PENTEST POST-MORTEMS

A DECADE OF LESSONS LEARNED

What (Should) Keep You Up at Night

- P@ssw0rds are still w3@k! (+bonus content from Chad Finkenbiner, Information Assurance Consultant)
  - MFA is not fully implemented
- Employees are still your biggest weakness
- Scanning can give a false sense of security and so can your NG controls
- People make mistakes and poor decisions; even those in IT security
  - Hackers and pentesters have come to rely on these mistakes to propagate their access and gain privileges
- Capabilities of offensive security professionals have increased faster than those of defenders
- Developers still not trained in secure coding and S-SDLC not (fully) implemented
- Compliance gets in the way of security

SYNERCOMM

There is Good News

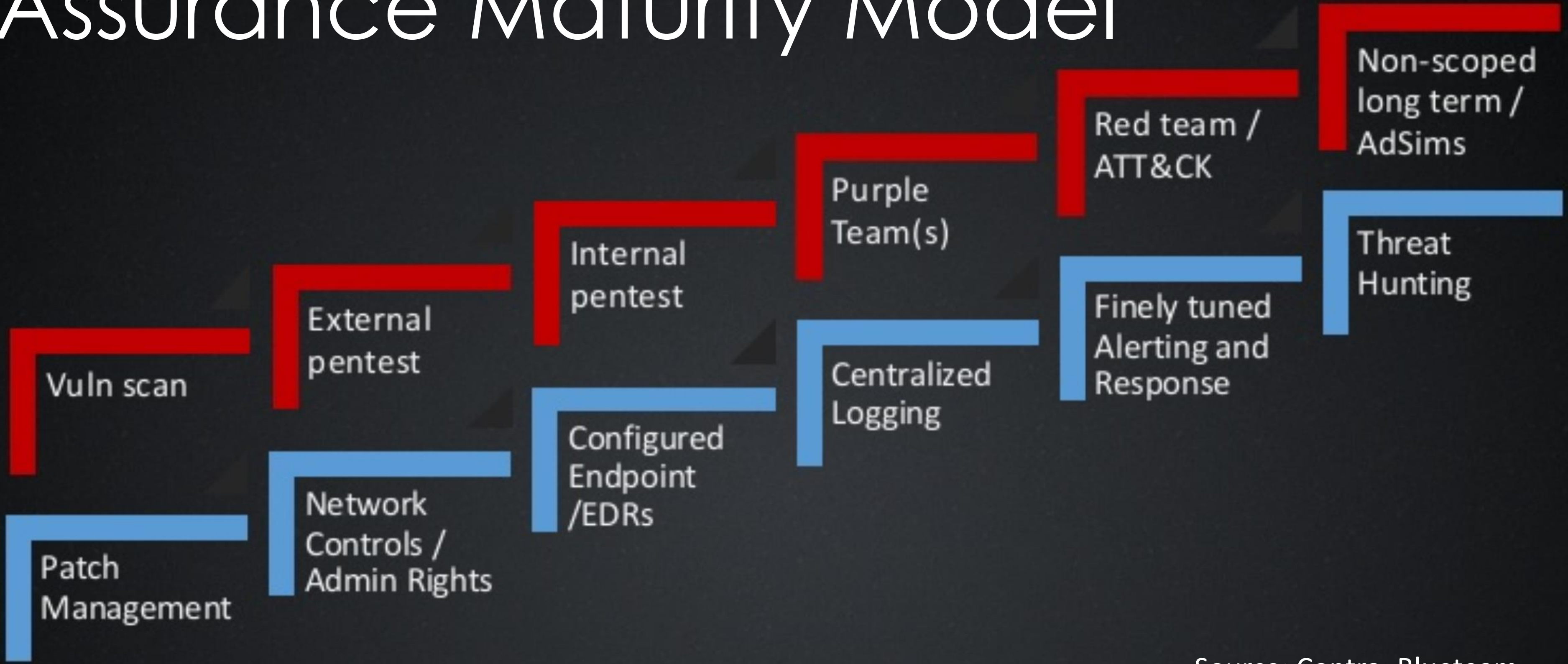
- Most companies now consider information or data security a top concern
- Widely exploited software vulnerabilities are down* (MS08-067, Adobe, Java, etc.)
  - Patching “may” also be improving???
- Best of class controls are available to companies of all sizes
- Perimeter security is “pretty good”
- Being good with Microsoft Windows, Active Directory, and Group Policy affords better detection, better prevention, and better security
- Visibility through centralized log aggregation, correlation, and alerting is possible!

SYNERCOMM

Validation Methods are Improving!

- Audits are Getting Technical
- (Properly Scoped) Network Penetration Testing
  - Your pentesters are getting better and the community of really good pentesters is growing
- Adversary Simulation New!
- Continuous Penetration Testing New!
- Red Team Exercises New!

