All of the threats

Intelligence, modelling, simulation and hunting through an ATT&CKers lens

Tim (Wadhwa-)Brown

Security Research Lead, CX EMEAR Technology & Transformation Group

August 2020

ATT&CK is a game changer and where it works, it can enable both blue and red to co-exist and work effectively together

- However, what happens when it falls short and the threat intelligence and hypotheses don’t exist?
- How do you build threat intelligence, threat models, threat simulations and threat hunt hypotheses from first principles?

Introduction

Introduction

- TLDR
- # whoami
- # cat .plan

TLDR

- Not a data scientist
  - Could play one in a movie
  - No particular brief to think blue or red
- This is not a solved problem

# whoami

- Tim (Wadhwa-)Brown
  - Background in telecoms and financial services sectors
  - 15+ years at Portcullis (and now Cisco)
  - Security Research Lead, CX EMEAR Technology & Transformation Group
    - Ex-NCSC CHECK Team Leader (9 years)
    - CREST Registered Threat Intelligence Analyst
    - CREST Practitioner Intrusion Analyst
    - ISO 27001 LA
- >150 CVEs to my name
  - Covering Windows, Linux, AIX and Solaris platforms
    - Userland through to kernel
  - Most recent research: Where 2 Worlds Collide: Bringing Mimikatz et al to UNIX, Black Hat Europe 2018

# cat .plan

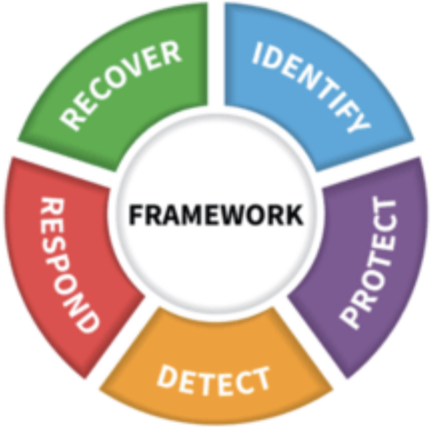
- Background
- Building bespoke threat models
- Expressing threat models as kill chains
- CVSS is not a shoe size contest
- Comparing our data with the real world
- Improving our threat models
- Recommendations
- Conclusions

Background

Background

- Bringing the 5 functions together
- An ideal approach
- Threat intelligence
- Threat modelling
- Threat simulation
- Threat hunting

Bringing the 5 functions together



An ideal approach

- Targetting
  - Actors
  - TTPs
  - Assets
- Hypothesis
  - Graphs
  - Dictionaries
- Hypothesis validation
  - Posture
  - Telemetry

Threat Intelligence

- Mission
  - Identify
    - Emerging TTPs
    - Malicious behavior
  - Collect, enrich and evaluate
    - IOCs
    - Not just IOCs
  - Provide situational awareness

Threat Modelling

- Mission
  - Describe assets in terms of
    - Tools, tactics and procedures (TTPs)
    - Attack surfaces
    - Vulnerabilities and weaknesses
    - Motivation
    - Impact

Threat Simulation

- Mission
  - Simulate possible threats
  - Evaluate defence efficacy
- Simulation vs emulation vs traditional testing/assessment
- Combines threat intelligence and threat modelling modelling translation of TTPs that are seen in the wild into reproducible test cases

Threat Hunting

- Mission
  - Hunt active threats
  - Improve defence efficacy
- Combines threat intelligence and threat modelling with validation of TTP usage using posture and telemetry

