymous with strong likelihood
- is likely more susceptible to being successfully recruited into a “hactivist” operation against a bank than is a user who follows Andrew Breitbart and the Wall Street Journal

modeling the asset's “posture”

- use company sentiment
  - we want to identify as many users most at risk of compromising
- use negative employee morale to stage attack
  - Glassdoor.com, insidebuzz.com, and jobitorial.com
  - identify any negative widespread sentiment against the employer
  - users liberal with social media profiles considered “low hanging fruit”
- use social media to gather company lingo
  - facility and project nicknames valuable when launching social engineering
- tools enable automation of sentiment analysis[1][2]
  - manual analysis still preferable to automation

example



Try the Lymbix Sentiment API by entering an article and selecting which fields to return in the boxes below:

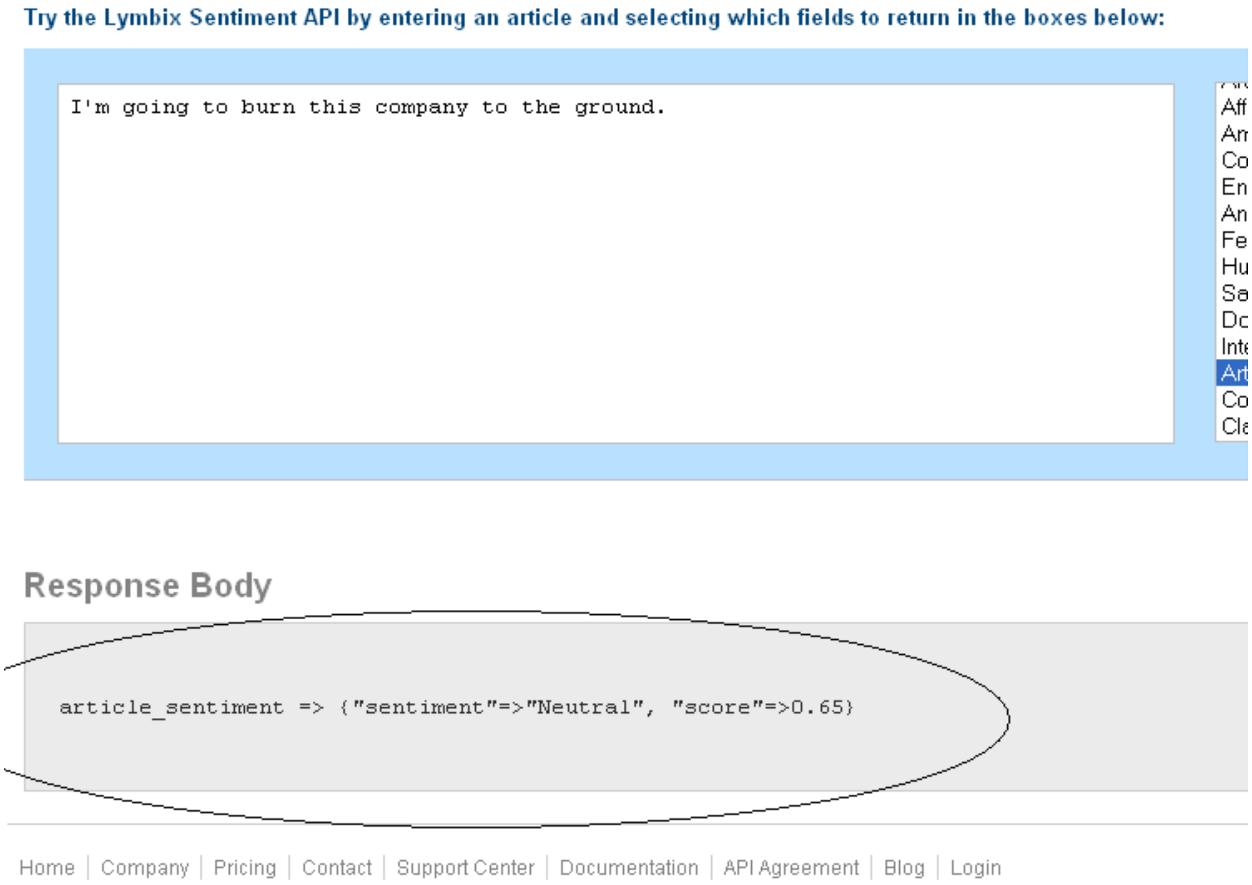
```
I really can't wait to quit this job. I'm seriously fed up with the bs in this
company and will jump ship the first chance I get.
```

