Pen Testing for OpenEdge

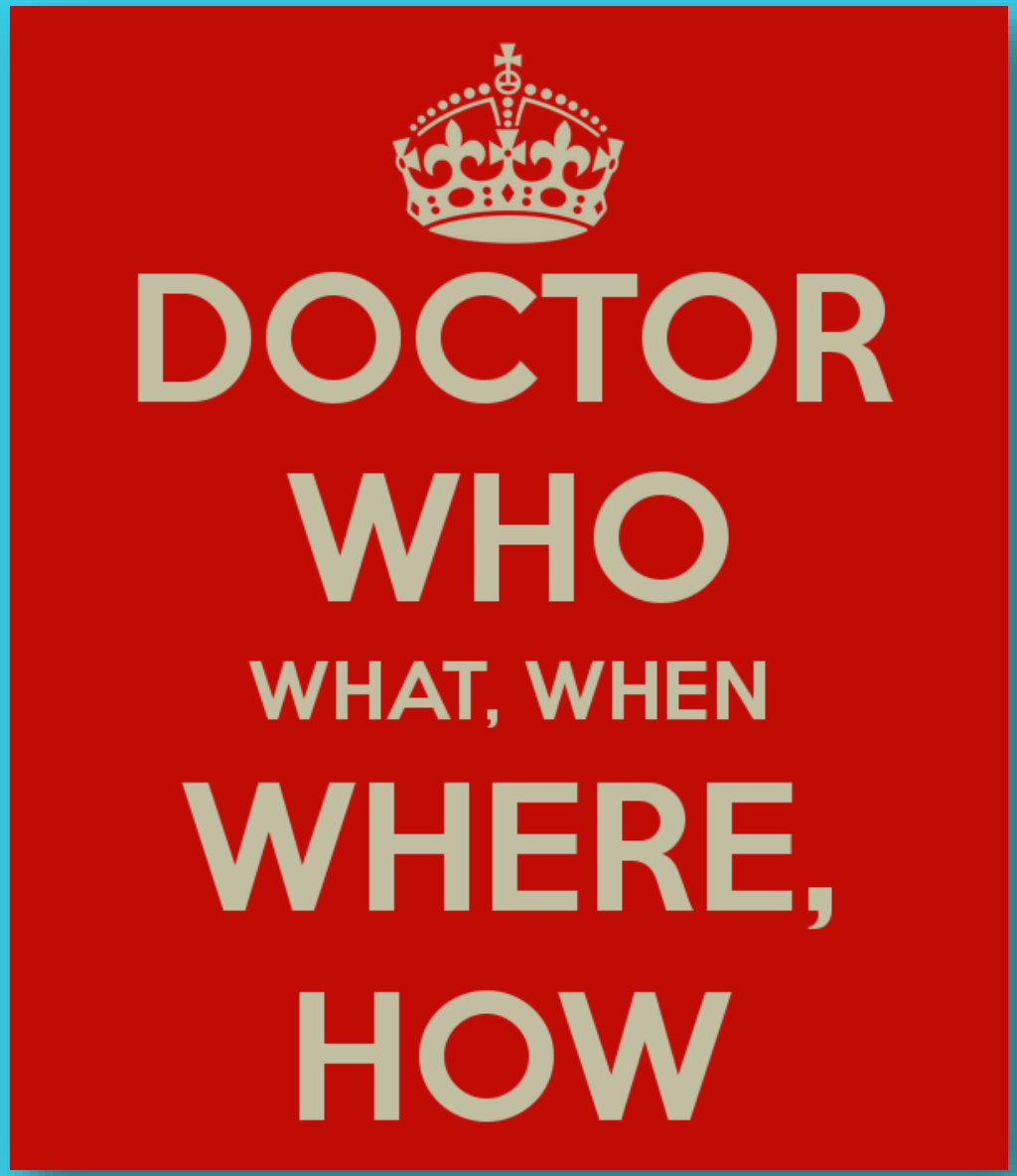
How penetration testing techniques can help secure your OpenEdge environment

Michael Solomon, Ph.D.