Building bespoke threat models

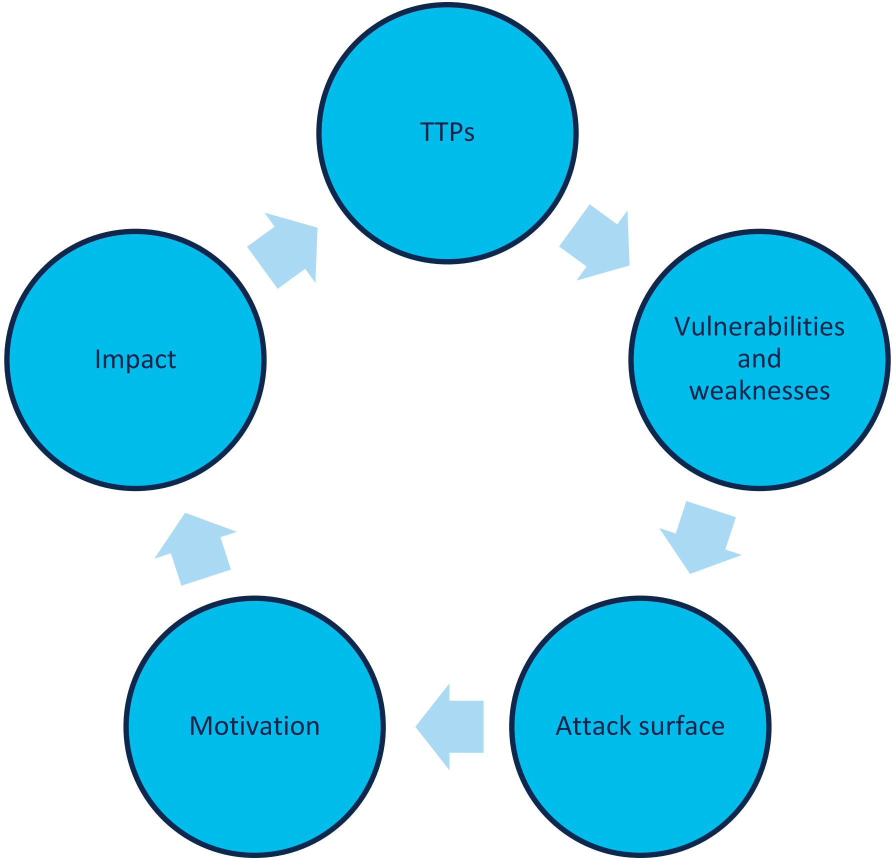
Building bespoke threat models

- Requirements
- Workflow
- Iterating effectively through the workflow
- Applying hypotheses to real world platforms and applications
- Enterprise use cases for threat models
- Capability gaps that exist in enterprises today
- Threat intelligence collection as a backstop

Requirements

- Targetting
  - Mission
    - The value of the system is the data
  - Threat visibility
- Hypotheses
  - Organisational alignment
  - Access to design
- Hypothesis validation
  - Target visibility
    - Threat intelligence
      - 3rd party sourced evidence that supports a given hypotheses
    - Threat simulation
      - Network and/or system access
    - Threat hunting
      - System configuration
      - Audit events and logs

Workflow



TTPs

Vulnerabilities and weaknesses

Attack surface

Motivation

Impact

Iterating effectively through the workflow

- Read up on the platform and applications
  - Filter TTPs
  - Filter vulnerabilities and weaknesses
- Prepare questions for key SMEs
  - People
  - Roles
  - Processes
- Draw a diagram
  - Pen and paper
  - Whiteboard
  - Microsoft’s Threat Modelling Tool
  - Visio
  - Excel
- Establish a worksheet to track hypotheses

Applying hypotheses to real world platforms and applications

- Tools, tactics and procedures
  - ATT&CK
- Attack surfaces
  - Physical
  - Local
  - Adjacent network
  - Network
- Vulnerabilities and weaknesses
  - CAPEC
  - CWE
- Motivation
  - Threat group
  - System value
- Impact
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of service
  - Elevation of privileges

Enterprise use cases for threat models

- Manual design validation
- Sourcing IOCs
- Telemetry configuration
- Response prioritisation

Capability gaps that exist in enterprises today

- Situational, platform and application awareness
  - Analysts
  - Telemetry
- Collection and routing
  - Logs
  - Audit events
  - Telemetry
- Orchestration of enrichment and action for non-standard platforms
  - What data is useful?
  - How do we use it?
- Behavioural threat specifications
  - What does bad look like on
    - An ERP?
    - A UNIX estate?
    - Microservices?