Response Body

```
article_sentiment => {"sentiment"=>"Positive", "score"=>4.68}
```

Home | Company | Pricing | Contact | Support Center | Documentation | API Agreement | Blog | Login

example



Try the Lymbix Sentiment API by entering an article and selecting which fields to return in the boxes below:

I'm going to burn this company to the ground.

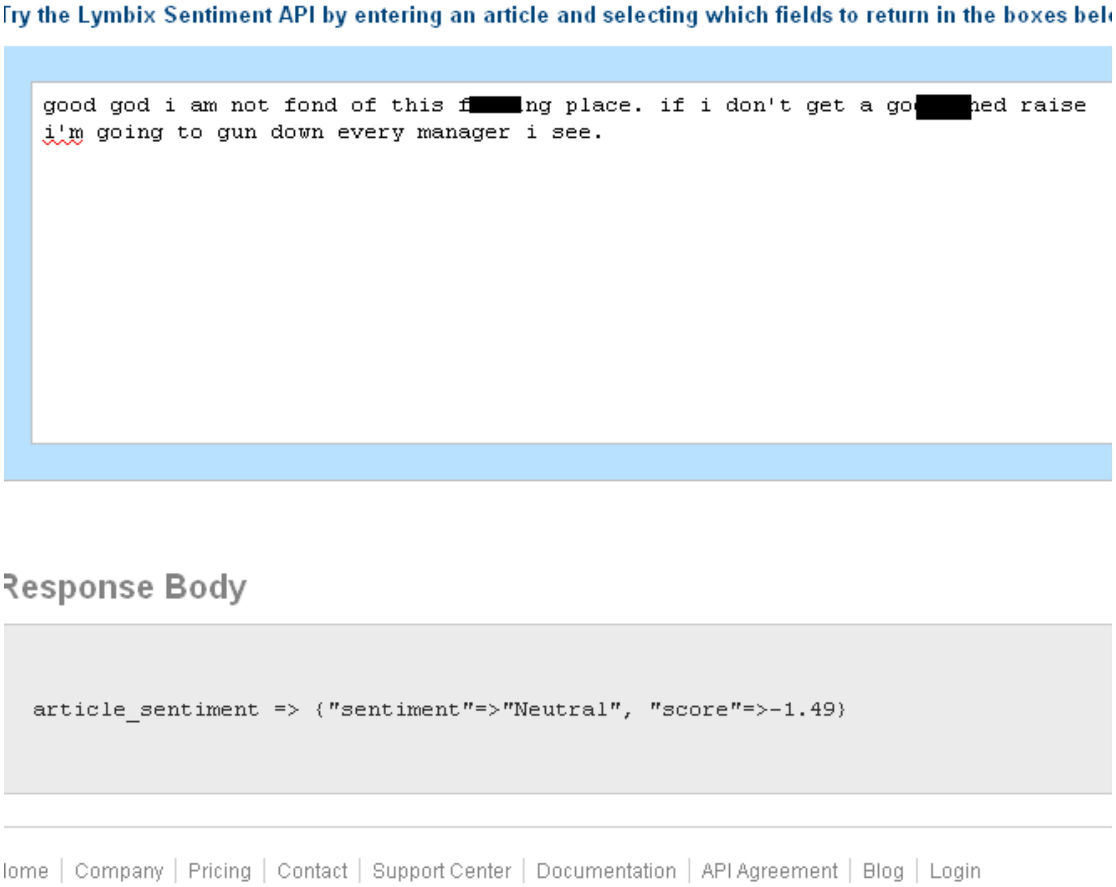
Aff
An
Co
En
An
Fe
Hu
Sa
Dc
Inte
Art
Co
Cla