Your speaker

- **Michael Solomon, Ph.D.**
  - Solomon Consulting Inc, President and Principal consultant
  - GRC as a Service, LLC Principal Consultant
- CISSP®, CISM®, PMP®, PenTest+®
- Professor of CyberSecurity and Global Business with Blockchain Technology graduate programs, University of the Cumberlands, Williamsburg, KY
- Specializes in GRC Consulting for Complex Enterprise Environments with “Sensitive” Data
- Book Author (textbooks and cert prep), Cybersecurity and Project Management training video architect
- Private pilot and Star Wars miniatures games enthusiast

Agenda



PENETRATION TESTING

Three takeaways: Penetration testing is …

- Harder than you think
- More valuable than just a hacker game
- Instrumental in making your IT personnel better

Who should conduct a penetration test?

IT asset owner

Or authorized delegate

DO NOT pen test systems without authority!

Authorized individuals who want to know about

IT assets

Security vulnerabilities

Best practice gaps

Reasons to learn pen testing

Fun and Dangerous

Yields actionable information

Sharpens skills

What is penetration testing?

IT asset discovery

Security assessment (one type)

- **Vulnerability assessment**
  - Identify risks, vulnerabilities, and misconfigurations
  - Prioritized remediation action items
- **Penetration testing**
  - Automated & manual techniques to find AND exploit vulnerabilities
  - Goal is to realize threats
- **Social engineering**
  - Exploit flaws in human behavior and confidence

Pen Testing addresses one important need

- Demonstrating that exploits work

What is penetration testing?

- Active and commonly intrusive
  - May be destructive
- Tests the effectiveness of security controls
  - “Success” is finding security holes
- Mirrors the activities of attackers
  - Not a simulation
  - The goal is to beat the attackers to the punch
- Overall purpose is to reduce risk in an information system

Why should you conduct pen tests?

IP discovery and asset inventory

Do you REALLY know what's out there?

Compliance

PCI-DSS, NIST, HIPAA, FFIEC, FINRA

Security best practices

Stakeholder assurance

Risk management – vulnerability management life cycle

Keeping up with the attackers (they use it)

Red team/blue team

Ongoing war games

OpenEdge scope

Database

Application

Integration

When should you pen test?

Pen testing - an essential activity

- Should be performed regularly
  - Sometimes mandated
- Secures the functioning of a system

Pen test indications

- Identifying new threats
- Adding a new network infrastructure
- Updating a system or deploying new software
- Relocating physical assets (IT or other)

Organizational changes

- Premerger
- Supply chain participant change

Where (or what assets) should you test?

Target scoping

- Internal
- External
- Physical/virtual servers and devices
- Users
- Applications

Inclusions/exclusions

- Consider impact to production environment

Rules of engagement

- How far can you go?

How Do You Carry Out Pen tests?

Project management is essential

- Activities can easily get out of hand

Scheduling

- When (days/times) can/should test be run?
- Who (if anyone) should be notified?
- When must tests be completed?

Scope Creep – common in nearly all projects

- Occurs when client requests additional tasks after SOW is signed
- Many may seem “doable”
- Takes resources away from core SOW tasks
- Must get authorization for any SOW modifications

Planning

Working with a customer to clearly define and document assessment objectives, scope, and rules of engagement.

Gathering Information

Collecting and examining key information about an application and its infrastructure.