Threat intelligence collection as a backstop

- Constructing hypotheses
  - What critical functionality is being operated?
  - Have similar assets previously been breached and how?
  - What TTPs are available? Map these on to ATT&CK
  - What was the suspected motivation? Activist, criminal, state?
  - What was the impact?
- Validating each hypothesis using threat intelligence
  - For each hypothesis, track what we looked for and all identified cases, source data etc)
  - Are there examples of how these could be breached in the specific environment?
  - Is the environment exposed?
- Reporting
  - For each source, document the finding, validity and sensitivity
  - Provide details of these could be breached in the specific environment?
  - What would be the goal of an actor?

Expressing threat models as kill chains

Expressing threat models as kill chains

- Vulnerability/weakness reporting model
- Extending Cisco’s reporting engine
- Labelling findings
- Analysing our data

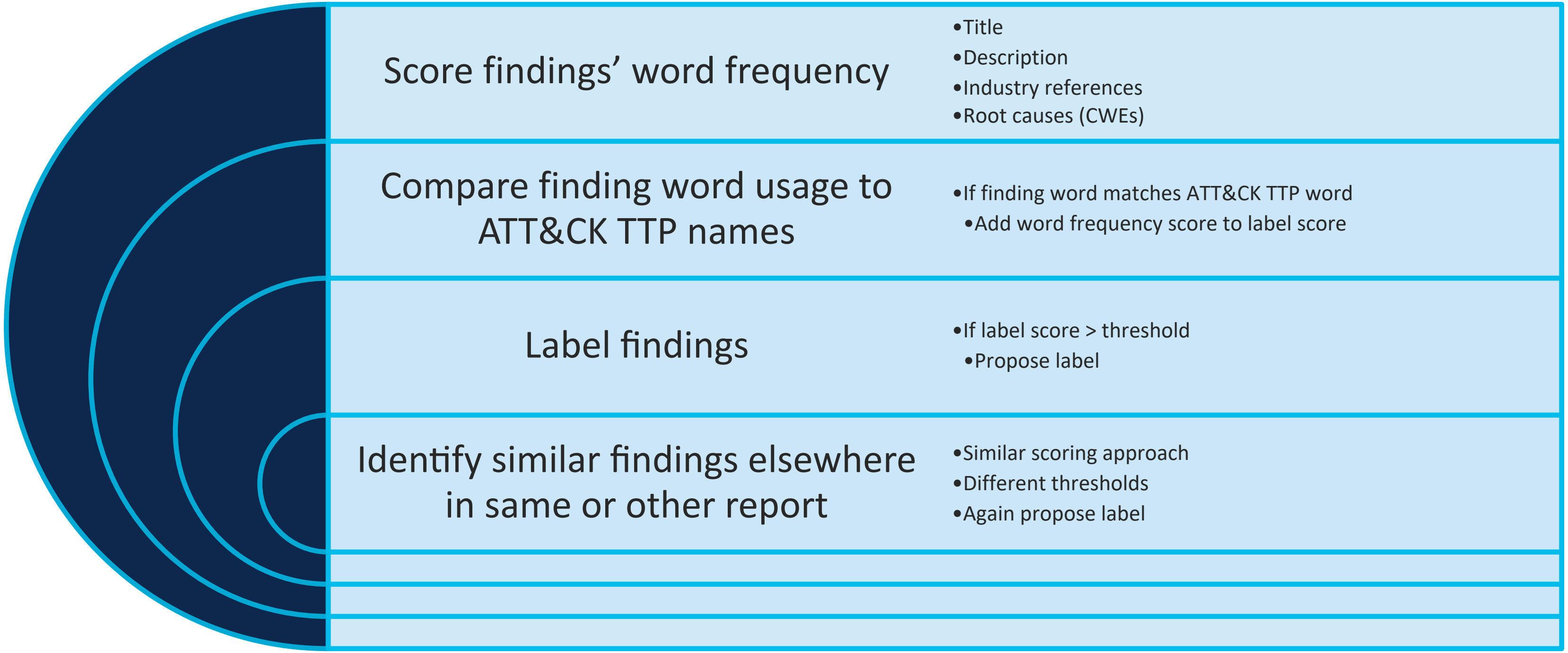
Vulnerability/ weakness reporting model

- Current findings schema
  - Title
  - CVSS/CWE
  - Description/Impact/Recommendation
  - …
  - Industry references/Tool references
- VDB imports
  - Internal VDB
  - Imports from Nessus
  - Imports from MITRE
  - Imports from other sources
  - …

Extending Cisco’s reporting engine

- Goals
  - Automated scenario generation
  - Report labelling using ATT&CK’s TTPs
