Welcome to

11. Forensics 2: Incident Response

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

11-forensics-incident-response.tex in the repo security-courses

Plan for today

Subjects

- Attack and Response
- Attack graphs
- Attack surfaces, and reducing them
- Intrusion Handling, phases
- Digital Forensics

Exercises

- Clean or rebuild a server, use example Debian with your cron job vuln as example
- Cloud environments influence on incident response

Reading Summary

Bishop chapter 27

Incident Handler's Handbook - ca 18 pages

Browse / skim this:

Attack and Response

Definition 27-1 *Attack* is a sequence of actions that create a violation of a security policy.

Definition 27-2 A *goal* is that which the attacker hopes to achieve.

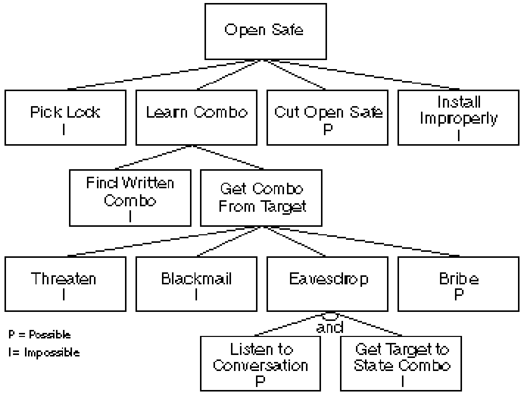
Definition 27-3 A *target* of an attack is the entity that the attacker wishes to affect.

Definition 27-4 A *multistage attack* is an attack that requires seceral steps to achieve it's goal.

Most attacks are multistage.

Example goals: access to systems for learning, stealing, for spamming, for embarrassment

Attack trees



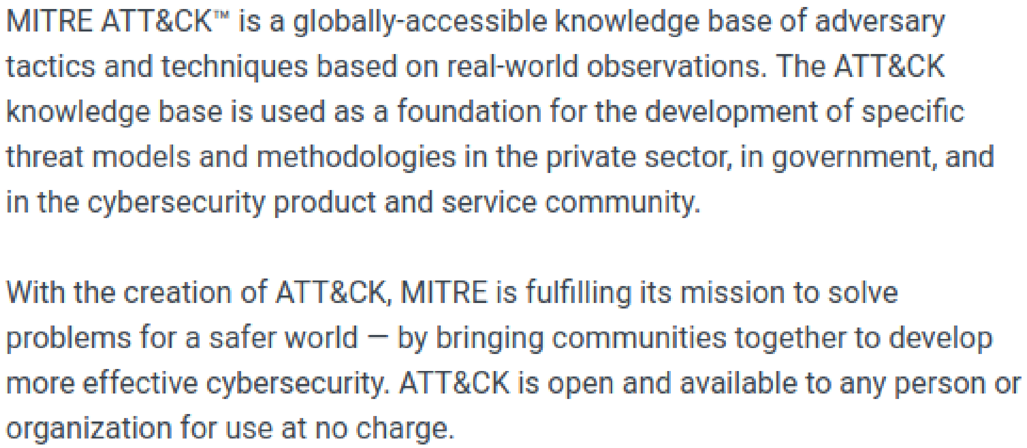
- Attacks can be said to be based on a chain of dependencies, or graphs
- To achieve goal, need to achieve sub goal x, y, and z – Break the chain and the attack fails!
- Simple example, installing updates remove a dependency for a vulnerability
- Attack trees, picture from:

`https://www.schneier.com/academic/archives/1999/12/attack_trees.html`

Attack surfaces, and reducing them

- Incident prevention
- Real-time intrusion detection systems (IDS/IPS)
- **Definition 27-7** An *attack surface* is the set of entry points and data that attackers can use to compromise a system.
- Address space layout randomization (ASLR) is a host-level moving target defense.
- OpenBSD even randomizes the kernel on install – kernel address randomized link (KARL)

Remember the MITRE ATT&CK framework



MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

https://attack.mitre.org/

Penetration testing

Verification of the system in place

Examines procedural and operational controls

Is the system in fact installed and operated as expected

Example, is the firewall even enabled?

Penetration testing methodologies
https://www.owasp.org/index.php/Penetration_testing_methodologies

Security Assessment Frameworks

- Structured approach to testing, finding and eliminating security flaws
- Information Systems Security Assessment Framework ISSAF
- Penetration Testing Execution Standard (PTES)
- PCI Penetration testing guide, Payment Card Industry Data Security Standard (PCI DSS)
- Technical Guide to Information Security Testing and Assessment (NIST800-115) (GISTA)
- Open Source Security Testing Methodology Manual (OSSTMM)
- CREST Penetration Testing Guide

Which one to choose?

From the book Bishop and `https://www.owasp.org/index.php/Penetration_testing_methodologies`

Intrusion Handling, phases

- *Preparation* for an attack, establish procedures and mechanisms for detecting and responding to attacks
- *Identification* of an attack, notice the attack is ongoing
- *Containment* (confinement) of the attack, limit effects of the attack as much as possible
- *Eradication* of the attack, stop attacker, block further similar attacks
- *Recovery* from the attack, restore system to a secure state
- *Follow-up* to the attack, include lessons learned – improve environment

These are very high-level. Multiple books and courses exist on this subject alone. A short example for today was the *Incident Handler's Handbook* by Patrick Kral

Honeypot Definition

> In computer terminology, a **honeypot** is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked.