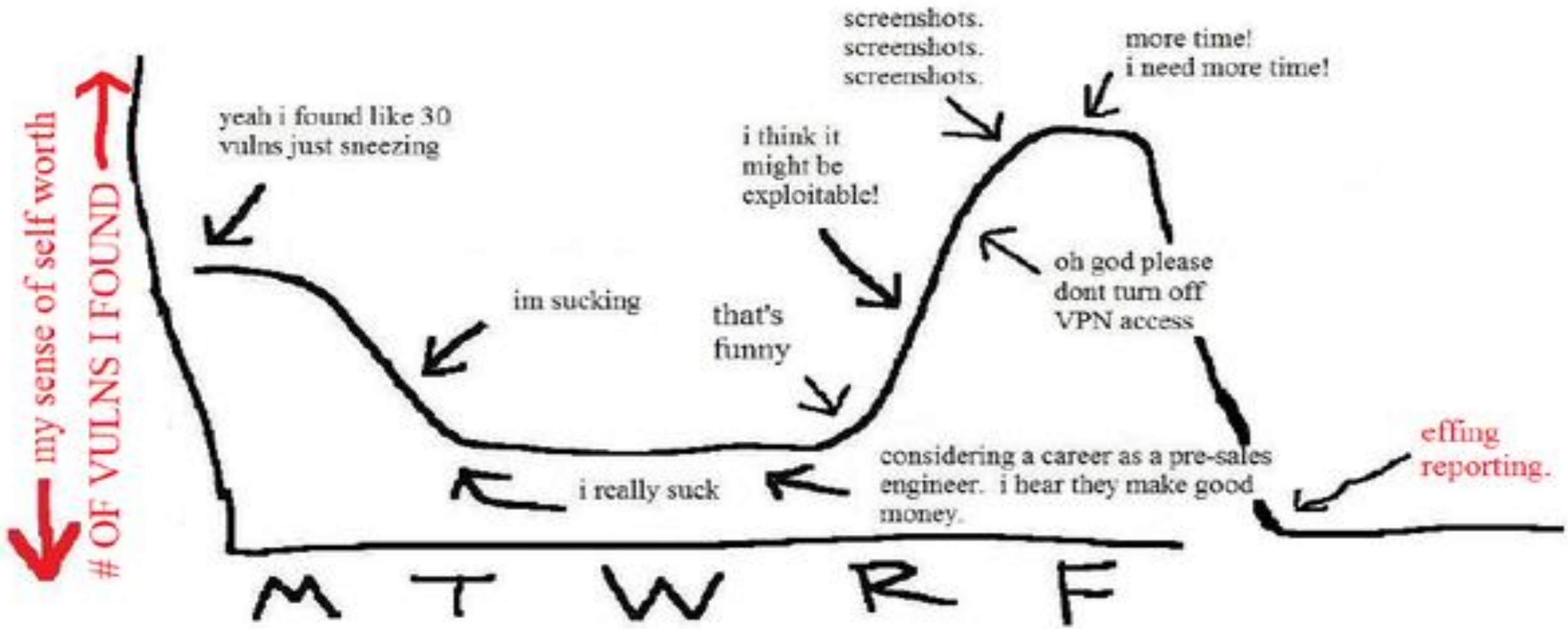
Discovering Vulnerabilities

Finding existing vulnerabilities, using both manual and automated techniques.

Reporting

Providing a comprehensive report with deep analysis and recommendations on how to mitigate the discovered vulnerabilities.

Real World Pen Testing



Stage 1 - Planning

Get written authorization

- Only way to stay out of trouble
- Make sure the issuer has the authority

Get the management team on board

- Pen tests can crash, corrupt, or slow down services
- Establish communication and escalation path

OpenEdge asset scope

- DB servers / AppServers / Web servers
- Interface layers / Supporting service providers
- Clients
- Physical infrastructure / humans

Stage 2 - Information Gathering

Mainly scanning and enumeration

Lots of tools

nmap

whois - not just for unknown entities

netcat, nc, ncat, hping

Wireshark, aircrack-ng

Fingerprinting

Open Source Intelligence Gathering (OSINT)

Stage 2 – OSINT resources

- OSINT resources
  - Google / DuckDuckGo (yeah, Bing, too)
  - CERT (Computer Emergency Response Team) - https://www.us-cert.gov/
  - NIST (National Institute of Standards and Technology) - https://csrc.nist.gov/
  - JPCERT (Japan's CERT) - https://www.jpcert.or.jp/english/vh/project.html
  - CAPEC (Common Attack Pattern Enumeration & Classification) - https://capec.mitre.org/
  - Full disclosure – Popular mailing list from the folks who brought us nmap - http://seclists.org/fulldisclosure/
  - CVE (Common Vulnerabilities and Exposures) - https://cve.mitre.org/
  - CWE (Common Weakness Enumeration) - https://cwe.mitre.org/

Stage 2 – Information gathering examples

Discovery scan – used to find potential targets

- nmap ping sweep: nmap –sP target

Full scan – scans ports, services, and vulnerabilities

- Full scan (with fingerprinting):
  - nmap –A target
  - perl nikto.pl –h target
  - OpenVAS / Nessus
- Port scan: nmap –p ports target