  - Import of TI and export of reports as STIX
  - Cross-team data sharing
  - More effective business risk analysis

Labelling findings



Score findings’ word frequency

- Title
- Description
- Industry references
- Root causes (CWEs)

Compare finding word usage to ATT&CK TTP names

- If finding word matches ATT&CK TTP word
  - Add word frequency score to label score

Label findings

- If label score > threshold
  - Propose label

Identify similar findings elsewhere in same or other report

- Similar scoring approach
- Different thresholds
- Again propose label

Analysing our data

- Develop plugins to scrape existing report data for attack surfaces
  - By customer
  - By software platform
  - By attack surface (we structure findings in reports into groups by affected attack surface)
- Extend our findings with meta-data using standardised dictionaries including Talos threat data, STRIDE, LHM Cyber Kill Chain, ATT&CK, CAPEC
  - Develop plugins to automate importing dictionaries as new labels of type industry reference
  - Develop plugins to propose labels for findings
  - Develop plugins to render lists of vulnerabilities/weaknesses as
    - STRIDE
    - LHM Cyber Kill Chain
    - ATT&CK
    - …

CVSS is not a shoe size contest

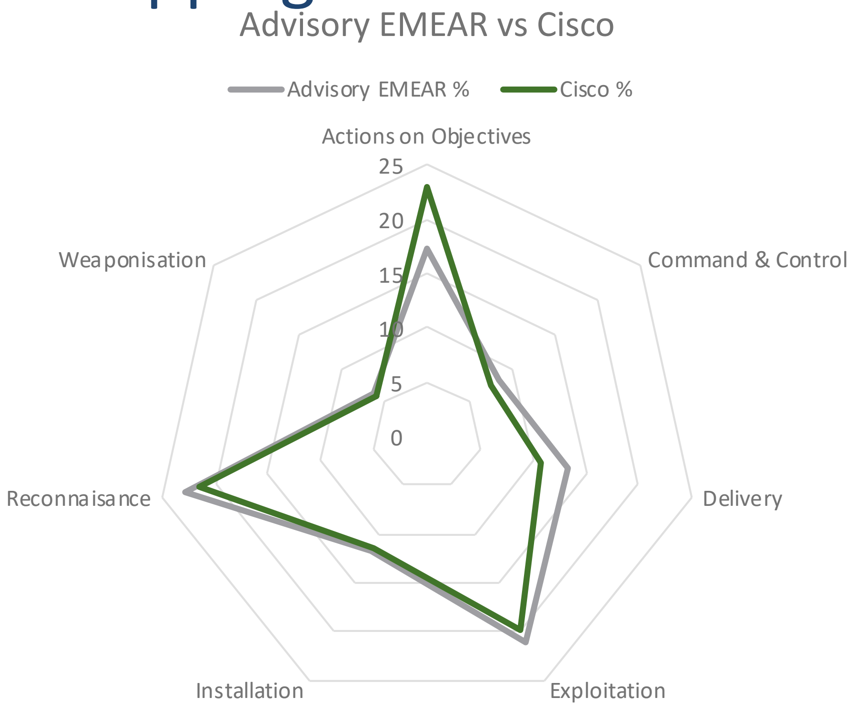
CVSS is not a shoe size contest

- Mapping MITRE’s CVSS to LHM Cyber Kill Chain stages
- What does this mapping look like?
- Using FAIR to capture business impact through CVSS

