HIMSS18 The leading health information and technology conference

WHERE **THE WORLD** CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

Attacking Your Own Network

Session 107, March 7, 2018

Chuck Kesler, Chief Information Security Officer, Duke Medicine

John R. Nye, VP, Cybersecurity Strategy, CynergisTek

ENGAGED

www.himssconference.org

#HIMSS18

Conflict of Interest

John Nye, BS

Has no real or apparent conflicts of interest to report.

Chuck Kesler, MBA

Has no real or apparent conflicts of interest to report.

Agenda

- Why We Need to Attack Ourselves
- What is Ethical Hacking?
- Starting and Evolving an Offensive Security Program
- Conclusions

Learning Objectives

- Explain terms and techniques used by ethical hackers during offensive assessments
- Discuss common issues that arise during these types of assessments and how to avoid them
- Identify benefits of offensive security assessments and risks of not conducting them
- Develop non-technical attendee's perception of offensive assessments

Why We Need to Attack Ourselves

Being proactive is the only way

Healthcare is a Target

Year	Number of Breaches (500+)	Number of Records Exposed
2016	329	16,471,765
2015	270	113,267,174
2014	307	12,737,973
2013	274	6,950,118
2012	209	2,808,042
2011	196	13,150,298
2010	198	5,534,276
2009	18	134,773
Total	**1801**	**171,054,419**

Source: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/

Why is This Happening?

- Digital data theft (the “product” of a breach) is a booming business
- Healthcare records are worth substantially more than others
- Healthcare orgs have traditionally been less secure
  - Complicated IT environments
  - Vendors not building secure products and are slow to patch
  - Insufficient budget for building substantial infosec programs
  - Small providers are particularly at risk

Solution: Being Proactive

- If you're only reacting to attacks it's already too late
- Proactively finding and remediating vulnerabilities is the ONLY option
- Conducting offensive assessments can help you proactively find issues
- But it's not enough to just find the issues, you also have to address them
- You must also educate IT staff and users on the tactics used by hackers
- Failure to do these things increases the risk of a breach

What is Ethical Hacking?

Hint: it's not "hackers in the mainframe"

What Hacking Isn't

- The movie "Hackers" or "Firewall"
- Basement dwelling, non-social creatures
- Cannot "just hack" whatever you want hacked
- A skill that is almost magical
- Requires a nerdy obsession with video games, sci-fi, or role playing games

What Hacking Is

- Some shows and movies that reflect a more realistic depiction of hacking include “Mr. Robot” and “Sneakers”
- An engineering mindset – wanting to know how things work and how they might break
- The best of the best are very social and great communicators
- Many are very good at manipulating people, like digital “con artists”
- Skillsets are becoming increasingly specialized (i.e. goes deep in a few areas vs. wide in many)
- For the most part it’s not something to fear

All Hackers Aren't Bad

- A hacker can be thought of as an individual who has specialized skills in testing networks, systems, and applications
- But different hackers have different motivations:
  - Black Hats: criminally motivated
  - White Hats: professionally motivated
  - Gray Hats: usually not criminally motivated, but often acts without permission (and sometimes recklessly) based on their perception of what is right

Hacker and Pen Test Terminology

- Ethical Hacker: synonymous with white hat (and some gray hats)
- Security Researcher: usually a white or gray hat hacker who independently tests networks, systems, and applications looking for zero-day vulnerabilities
- Penetration Test: a contracted, professional assessment to simulate an attack against networks, systems, or applications
- Penetration Tester: an ethical hacker who works as consultant who is contracted to conduct penetration tests
- Red Team: A group of penetration testers with various specialties that use all attack vectors available to compromise a target
- Blue Team: A group of IT and infosec professionals who have been assembled to defend against the actions of the red team during some penetration tests

More Terms

- Zero-day: A new vulnerability that has been identified by a hacker but has not been publicly announced
- Bug Bounty: A new approach to offensive assessments where companies offer financial rewards to independent researchers who report vulnerabilities
- Vulnerability Assessment: NOT the same as a pen test, but some will sell it that way; objective is to enumerate vulnerabilities instead of breaching the environment
- Malware: Any type of code or software that has malicious intent (includes ransomware)
- Social Engineering: Using non-technical methods to gain access to IT systems or networks by exploiting weaknesses in human behavior
- Phishing: Using email as the attack vector, can deliver malware or be used in social engineering