Response Body

```
article_sentiment => {"sentiment"=>"Neutral", "score"=>0.65}
```

Home | Company | Pricing | Contact | Support Center | Documentation | API Agreement | Blog | Login

example



Try the Lymbix Sentiment API by entering an article and selecting which fields to return in the boxes bel

```
good god i am not fond of this f[redacted]ng place. if i don't get a go[redacted]hed raise
i'm going to gun down every manager i see.
```

Response Body

```
article_sentiment => {"sentiment"=>"Neutral", "score"=>-1.49}
```

Home | Company | Pricing | Contact | Support Center | Documentation | API Agreement | Blog | Login

modeling the asset's “posture”

- but wait!
  - if we have access to email, chances are we have already gained access to internal systems right?
  - single system access is often not enough
- need to penetrate systems further to gain strong foothold
  - need to further our attempts to escalate privilege
- goal of an “APT” attack is not simply to gain root access
  - create many different vectors of infiltration
  - sentiment analysis allows us to identify other targets within the enterprise
  - determine good targets for exploiting their disenchantment with the organization

modeling the asset's “posture”

example: the conference-going security analyst

- planning time-based physical attacks
  - physical plant/social engineering which rely on the target not being around
  - time-based attacks rely on knowing schedules
- physical attack on the target at the conference
  - physical attack can be gaining access to their physical machine
  - attackers can employ a honeytrap
- further advantage if the target is a speaker
  - research the speaker to identify avenues for connecting to the speaker

modeling the asset's “posture”

example: exploiting time windows

- maintenance windows provide opportunities for low-risk access
  - can be gleaned either from social engineering or monitoring behavior
  - identifying a window is the difference between success or failure
  - delivery of new systems
  - construction projects at corporate facilities
  - mass hiring or layoffs exploit human confusion

all identified easily from physical surveillance or social engineering

P is for “Pwn”

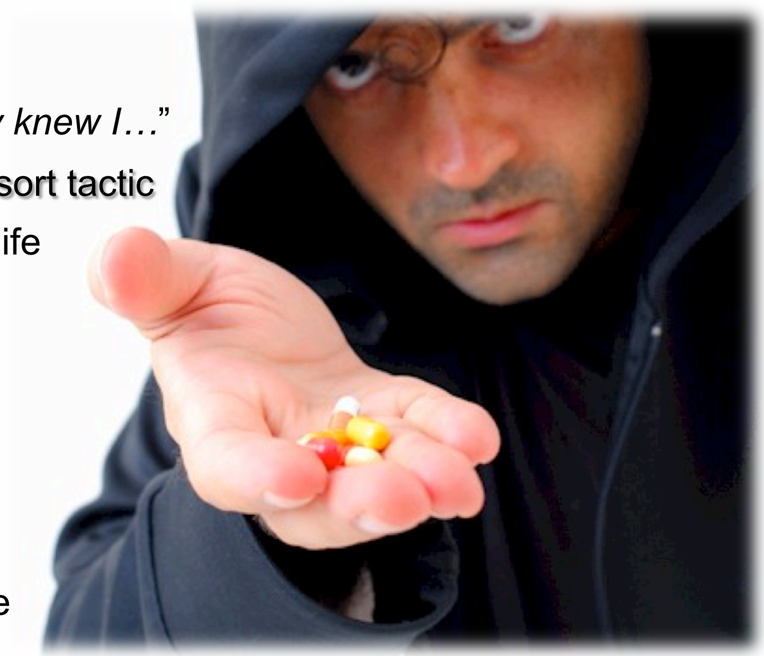
- directly engage the defenders, or relevant human assets
  - USB tokens offer a hard-to-resist attack vector
  - direct phishing against human assets
    - utilizing enticing offers, free ‘stuff’, or catering to their specific interests
  - physical information gathering (“dumpster diving”) at home or work
  - utilize social media to “track down” the asset
    - engage directly where humans are weakest – bars, clubs, when the guard is down
    - 4Square, FaceBook, Twitter, G+, etc will tell you where your assets are
    - exploit and incapacitate the asset(s) so they cannot respond to incident
    - exploit items on asset’s person (smart phone, laptop, access badge, etc)