Mapping MITRE’s CVSS to LHM Cyber Kill Chain stages

LHMCKC Stage	Access vector	Access vector2	Attack complexity	Privileges required	User interaction	Sope	Confidentiality	Integrity	Availability
Reconnaisance	Network		Low	None	None	Changed	High	High	
Weaponisation	Network		Low						
Delivery	Network		Low		None				
Exploitation	Network		Low	None	None	Changed		High	
Installation		Local	Low	None	None	Changed		High	
Command & Control	Network	Local		None		Changed		High	
Actions on Objectives		Local		None	None	Changed	High	High	High

What does this mapping look like?



Using FAIR to capture business impact through CVSS

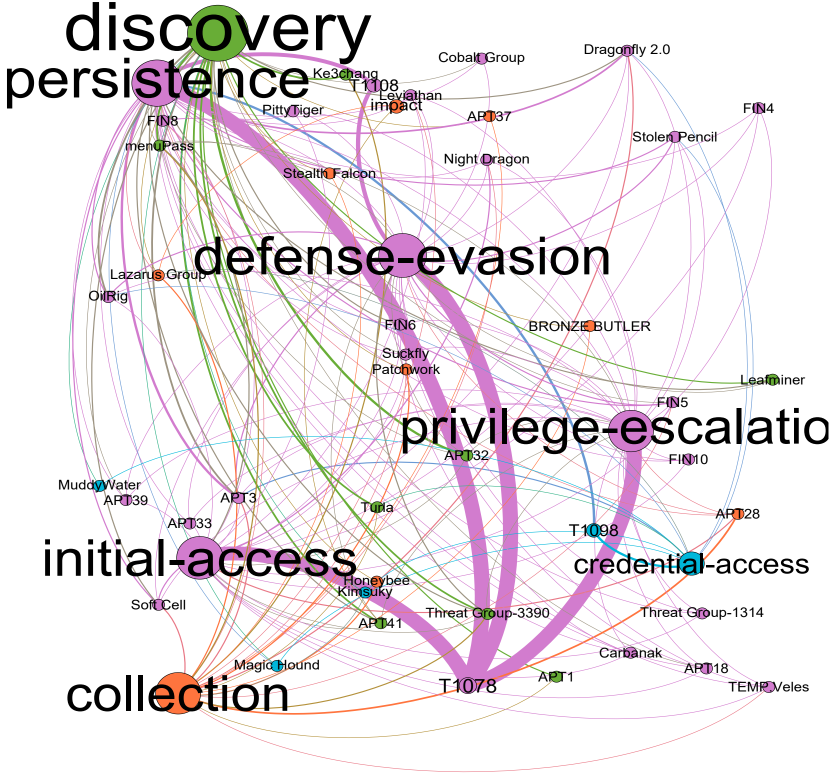
- Resistant strength
  - Access vector
- Threat capability
  - Attack complexity
- Probability of action
  - Privileges required
  - User interaction
- Primary loss
  - Confidentiality/Integrity/Availability
- Secondary loss
  - Scope

”Defenders think in lists, attackers think in graphs. As long as this is true, attackers win.”