Assurance Maturity Model



Vuln scan

Patch Management

External pentest

Network Controls / Admin Rights

Internal pentest

Configured Endpoint /EDRs

Purple Team(s)

Centralized Logging

Red team / ATT&CK

Finely tuned Alerting and Response

Non-scoped long term / AdSims

Threat Hunting

Source: Contra_Blueteam

Audits are Getting Technical

- The days of checklist “audits” are long gone (or at least they should be)
- Assessors should be validating your patch management, not running scans for you
- Passwords should be assessed through hash cracking to validate password policies and security awareness
- Active Directory and Group Policy is critical to security and visibility and should be reviewed
- Pentest techniques used in adversary simulations are more of a controls audit than a pentest
- Focus on the vulnerabilities and “mistakes” that allow successful attacks!

Pentest Scope Matters

- The “bad guys” don’t play by rules, so why do we enforce unreasonable constraints on a penetration tester?
  - External only, no propagation
  - No social engineering or no targeting executive leadership
  - Only test during nights and weekends
- Penetration testing is a ~~simulation of a~~ real attack
  - Make sure your pentests validate your security controls
  - Blend together reconnaissance, external penetration testing, social engineering, and internal penetration testing into a single scope
    - Add wireless pentesting and physical access attempts where and when it makes sense

Benefits of Adversary Simulation

- Train and prepare IT, security and response staff
  - 1-on-1 collaboration with a penetration tester revealing their tools, tactics and procedures
- Validate, tune and improve control effectiveness
  - Know which attacks you've got "covered" and where you remain vulnerable
  - Focus is on SIEM collection and alerting

Continuous Penetration Testing

- Extending “Point in Time” Pentests to Cover Long Gaps
- Using Automated Hourly and Daily Recon “Scans, Probes & Monitors” to Alert Human Pentesters
  - Changes to live IP addresses, services, subdomain registrations, certificates, applications, etc.
  - *Guaranteed “per month” human-led pentest

Background

Chad Finkenbiner

- 12 years in industry
- 3 years with ISSA Kentuckiana
- CISSP, CPAS, ITIL, Sec+, Net+, A+
- Defense Network Specialist – USMC
- Medical Imaging Systems Coordinator/Application Analyst – PACS
- Information Assurance Consultant, Auditor/Penetration Tester

Password Strength

- Key space: *how many possible characters*
  - Upper - 26
  - Lower - 26
  - Number - 10
  - Special - 33+
- Length: *number of used characters*

Password Strength

- Key space$^{\text{Length}}$
- A four-digit PIN has a key space of 10 and length of 4
  - 10,000 possible variations (10^4)
- An eight-character password consisting of uppercase, lowercase, and numbers has a key space of 62 and a length of 8
  - 218,340,105,584,896 possible variations (62^8)

Password Strength

- Which password is stronger?
  - P@ssW0rd
  - StrongestPassword

Password Strength

- Which password is stronger?
  - P@ssW0rd = 95^8
  - StrongestPassword

Password Strength

- Which password is stronger?
  - P@ssW0rd = 95^8
  - StrongestPassword = 52^{17}

