NORTH TEXAS ISSA

#NTXISSA

HELP! My Vulnerability Management Program is Failing!

Kevin Dunn

Technical VP

NCC Group

02 October 2015

Session Overview

- Welcome & Introductions
- Scenario – Your Day is Ruined
- Vulnerability Management Programs
- Penetration Testing Mechanics
- VM Program Gaps & Failings
- VM Program Easy Wins
- Design Improvements to Enterprise Sec.

Welcome & Introductions

NCC Group – A Global Security Firm

- Formed in June 1999 with immense growth over 16 years.
- 1200 employees, in 24 office locations
- North America, the United Kingdom, Europe and Australia.
- We strive to provide Total Information Assurance

NCC Group in North America

- Currently 7 offices in the US: New York, Atlanta, Chicago, Austin, Seattle, San Francisco and Sunnyvale.
- NCC Group combines the best of bread US security brands of iSEC Partners, Matasano, Intrepidus Group and NGS.

Welcome & Introductions

NCC Group – Security Consulting

- Attack & Penetration Focus
- Applications
- Mobile
- Networks & Infrastructure
- Physical Security
- Embedded Systems
- Red Teaming
- Incident Response & Forensics

Welcome & Introductions

Your Speaker – Kevin Dunn

- Technical VP for NCC Group, based in Austin TX.
- 15 year career: Attack & Penetration / Security Remediation
- Development of NCC technical practices:
  - Strategic Infrastructure Security (SIS)
  - NA Computer Incident Response Team (NA-CIRT)

- Specialist in Red Team / Black Ops engagements
  - Forms of extreme penetration testing and attack modeling

Scenario – Your Day is Ruined

- You're in charge of VM for your company
- You have scanning sensors deployed
- You have hardening plans in place
- You have remediation strategies and goals

- A pentest is commissioned from an outside firm
- They prove traversal from the outside to the inside
- They become Domain Admin on your network
- They access your most critical data and systems.

Vulnerability Management Programs

- Inventory Discovery & Management
- Vulnerability Discovery
- Vulnerability Risk Classification
- Vulnerability Remediation
- Specific Threat Response
- Continual Lifecycle Process

Vulnerability Management Programs

- **Inventory Discovery & Management**
  - You can't secure what you don't know about
  - Manual, semi-automated and automated discovery
  - Find servers, the services they provide, and their general purpose within the org.

Vulnerability Management Programs

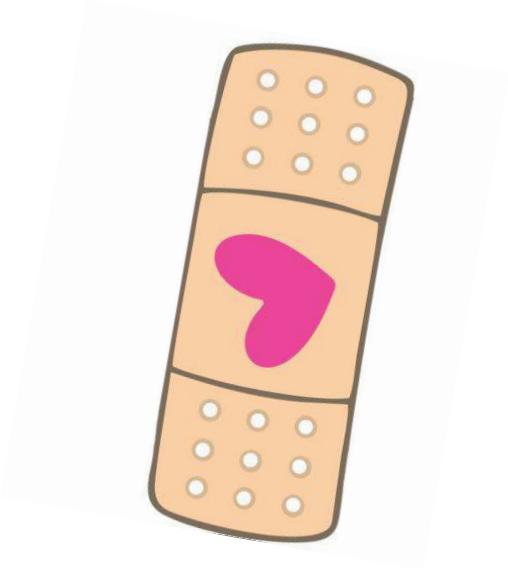
- **Vulnerability Discovery**
  - Operating systems and platform software suffer from flaws and security problems.
  - Some are fixed with patches, some are fixed with configuration.
  - Finding these problems is key.

Vulnerability Management Programs

- **Vulnerability Risk Classification**
  - How you classify your vulns.
  - Likely relates to how you prioritize fixes
  - Classifying security impact is easy
  - Classifying business risk is harder
  - Do you include business risk?
  - Do you ignore business risk?

Vulnerability Management Programs

- **Vulnerability Remediation**
  - So you've got vulns? Now what?!
  - You have to fix them
  - Generally a large work effort
  - How do you prioritize?
  - Are you on an annual cycle?
  - If so, you need a smaller cycle



Vulnerability Management Programs

- **Specific Threat Response**
  - Argh! One of those pesky ‘named bugs’ shows up
  - Your management wants to know:
    - Are we vulnerable?
    - How many servers?
    - What are we doing to fix it?
  - VM programs should support this

Vulnerability Management Programs

- **Continual Lifecycle Process**
  - It never stops, and it never should
  - A program like this is needed to gain a reasonable baseline of security in your org.
  - Do you have one?
  - You need one!
  - But there is so much more…

Penetration Testing Mechanics

- At NCC we carry out a lot of Pentests
- Some have external focus, some internal
- Most of them have both
- We have a very high success rate
- Even against firms that have a Vulnerability Management Program

Penetration Testing Mechanics

- **Penetration Testing**
  - Goal driven – not breadth
  - Look for the path of least resistance
  - Capitalize on the things you have:
    - De-prioritized
    - Forgotten
    - Don’t know about
    - Can’t control
  - I.e. we cheat to win, because the attackers will too!

Penetration Testing Mechanics

- Typical External pentest results.
  - We find fewer missing patches than we used to
  - Very little RCE on server OS or platforms
  - We still find application vulns. like SQLi
  - We find a lot of information disclosure
  - We use info. disclosure to target users
  - We use targeted spear phishing
  - Spear phishing gives us shells or creds
  - We either hit the cloud with creds
  - Or pivot with shells.