@JohnLaTwC

Distinguished Engineer, Microsoft Threat Intelligence Center

We can also output to Gephi



Comparing our data with the real world

Comparing our data with the real world

- Targetting
- Hypotheses
- Hypothesis validation
- Applying threat intelligence learnings to real world platforms and applications
- Missed opportunities

Targetting

- As a team, we have decades of experience looking at UNIX from an offensive standpoint, from kernel through to userland
- We have unparalleled access to data about our customers, their use of these environments and the weaknesses and vulnerabilities that affect them

Hypotheses

1. Attackers are using our tools to target UNIX environments
2. Attackers are using techniques from ATT&CK to target UNIX environments
3. ATT&CK is not representative of the TTPs that we find success with

Hypothesis validation

- Small subset of our TTPs
  - Unix-privesc-check – https://github.com/pentestmonkey/unix-privesc-check
  - Linikatz – https://github.com/portcullislabs/linikatz
- Faced with a lack of DFIR reports, how do you validate your hypotheses
  - Checking for previous detonations
  - Examining ATT&CK for signs of life
  - Google’ing furiously
  - Reviewing other data sources

H1: Attackers are using our* tools to target UNIX environments

- Checking for previous detonations
  - unix-privesc-check 1.4 tar ball
    - https://www.virustotal.com/gui/file/b278797b8698160ca2d26425930ad13c/detection
    - First seen: 2015-01-21 03:58:37
    - Most recently seen: 2019-11-09 15:19:49
    - Undetected! ✖
  - unix-privesc-check 1.4 shell script
    - https://www.virustotal.com/gui/file/387abc4650734e4cc2c991ac4c8a981e/detection
    - Contents first seen: 2015-07-16 12:00:10
    - Contents most recently seen: 2015-07-16 12:00:10
    - Undetected! ✖
  - unix-privesc-check 1.3
    - https://www.virustotal.com/gui/search/bb6a77640f236386fc4a63b64d65e944
    - https://www.virustotal.com/gui/search/f32d99a8c43806f64a93c9294ccb8539
    - No match on tar ball or contents ✖
- * unix-privesc-check v1 by pentestmonkey, v2 by myself, pentestmonkey with community contributions

H1: Attackers are using our* tools to target UNIX environments

- Checking for previous detonations
  - linikatz shell script
    - https://www.virustotal.com/gui/search/c68c36fb5df840d9c475767444c894c1
    - No match on released shell script from GitHub ✖

H1: Attackers are using our* tools to target UNIX environments

- Examining ATT&CK for signs of life
  - Neither linikatz nor unix-privesc-check are mentioned ✖
- Google'ing furiously
  - Lots of tutorials for penetration testers, but how about malicious use?
    - https://www.exploit-db.com/papers/41913
    - Name checked by Phineas Phisher ✖

H2: Attackers are using techniques from ATT&CK to target UNIX environments

- This is actually quite hard!
  - Most UNIX related DFIR reports relate to
    - IOT
    - Frontend systems
  - Why? Is it a
    - Chicken and egg problem?
    - Reluctance for organisations to acknowledge just how deep breaches went?
- Anecdotally…
  - UNIX backend breaches do occur
  - In almost all cases there is some level of application level interaction
  - Some actors are truly incompetent if it’s not a Linux host
  - For the most part, TTPs overlap with what ATT&CK reports

