Version 2009-02
See http://resources.MavenSecurity.com for the most recent version

A CISO's Guide to Ethical Hacking

Maven Security Consulting Inc.

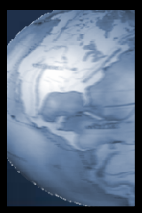
+1-877-MAVEN-HQ (+1-877-628-3647)
www.MavenSecurity.com

Session Agenda

Do not just sit there:

- Ask questions
- Share your experience
- Challenge me

slide 2



- ***What is Ethical Hacking?***
- ***Key Features of Ethical Hacking***
- ***Ethical Hacking Pros & Cons***
- ***Why use Ethical Hacking?***
- ***Limitations of Ethical Hacking***
- ***Who should perform the work? External vs. Internal***
- ***How often should EH be used?***
- ***When in the lifecycle should you use EH?***
- ***Shopping for EH - Things to Look for***
- ***The Risks of Ethical Hacking***
- ***Safety Measures***
- ***Using Ethical Hacking for Your 3rd Party Service Providers***
- ***EH Recommendations***
- ***Game Plan / Recommendations***

I am the one on the right.

<PROPAGANDA>
David Rhoades is a principal consultant with Maven Security Consulting Inc. (www.mavensecurity.com). Maven Security Consulting Inc. provides information security assessments and training, and is headquartered in Delaware.

David's expertise includes web application security, network security, and ethical hacking. David has been active in information security consulting since 1996, when he began his career with the computer security and telephony fraud group at Bell Communications Research (Bellcore).

David teaches domestically and internationally at various security conferences, and teaches for USENIX (www.usenix.org), MIS Training Institute (www.misti.com), ISACA (www.isaca.org), and previously for the SANS Institute (www.sans.org).

David has a Bachelor of Science degree in Computer Engineering from the Pennsylvania State University (psu.edu).

Maven Security Consulting Inc. provides information security services for a global client base. Their clientele span numerous industries, including government, banking, insurance, aerospace, software, and recreation. Services include ethical hacking; web application security testing; training; and architecture analysis, design, and security testing for Next Generation Networks (NGN), including VoIP.

www.MavenSecurity.com

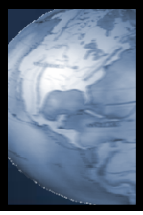
</PROPAGANDA>

What is Ethical Hacking?

I'll use the initials EH to refer to Ethical Hacking from this point forward.

- ***Ethical hacking (EH) is the process of having authorized individuals exercise the security of a target.***
  - *A.K.A. Penetration Testing, Tiger Team*
  - *Find the flaws and mitigate the risks*
- ***An ethical hacker is someone who has permission to exercise the security of a target.***

slide 4



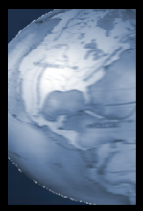
Maven SECURITY CONSULTING

An older term for ethical hacking is penetration testing. This is still very popular. An even older term is "tiger team". See http://en.wikipedia.org/wiki/Tiger_team

Key Features of Ethical Hacking 1

- ***EH has some distinct features when compared to routine security / vulnerability scans.***
- ***Vulnerability / Security scanning is:***
  - *Highly or completely automated*
  - *The goal is to find as many security flaws as possible*

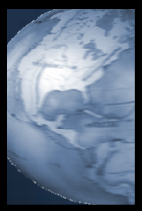
slide 5



Maven SECURITY CONSULTING

Key Features of Ethical Hacking 2

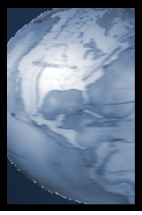
- ***EH focuses on an objective;***
  - *How far can the "attacker" go?*
  - *Can you get to system X or data Y?*
- ***A vulnerability scan could be a sub-set of EH (if desired).***
- ***Step 1: Find a weakness***
- ***Step 2: Exploit it to get additional access***
- ***Step 3: Repeat the process until objective reached (e.g. access to critical data or system)***



Maven SECURITY CONSULTING

Key Features of Ethical Hacking 3

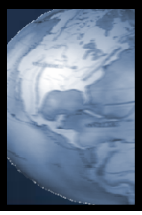
- ***EH will typically exploit the security flaws in order to gain access to data or another system***
- ***This eliminates false-positives by validating the flaw***
  - *A security scanner can have many false-positives*



Maven SECURITY CONSULTING

Ethical Hacking Example 1

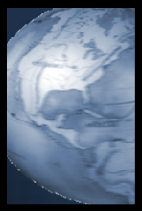
- ***1) Scan the web server***
  - *Locates a buffer overflow (flaw #1)*
  - *Exploiting flaw #1 results in an account on the web server*
- ***2) (From web server) Scan the database behind firewall (web and DB trusted each other, firewall allowed traffic)***
- ***3) Find weakness in DB (flaw #2)***
  - *Exploiting flaw #2 results in retrieving the DB password*
  - *The password is cracked*
  - *DB user/password is the same as the firewall (flaw #3)*
- ***4) Firewall is compromised; custom rule allows EH team to pass any traffic through***