Penetration Testing Mechanics

- Typical Internal pentest results.
  - We find fewer missing OS patches
  - We find printers harboring domain creds
  - We get into the SharePoint repo
  - We find lots of poorly configured systems
  - We find default or easy to guess passwords
  - We pillage open NFS and SMB
  - We find hard coded creds, keys, certs etc.
  - We gain SYSTEM on member servers / root
  - We steal domain admin tokens

Penetration Testing Mechanics

A. Find external entry vulnerabilities

B. Find internal entry vulnerabilities

1. Gain any domain credentials to facilitate intel gathering on the network

2. Gain privileges of Local SYSTEM on Domain Member Servers

3. Traverse to different servers looking for powerful tokens & hashes

4. Steal tokens and hashes for powerful domain users & administrators

5. Use domain admin against Business

Penetration Testing Mechanics

- Our penetration tests are almost always successful at gaining access and gaining privileges…

- Why does this happen?
- Does the VM program help at all?
- What else do you need to do?

VM Program Gaps & Failings

- Pentests are good at exploiting:
  - Things you don't know about
  - Things you have forgotten
  - Things you are ignorant to
  - Things you have de-prioritized
  - Things you can't control

VM Program Gaps & Failings

- **Things you don't know about:**
  - Hosts that have been deployed
  - Services that exist via product installs
  - Unauthorized / unknown external gateways
  - Wireless networks connected to corp.
  - Infrastructure from acquisition of businesses
  - General shadow IT shenanigans

VM Program Easy Win [1]

- **Things you don't know about:**
  - Search for these
  - Use your VMP as asset discovery
  - Scan all your IP space
  - Investigate all wireless in the vicinity
  - Build an inventory – keep it up-to-date
  - Design process around asset ownership

VM Program Gaps & Failings

- **Things you have forgotten:**
  - Good hardening in most areas, but…
  - Some vendor default passwords sneak through
  - Some Tomcat consoles are still there (etc.)
  - Development servers with weaknesses
  - Legacy things you no longer use
  - Special configurations for special projects
  - Ex-employees / exit processing

VM Program Easy Win [2]

- **Things you have forgotten:**
  - Be rigorous
  - Search specifically for these things
  - Know each and every host and service
  - Check each service for default passwords
  - Look in every shared file location
  - Question whether hosts should ‘still be there’
  - Correlate users to employment records

VM Program Gaps & Failings

- **Things you are ignorant to:**
  - Setting an org-wide default password (onboarding)
  - Having a shared local admin / root password
  - Allowing users to be admin on their own box
  - Having a flat network with no segmentation
  - Printers can be your downfall
  - Use of single-factor authentication is a single point of failure (wireless, VPN, cloud, domain)

VM Program Easy Win [3]

- **Things you are ignorant to:**
  - Listen to your Pentesters
  - Learn about weaknesses
  - Figure out what everyone else is doing
  - Do at least that – then do more
  - Some things will be hard(er)

VM Program Gaps & Failings

- **Things you have de-prioritized:**
  - VMP is geared only to ‘critical production’ assets
  - Lower priority servers are not yet included
  - “Ah that system is going away soon(ish)”
  - “Admins are admin on their own build, because they are admins!”

VM Program Easy Win [4]

- **Things you have de-prioritized:**
  - Prioritization is of course important
  - But recognize that if an asset is:
    - Domain joined
  - It's security is as important as 'prod'
  - From an attacker's perspective it doesn't matter
  - De-prioritized systems are ways in
  - Exceptions to rules / process are ways in

VM Program Gaps & Failings

- **Things you can't control:**
  - Your users
  - (Mic drop)

VM Program Easy Win [5]

- **Things you can't control:**
  - There aren't many easy wins for users
  - Remove their privileges
  - Educate them (but recognize limits)
  - Be more direct – show them consequences
  - Think about designing solutions that:
    - Protect the org. from user actions

Design Improvements to Ent. Sec

- Securing an enterprise network is hard
- You will fail to secure it 100%
- Pentests exploit:
  - Size / Complexity
  - Human Error
  - Your 1%

- Embrace this problem and innovate through security design.

Design Improvements to Ent. Sec

1. Threat Model for Failure
2. Innovate from Failure Planning
3. Enhance Your VMP via Sec. Engineering

Design Improvements to Ent. Sec

Threat Model for Failure

Assume the worst, in-fact start there

1. Attackers are on your network (right now)
2. The attackers have control of your AD as DA

If 1 + 2 = true, how do you:

- Stop the attacks from getting your highest value data?

Hopefully you are thinking:

- “Store critical data away from the AD domain”

Design Improvements to Ent. Sec

Innovate from Failure Planning

Don't trust the domain for auth-N?	Use token based MFA
Physical office LAN compromise?	Create an 'empty network'
Your users can get phished?	Separate job ops from email
Attackers are on your network?	Funnel them into safe areas
	Waste their time
	Make things noisy
	Detect and contain!

- You don't have to do 'just the same as everyone else'

Design Improvements to Ent. Sec

Enhance Your VMP via Sec. Engineering

- Pentests often uncover systemic issues
- But remediation isn't tackled that way
- Most require 'fortification projects'
- These are bigger and take time
- But they get you where you need to go

Design Improvements to Ent. Sec

Final Thoughts

- It is a winnable war
- Your VMP is a good start
- You need to enhance it
- Listen to your ‘paid attackers’
- Patching & config. is not enough
- Plug those gaps the pentest uncovers

Thank You – Please Stay In Touch

- **Kevin Dunn**
- Technical VP – NCC Group
- **E:** kevin.dunn@nccgroup.trust
- **L:** https://www.linkedin.com/in/kevdunn
- **W:** https://www.nccgroup.trust/us

The Collin College Engineering Department

Collin College Student Chapter of the North Texas ISSA

North Texas ISSA (Information Systems Security Association)

Thank you