H2: Attackers are using techniques from ATT&CK to target UNIX environments

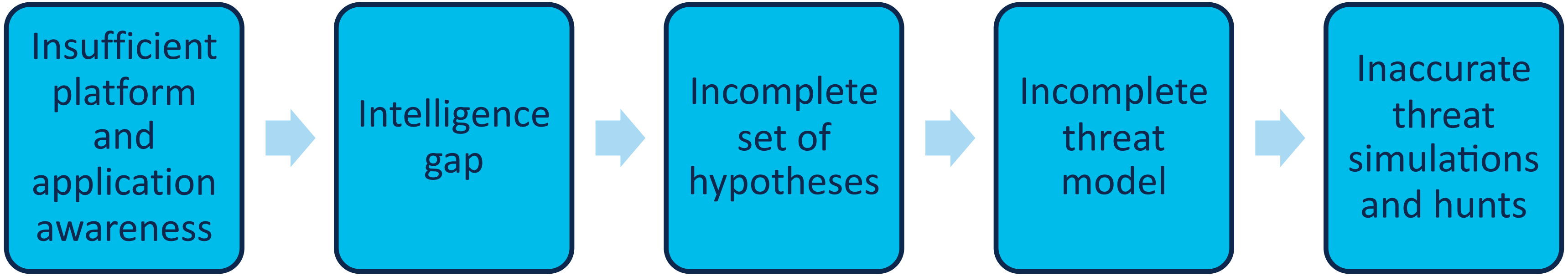
- Probably the best public UNIX breach report I've read
  - https://github.com/fboldewin/FastCashMalwareDissected/
    - Persistence & Privilege Escalation & Credential Access ✖: Hooking ✔: Windows ✖
    - Defence Evasion & Privilege Escalation: ✔ : Process Injection ✔ : Linux ?
    - Defence Evasion & Persistence ✔ : Hidden Files And Directories ✔ : Linux ?
    - Defence Evasion ✔ : Obfuscated Files Or Information ✔ : Linux ?
    - Impact: ✔ : Runtime Data Manipulation ✔ : Linux ?
    - Speculation on application and entry point
    - ATT&CK doesn't mention FastCash or the associated actor Lazarus Group/HIDDEN COBRA ✖

H3: ATT&CK is not representative of the TTPs that we find success with*

- Missing Security Patches ✔
- Role Accounts Used For Interactive Logins ✖
- Firewall Enabled But Rules Not Fully Configured ✔
- `SetUID'/`SetGID' Binaries Allow Privilege Escalation Via Insecure `RPATH’ ✖
- Passwords Reused Across Multiple Systems ✔
- Weak Password Policy In Use ✔
- Files And Directories Are World Writable ✔
- Commands Allowed Via `Sudo' Rules Can Be Subverted To Escalate Privileges ✔
- Files And Directories Have Weak Permissions And Allow Privilege Escalation ✔
- SNMP Server Weak Community String Configured ✔

* This only gets worse when you look at lower SCORED AND/OR less used TTPs

Missed opportunities



Insufficient platform and application awareness

Intelligence gap

Incomplete set of hypotheses

Incomplete threat model

Inaccurate threat simulations and hunts

Improving our threat models

Improving our threat models

- Threat modelling can improve the blue team at scale
- Increased visibility improves threat models accuracy
- Refocusing offensive services

”There aren’t enough bums on the blue team seats.”

Me

Threat modelling can improve the blue team at scale

- We can’t directly fix architecture, alignment or mission
- We can however…
  - Improve threat visibility
  - Improve target visibility

Increased visibility improves threat models accuracy

- Knowledge of current threats that affect more systems will enable us to better
  - Protect customers
  - Protect ourselves, our data and brand reputation
  - Keep us safe
- Accurate threat models will enable better designs and more secure implementations
  - SDLC can be more consistently applied
  - Hopefully less vulnerabilities will make it to production
- Bottom line, most organisations are profit motivated entities
  - Sales conversations where we can speak to the customer’s threat model will help

Refocusing offensive services

- We need to track threat briefings and vulnerability research more effectively
  - There is life beyond Nessus and MITRE
  - Onboard them into our platform for analysis
- We need to use ATT&CK more effectively
  - Generate bespoke briefings from TTPs
  - Craft war games from actual kill chains
- We need to ensure we can articulate the threat model and kill chains when we engage with the wider world
  - Better meta-data
  - Visual representation
- We need to refine our assessment methodologies
  - Help others think more like a threat (hunter)

Conclusions

Conclusions

- What have we learnt?
- How do we do this better?
- Next steps?

What have we learnt?

- Automated extraction of hypotheses is possible
- Bespoke threat modelling can build on automated extraction
- Vulnerability findings can be labelled with meta-data using standardised dictionaries
- Visual representation of actual threat models and kill chains from penetration tests helps give situation awareness
- Automated control sets can be generated and validated
- Better analysis and communication of threats with our peers through richer exchange of meta-data will improve the situation further

How do we do this better?