Maven SECURITY CONSULTING

Ethical Hacking Example 2

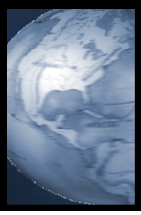
- ***A typical vulnerability scan would have stopped at step 1.***
  - *Flaw #1 on the web server*
- ***Therefore the true extent of the risk would not have been known.***
- ***Also, the DB flaw would have gone unnoticed (unless an internal scan was also performed)***



Maven SECURITY CONSULTING

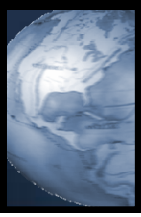
Ethical Hacking Pros & Cons

- ***Advantages:***
  - *Find true level of exposure, not just the surface*
- ***Disadvantage***
  - *Disruption potential*
    - Exploiting flaws in production?!?
  - *Higher skill set needed*
  - *Other issues may be ignored due to time limits*

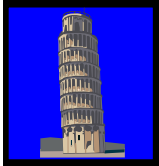


A Note about Terminology

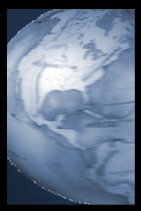
- ***What one person calls "ethical hacking", another person will call "security testing" or a "vulnerability assessment".***
- ***The key is to define the objective and the rules of engagement.***
- ***Example: Maybe you only want exploitation of flaws performed on a case-by-case basis (i.e. approval required) rather than a no-holds-barred approach.***



Why use Ethical Hacking?



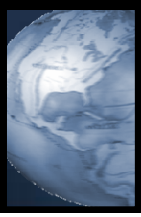
slide 12



- ***Provides proof of insecurities***
- ***Helps expose the true risk of flaws found***
- ***The process of using EH is generally accepted best practice; therefore it…***
- ***Demonstrates due care in maintaining a secure environment***
- ***Alternatively, NOT using EH could be grounds to suspect a lack of due care***

Limitations of Ethical Hacking

slide 13

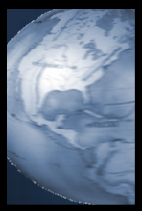


- ***Only a snap-shot in time***
- ***Only a small part of a larger security program***
  - *Security requirements during design phase is the most important*
  - *Code reviews are great*
- ***Cannot prove the system is secure, EH can only prove the system is not secure (by failing the audit)***
- ***EH will only find a subset of flaws, whereas code reviews and policy audits find others.***

Who should perform the work? External

- ***Most organizations use a trusted third party***
  - *Core competency*
    - Cost effective; better results
  - *Neutral party*
    - Unbiased results
  - *Extra layer of due care*
  - *"3rd party" required by law*
    - Maybe that could be a separate internal group?
    - Idea of a true 3rd party seems best

slide 14

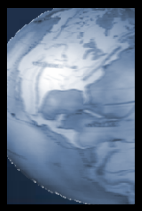


Maven SECURITY CONSULTING

Who should perform the work? Internal

- ***Internal resources are useful if you can afford them.***
- ***Typically seen for high-security situations: Financial & Military***
  - *However, becoming more common*
- ***Great resource for development - check the security bugs early and save money***
  - *Beware of developer turn over - bad security habits will return as senior developers get promoted and junior ones take their place*

slide 15



Maven SECURITY CONSULTING

How often should EH be used?

- ***At least once a year (like financial audits) by a 3rd party***
- ***Internal tests can be conducted as often as practical; typically after a major revision***

slide 16

Maven SECURITY CONSULTING

When in the lifecycle should you use EH?

- ***At the very least you should test before going into production***
  - *Reality shows this is not the most common scenario*
- ***Ideally do some testing during development***
  - *Limited testing of common issues*
- ***Thorough testing after the system/application is stable (i.e. after UAT if possible)***
- ***TIP: Plan on sufficient lead time to fix the problems found.***
  Don't test the night before going live!