A Day in the Life of an Ethical Hacker

- Running automated scans (e.g. Qualys, Nessus, etc)
- Maintaining various Linux-based systems
- Keeping up to date on the latest vulnerabilities and attacks
- Reviewing results of automated scans, then manually eliminating false positives
- Demonstrating how one or more vulnerabilities can be used to create a breach
- Sometimes working overnight hours to avoid disrupting production systems
- Thinking creatively and drinking A LOT of coffee!
- Taking MANY screenshots to document what happened
- Writing up findings and drinking MORE coffee!
- Discussing findings and recommendations with the client

Starting and Evolving an Offensive Security Program

Approach #1: Outsourced Pen Test

- The most common approach for those just getting started with an offensive security program
- Pros:
  - No need to recruit and hire highly specialized staff
  - Third-party, unbiased view of your environment
  - Quick turnaround to get results
- Cons:
  - Point in time view, so evolving threats may be missed
  - You get what you pay for – not all pen test firms are equal

Options for Outsourced Pen Tests

- Time boxing
  - Specifying how long testing will occur
- Blind vs. informed
  - Will you inform your staff that a pen test will be performed?
- Scoping
  - External vs. internal
  - Network, applications, physical, social engineering, etc.
- Red team/blue team
  - ”War Games” approach

Approach #2: In-House Pen Testing

- Typically only done by organizations with mature security programs and significant budgets
- Pros:
  - Ongoing assessment of threats and vulnerabilities
  - Becomes engrained in the organization's culture and processes
  - Easier to test new systems before they go into production
- Cons:
  - Can be a challenge to hire and/or nurture skilled ethical hackers
  - It's still possible to miss things, particularly in large environments

In-House Considerations

- There are certainly aspects that can be handled in-house
  - Especially if the talent exists or skills/interests are there to nurture
  - Some things like automated scans can be handled internally
- But don't try and do it all
  - Outside experts may be needed in specialized areas (e.g. social engineering, wireless, physical security assessments)
- Internally discovered issues sometimes become stagnant
  - They may lack the executive visibility of a report from a third party

In-House Specialty

- Creating a culture that is truly aware can ONLY be done in-house
- Third parties can help set it up, can help develop it, but only internal buy-in and devotion can make it actually work
- Training is another aspect that is better done in-house
  - No one knows your culture like you
  - No one can develop training with more impact
  - Training has to be targeted as much as possible

Approach #3: Bug Bounties

- A new approach where an organization announces that they will reward independent researchers who responsibly identify and report issues
- Pros:
  - White hat and gray hat hackers constantly looking for vulnerabilities
  - Some firms will now coordinate bug bounty programs for you
- Cons:
  - You must be prepared to promptly address any reported issue
  - Researchers with limited skills will report low quality findings
  - Difficult to budget for – how many bounties will you have to pay?

An Evolved Approach

- Mature programs may use a combination of all three
  - Annual, bi-annual, or quarterly third-party pen test
  - Internal team conducting ongoing assessments
  - Bug bounty program to catch things others may miss

The Secrets to Success

- Clearly identify the scope and objectives for any assessment
- Ensure that an appropriate amount of time (labor) is allocated
- Define the rules of engagement and communications channels
  - Consider who should be informed in advance and who should not
- Promptly identify and collect any pre-requisite information
  - IP address ranges, URLs, test login credentials, etc.
- Assess and plan for potential impact to production systems
  - In healthcare, this is particularly a concern for biomedical devices

Conclusions

What to take home with you

Conclusions

- Hacking is not always a bad thing
- Being proactive and doing offensive assessments is good
- The cost of a breach far exceeds facing problems head on
- Healthcare is no longer a target of “convenience”
- Breaches are growing in severity, frequency, and cost
- Educating users on these techniques is crucial

Questions

John R. Nye
VP, Cybersecurity Strategy
john.nye@cynergistek.com
512.405.8550 x7027
@EndisNye_com

CYNERGISTEK

Chuck Kesler
Chief Information Security Officer
Duke Health
chuck.kesler@duke.edu
@chuck_kesler

DukeHealth Information Security