- Greater consideration by the offensive security community for threat models, TTPs and behaviours and associated telemetry
- Del.icio.us-alike with APIs for cross-community vulnerability sharing
- A fully labelled VDB to run queries on
- Machine actionable presentation of customer, platforms, applications, vulnerabilities, TTPs, actor TI to include full stack documentation of behaviours and associated telemetry sources
- Improvements to EDR and workload protection products to incorporate threat models, TTPs and behaviours derived from offensive research

Next steps?

- Just because we're not looking for the bad guys, doesn't mean they're not there
- Attackers will use the easiest TTP that gets them to a root prompt
- If you're playing defence, for goodness sake, use start looking at behaviour
- If you're running threat simulations or hunts, here are some UNIX TTPs you should consider
  - Hooking
  - Process Injection
  - Hidden Files And Directories
  - Obfuscated Files Or Information
  - Runtime Data Manipulation
  - SetUIDs And GIDs With Insecure RPATHs
  - Access To Role Accounts
- You might also want to consider how you simulate and hunt
  - linikatz
  - Unix-privesc-check

Thanks

- Portcullis & Neohapsis Labs old-hands
- Cisco’s wider security community
- MITRE
  - ATT&CK community
- Swimlane
- Blue teams everywhere

Questions?

twadhwab@cisco.com

cisco

Bonus material

Intelligence sources for threat modelling

- Internet infrastructure databases
  - IP/routing/DNS history
- Internet telemetry
  - GreyNoise/Sh0dan
- Detonation sandboxes
  - Virus Total/Any URL
- MITRE
  - https://attack.mitre.org/
  - https://capec.mitre.org/
  - https://cwe.mitre.org/
  - https://cve.mitre.org/

Breach report sources for threat modelling

- Verizon Data Breach Investigation Report
  - https://enterprise.verizon.com/en-gb/resources/reports/dbir/)
- Privacy Rights Chronology of Data Breaches
  - https://www.privacyrights.org/data-breaches
- Center For Strategic International Studies Significant Cyber Incidents
  - https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Intelligence techniques for threat modelling

- CREST
  - https://crest-approved.org/wp-content/uploads/CREST_Technical_Syllabus-Threat-Intelligence-Manager-CCTIM-v2.0.pdf
- SANS
  - https://www.sans.org/reading-room/whitepapers/threatintelligence/threat-intelligence-planning-direction-36857
- Diamond model
  - https://www.recordedfuture.com/diamond-model-intrusion-analysis/
- US DOD
  - https://fas.org/irp/doddir/army/fm34-2/Appa.htm
- Wikipedia
  - https://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines
  - https://en.wikipedia.org/wiki/Parallel_construction

Mapping your VDB into actionable data

- Swimlane’s Pyattack
  - https://github.com/swimlane/pyattck
- OASIS’s STIX
  - https://stixproject.github.io/

Vulnerability Disclosure Bingo - @timb_machine				
Written off by Twitterati as unsufficiently technical	Was never reported to the vendor	Fixed by vendor on the day reported	Wildly misunderstood and overhyped onc e the common press get ahold of it	Finder is arrested
Was incorrectly fixed	Results in finder being called irresponsible by someone suitably (un)qualified	Earns the finder a pwnie award	Results in a worm that destroys half the Internet	Turns out "researcher" has overstepped the boundary and downloaded entire customer database
Results in calls to outlaw showers	Affects a library used in multiple closed source products that noone knew about	Did not end the world as we know it	Results in someone explaining vulnerability disclosure and bug bounties to Katie M	Requires user interaction and everybody knows that means it's not a real vulnerability
Finder has comissioned a marketing company to segment his offering and enable brand awareness (it has a logo!)	Vendor never responds	Remains unpatched to this day	Results in renewed calls from "community leadership" to stop releasing offensive tools	The plane being used by the researcher to demo it crashes. Everybody dies