slide 17

Maven SECURITY CONSULTING

UAT means user acceptance testing

Shopping for EH - Things to Look for 1

- ***STEP #1: Get a mutual NDA signed before talking to outsiders (CYA).***
- ***Background check of company. Lawsuits?***
- ***Verify the background check of the <u>specific</u> EH team members***
  - *Don't simply accept a verbal pass from the EH company.*
- ***Does background check mean criminal and financial? Maybe it should.***
- ***Read the liability release form (get out of jail free)- or write your own***

slide 18

Maven SECURITY CONSULTING

Shopping for EH - Things to Look for 2

- ***Are they incorporated, and where?***
- ***E&O insurance? How much?***
- ***Perform a site visit; reserve the right for future visits***
- ***Vendor neutral***
  - *Beware of up sell.*
- ***Separation of duties - design vs. test***

slide 19

Maven SECURITY CONSULTING

Shopping for EH - Beware of "Proprietary" Methodologies

- ***If an EH provider will not let you observe their work in progress because it is a "proprietary" methodology then something is not right***
- ***The methodology might have four parts:***
  - *Point, Click, Print, and Invoice*

slide 20

Maven SECURITY CONSULTING

Shopping for EH - Bait & Switch

- ***Beware of bait & switch***
  - *Senior consultant is brought out for pre-sales meetings or the kick-off,*
  - *but then the actual work is done primarily by a junior staff member.*

slide 21

Maven SECURITY CONSULTING

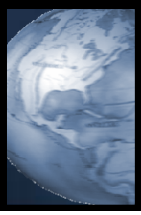
Beware of companies with staff members that brag about being “black hats” or ex-hackers. Most companies will deny that they hire people with prior computer related convictions. Many companies will insist they do background checks. But do they really? Ask to see the results of the background checks. While everybody deserves a second chance in life, you have to ask yourself, “Are you willing to give them that second chance while they have access to your company’s most sensitive data?”

Mr. Rootkit Story
A security consultant was hired to verify and maintain a secure OS configuration on a firewall system. He decided to install a rootkit to allow himself remote administration of the system - to make his job easier. The customer found out and was less than happy.

The Risks of Ethical Hacking

- ***We will discuss mitigating these risks next***
  - *Service disruptions*
  - *False sense of security*
  - *EH results fall into the wrong hands*

slide 23



Maven SECURITY CONSULTING

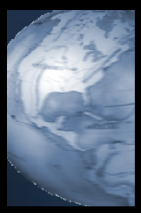
Safety Measures after Testing - Protect the Output

Story: Kinko's box - "I brought copies for everyone."

Story: Network printing of forensic data (pictures!) - bad idea.

- ***The output is sensitive (e.g. scanner files, the report)***
  - *Use existing information classifications (e.g. confidential, private, "DO NOT COPY OR FORWARD, etc)*
  - *Limit distribution of results*
    - Customize the level of detail based on the need to know
  - *Be sure tool output is not webified (Google Hacking)*
  - *Encrypt the raw files and secure on CD-R*
  - *Printed with local non-networked printer*
    - Not a public copy shop! Have you seen the people that work in those places at 2 AM?!?
- ***I like PDFs: strong crypto, restricts read access, prevents changes, prevents copy & paste, and/or printing if desired***
  - *http://www.pdfstore.com/*

slide 24



Maven SECURITY CONSULTING

Customized versions and distribution

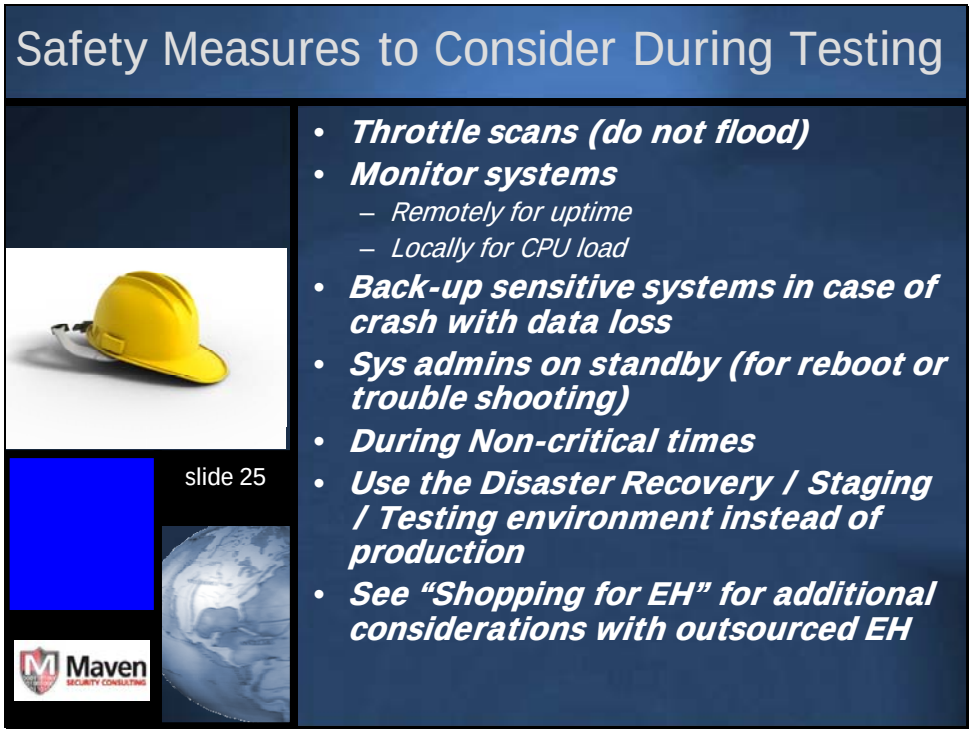
Everybody does not need the entire report; just the parts that pertain to them

E.g. Each department or system owner would get recommendations for their own systems.