P is for “Pwn”

- directly engage defenses
  - execute false-operations
    - execute multiple attacks to heighten sense of ‘danger’
    - force defenders to ‘tune down’ defensive posture
    - trick defenders into questioning their defensive posture
  - opportunistically attack systems or physical assets
    - change windows, upgrade periods, off-hours, or when defenses are weakest
    - when defenders are incapacitated, or otherwise not available to ‘defend’
  - exploit information overload, misdirection
    - noisy attack against front-end systems while back-end system is quietly exploited
    - create confusion, and mis-direction with overload of systems from high-noise (fake) attack
    - exploit human mental frustration, fatigue

P is for “Pwn”

- exploit dark side of human behavior
  - identify defenders with negative behavioral patterns
    - employee who fears their employer “*would fire me if they knew I…*”
    - this is a very dangerous avenue, and should be a last-resort tactic
    - easily destroy someone’s employment, relationships, or life
  - real attacks often require you to take extreme risk
    - human reaction to blackmail or discovery of negative behavior can be unpredictable
    - employ 3rd party assets (honey traps, hired ‘muscle’)
    - distance yourself from asset being engaged
    - you risk law-enforcement involvement, extreme response
  - attacks like this require long periods of planning, observation of the defenders



P is for “Pwn”

- exploit employee sentiment
  - disgruntled employees are easy to find
  - happy employees are often eager to help their employer (or you)
  - social media makes it simple to find corporate employees, learn their sentiment

- Lots of websites to troll and find unhappy employees
- unhappy employees are easily manipulated into ‘revenge’ against employer

P is for "Pwn"

- exploiting misdirection
  - create a situation of over-stimulation, confusion
  - attack quietly where no one is looking

ninja stealth over here

Guns blazing over here

- overwhelm defenses into panic
  - DDoS (distributed denial of service) forces adversary to tune down
  - most organizations cannot find 1 deadly needle in a stack of needles
  - human fatigue sets in quickly, defenders give up

“Poll” – monitor and update asset list

- monitoring compromised assets is critical
  - has the asset status (compromised) changed?
    - asset performing as desired
    - asset lost (recovered by defenders, or other condition)
  - if asset is lost, perform damage assessment
    - was attack information disclosed or leaked?
    - is the attack compromised? are we compromised?
  - cultivate under-performing assets
    - can we utilize an asset in a better way?
    - is a new asset open to acquisition?
  - defensive posture will change, you must adapt
    - assess, understand, overcome new defensive postures

Additional Resources

additional resources

- List of recommended OSINT aggregators and information gathering tools:
  - www.tacticalintelligence.org/blackhat_osint.html
- List of sentiment analysis keywords:
  - www.tacticalintelligence.org/black)hat_sentiment.html

- Updated version of these slides can be obtained at
  - http://tacticalintelligence.org/blackhat_slides.html
  - http://slideshare.net/RafalLos

additional resources

1. Lymbix’s Tonecheck plugin for Outlook/Gmail/Lotus Notes
   - performs basic and some extended analysis of email
   - results are less than stellar
   - crux of the software appearing to be highly dependent on extreme emotional words
     - examples: hate, despise, love, die
2. slightly better tool is Muse from Stanford
   - allows analysis of some chat, mbox email format, and mailing lists
   - accuracy also seems to be a bit better than the Lymbix products
   - http://mobisocial.stanford.edu/muse

THANK YOU!

@WH1T3RABBIT

@TACTICAL_INTEL