Stealth scan – try to avoid tripping defensive control thresholds

- nmap –sS target

Stage 2 – Information gathering demo

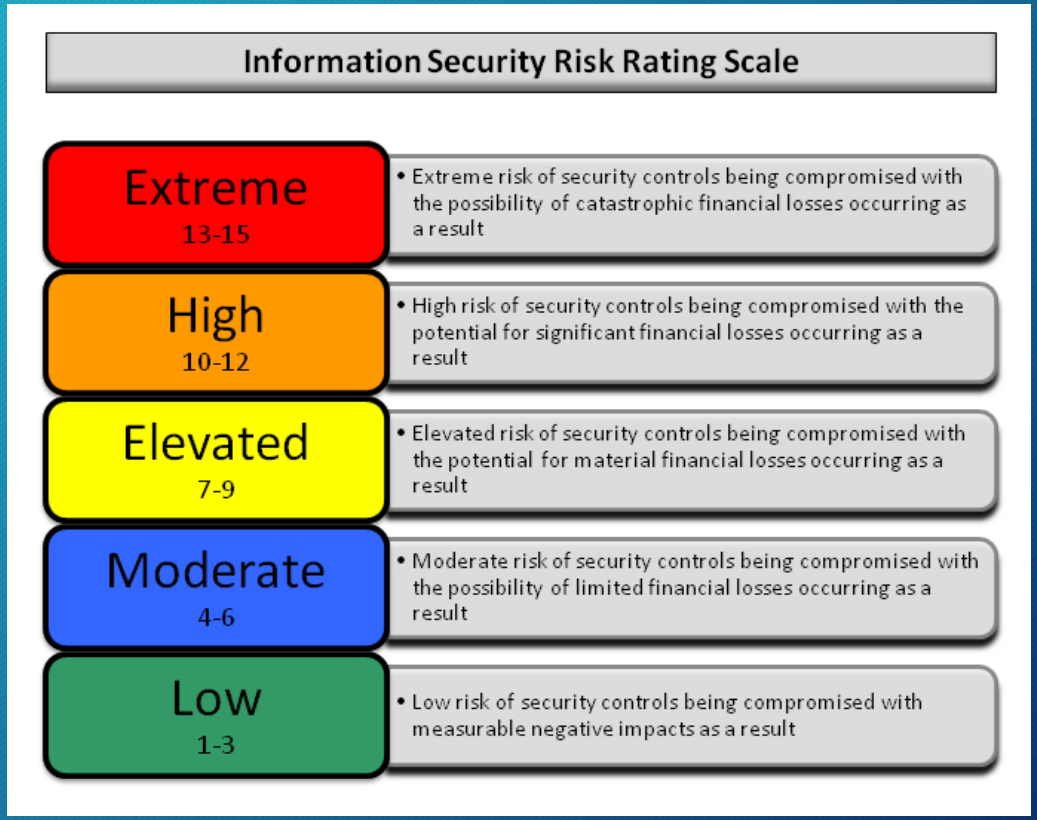
Stage 3 – Discovering Vulnerabilities

- Lots of tools (way too many to list here)
  - nmap
  - OpenVAS, Nessus, Metasploit, nikto, SQLmap
  - Many tools in Kali Linux
- Automated tools
  - Helpful, but not granular enough
- Scripting skills help a lot
  - Python
  - Bash / PowerShell
  - Ruby

Stage 3 – Discovering Vulnerabilities demo

Stage 4 - Reporting

- Prioritize
  - Much of the value is in identifying what's most important
  - Context sensitive to the sponsoring organization
- Summarize
  - Executive summary
  - Technical summary
- Translate
  - Bot all readers are technical / security savvy
- Visualize
  - A picture is worth a thousand words
  - A bad picture takes a thousand words to unexplain



Pen testing resources

- Penetration Testing Execution Standard
  - http://www.pentest-standard.org
- CompTIA PenTest+
  - https://certification.comptia.org/certifications/pentest
- Offensive Security Certified Professional (OSCP)
  - https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/
- SANS Pen Testing
  - https://pen-testing.sans.org/
- Ethical Hacking
  - https://www.ehacking.net/

CompTIA PenTest+

Learn how to be a pen tester

- Plan and scope penetration tests
- Find vulnerabilities and run exploits
- Scan and enumerate targets
- Conduct social engineering attacks
- Use tools like Oracle VM, Kali Linux, Metasploitable, and DVWA

Find it at Udemy.com today

From Total Seminars and Michael Solomon


QUESTIONS
poll
asking
query
ask
reply
questions
q&a
challenge
investigation
confusion
problem
answers
interrogation
who
what
how
when
puzzle

Michael Solomon
ms@grc-as-a-service.com