Perhaps explicit "how to exploit" details (if any) should be removed for some staff members

E.g. Instead of saying, “System X can be hacked using technique Z.”, you can say, “System X needs patch Y.”

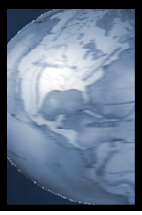
References:
http://www.legalstore.com/cat/Security+Paper.html
Security paper can help prevent copying by exposing hidden text when this type of paper is copied or scanned. This will alert the person to the fact that unauthorized duplication of the document is not permitted.
In my experience this is rarely done, but is something to consider for very sensitive reports.



Using Ethical Hacking for Your 3rd Party Service Providers - Remote System

- ***If you are not hosting the system then the easiest way seems to contract with your provider (e.g. ASP) and have them hire a mutually agreed upon 3rd party.***
- ***Contract states that you get a copy of the report.***
- ***NDA will be required from you to safeguard sensitive information about the 3rd party***
- ***Try to get them to pay for the EH (since they benefit)***

slide 26

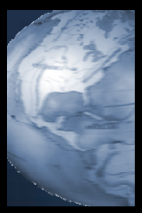


Maven SECURITY CONSULTING

Using Ethical Hacking for Your 3rd Party Service Providers - Local System

- ***If you are hosting the system / software; and it is not tied to 3rd party system or data, then MAYBE you can simply do it yourself***
- ***Check with legal counsel - some software vendors have restrictions in their licenses (e.g. first born child)***
- ***Try to split the cost in exchange for a copy of the report***
- ***Make them promise to fix high-risk issues by the next release (this is where being a big customer helps).***
- ***Consider NDA and/or sanitized report to protect your sensitive information***

slide 27



Maven SECURITY CONSULTING

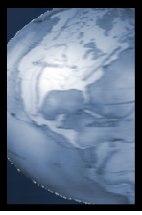
If you are hosting the system / software; and it is not tied to 3rd party system or data, then MAYBE you can simply do it yourself
Check with legal counsel - some software vendors have clauses in their licenses
"Though shalt not reverse engineer."
EH does not have to involve reverse engineering
Still, it is best to double check license restrictions
Try to get vendor to split the cost in exchange for a copy of the report

Make them promise to fix high-risk issues by the next release (this is where being a big customer helps)..
NDA will be required from them to safeguard your sensitive information in the shared report (or give them a sanitized version)

EH Recommendations - QA & Training

- ***Observe the EH team in action (at least for the first assessment). This provides:***
  - *Quality Assurance - see what you are getting*
  - *Knowledge Transfer - insist on knowledge sharing to help improve your internal resources (e.g. IT auditors)*
    - Two objectives (security test & training) in one expense
    - NOTE: This will slow things down a bit as time is taken to explain actions and results.

slide 28

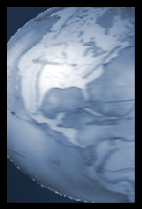


Maven SECURITY CONSULTING

EH Recommendation - Rotate Your Service Providers

- ***Rotate between two or three providers***
- ***Avoids tunnel vision***
- ***Allows you to compare providers for quality assurance purposes***
- ***Think bandwidth: Established relationships with multiple EH providers helps with sudden man-power issues***
  - *E.g. You just inherited a new group and there apps have never been tested.*

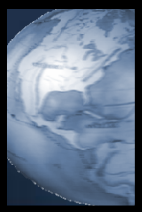
slide 29



Maven SECURITY CONSULTING

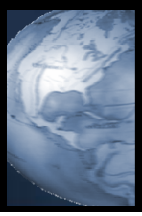
Game Plan / Recommendations

- ***Prioritize your systems / services by importance***
- ***Begin with preliminary "scan" via internal resources if possible***
- ***Use a 3rd party once a year; of after a "major" revision***
  - *Major revision should at least include changes in security functions/features.*



Questions? Fill out Evals! Download slides!

- ***Questions? Comments?***
- ***Fill out the course eval***
  - *Last page of agenda*
- ***By Monday these slides will be online at www.MavenSecurity.com***
  *(under **Resources** section)*
- ***Contact me at***
  - *David Rhoades*
  - *david.rhoades @mavensecurity.com*
  - *Assessments, onsite training, etc...*
    - www.MavenSecurity.com
    - Auditing web apps since 1996
- ***Thank you***



www.MavenSecurity.com

Honor + Knowledge = Security