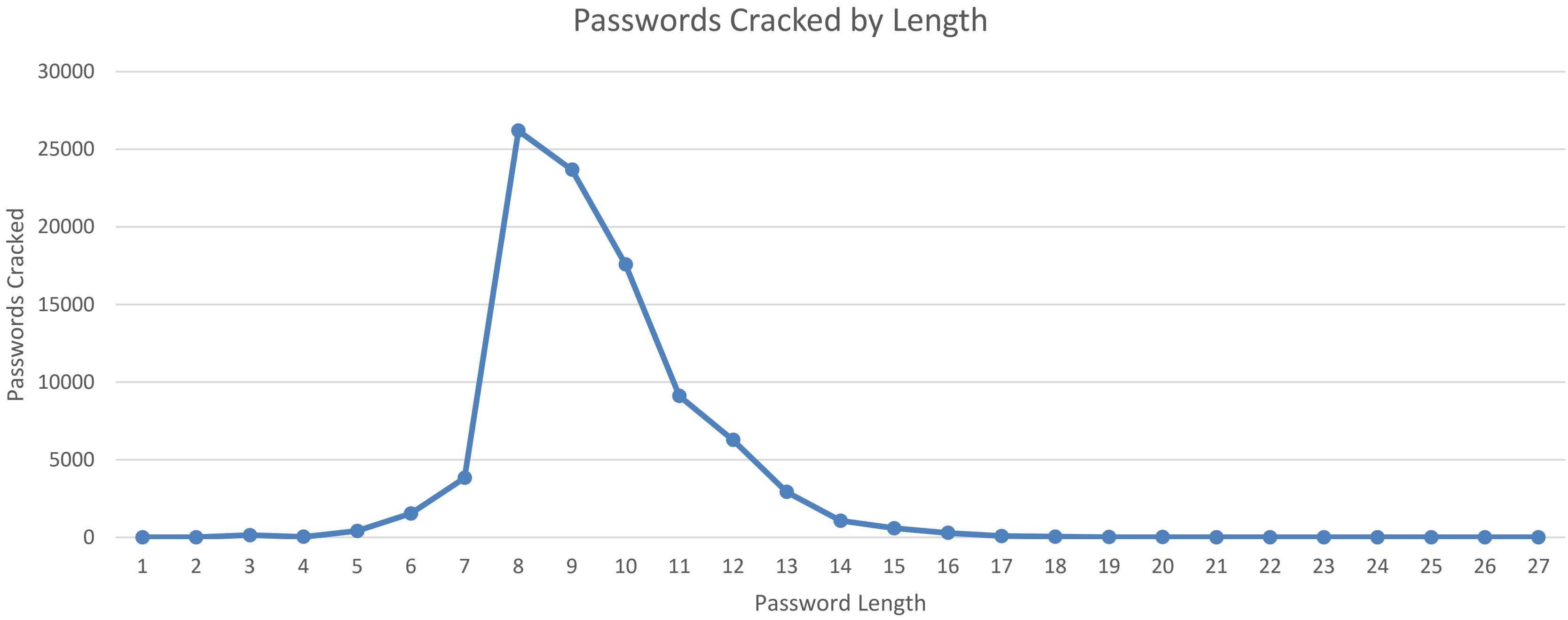
Password Strength

- Which password is stronger?
  - P@ssW0rd = 95^8 = 6,634,204,312,890,625
  - StrongestPassword = 52^{17}

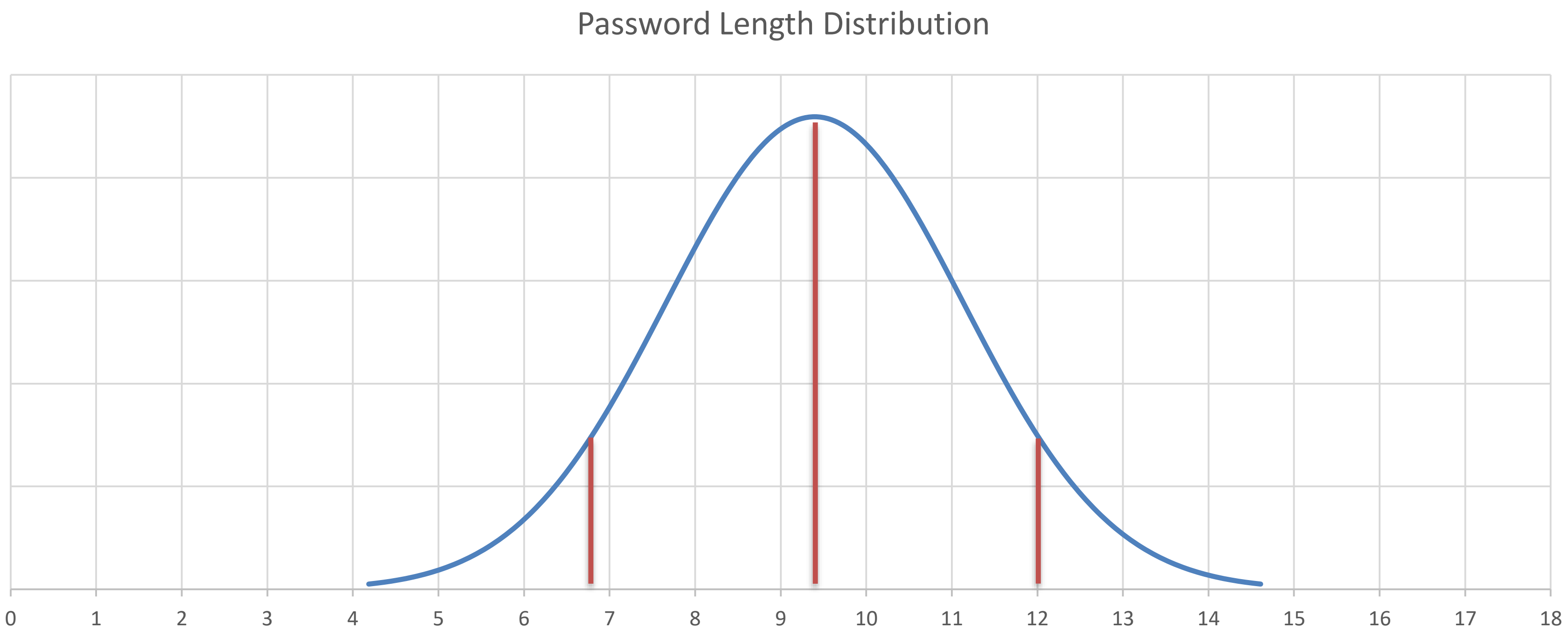
Password Strength

- Which password is stronger?
  - P@ssW0rd = 95^8 = 6,634,204,312,890,625
  - StrongestPassword = 52^{17} = 148,613,013,882,162,475,899,836,956,672

Analysis of password length



Analysis of password length



Questions ?

- Follow Us:
  - www.synercomm.com
  - Latest blogs:
    - Why 14 Characters?
      - SynerComm's 14-character minimum password recommendation
    - Thoughts on Blocking Powershell.exe
    - How to Build a (2nd) 8 GPU Password Cracker

SYNERCOMM