Source: `https://en.wikipedia.org/wiki/Honeypot_(computing)`

also used as Honeynet - monitored network infrastructure

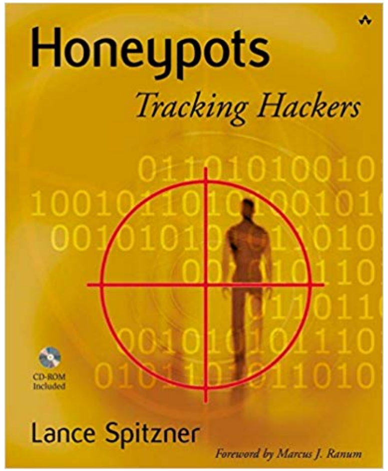
En honeypot består typisk af:

- Et eller flere sårbare systemer
- Et eller flere systemer der logger traffik til og fra honeypot systemerne

Meningen med en honeypot er at den bliver angrebet og brudt ind i, se også Canary Tokens

History of honeypots

An Evening with Berferd



Artikel om en hacker der lokkes, vurderes, overvåges

Et tidligt eksempel på en honeypot

Senere kom The Honeynet Project `http://www.honeynet.org`

Billede er: *Honeypots: Tracking Hackers* af Lance Spitzner, 2003

Honeypot Definition

> In computer terminology, a **honeypot** is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked.

Source: `https://en.wikipedia.org/wiki/Honeypot_(computing)`

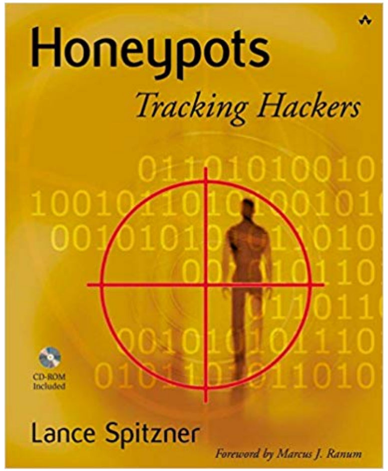
also used as Honeynet - monitored network infrastructure

En honeypot består typisk af:

- Et eller flere sårbare systemer
- Et eller flere systemer der logger traffik til og fra honeypot systemerne

Meningen med en honeypot er at den bliver angrebet og brudt ind i, se også Canary Tokens

History of honeypots – An Evening with Berferd



Artikel om en hacker der lokkes, vurderes, overvåges

Et tidligt eksempel på en honeypot

Senere kom The Honeynet Project `http://www.honeynet.org`

Billede er: *Honeypots: Tracking Hackers* af Lance Spitzner, 2003

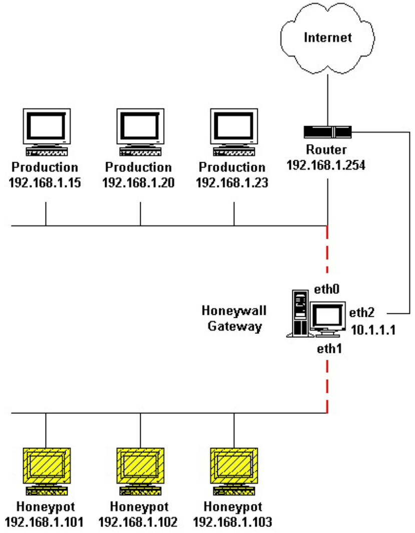
Honeypot High interaction and low interaction

High-interaction honeypots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste their time. By employing virtual machines, multiple honeypots can be hosted on a single physical machine. Therefore, even if the honeypot is compromised, it can be restored more quickly. In general, high-interaction honeypots provide more security by being difficult to detect, but they are expensive to maintain. If virtual machines are not available, one physical computer must be maintained for each honeypot, which can be exorbitantly expensive. Example: Honeynet.

Low-interaction honeypots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyd.

Source: `https://en.wikipedia.org/wiki/Honeypot_(computing)`

Honeynets - Why use them research, production



Creating a network architecture with multiple systems become a honeynet.

- Lessons Learned from `http://old.honeynet.org/papers/edu/`
- Out of all of this were a variety of lessons learned things to do and NOT to do. Hopefully this short list can help you avoid some common mistakes.

- Start Small - If you are going to install a honeynet within your enterprise, start small. Begin initially with two machines (in order to detect sweep scans of your honeynet) with operating systems that you are familiar with installed behind the reverse firewall.
- Maintain good relations with your enterprise administrators. THIS IS CRITICAL! Inform your network administrators of the types of exploits that you are seeing. In some cases, they will already be aware of these exploits, but in other cases, you will have been the first person to notice them.
- Focus on attacks and exploits originating from within your enterprise network. Theses are the attacks that can do the most damage to your enterprise. Inform your enterprise administrators immediately of these types of attacks since they indicate machines that have already been compromised within the enterprise.
- Don't publish the IP address range of the honeynet. There is no need to do this. Hackers and worms are constantly scanning across the Internet for machines to exploit. You honeynet will be found and attacked.
- Don't underestimate the amount of time required to analyze the data collected from the honeynet. This data must be analyzed every day. You will be collecting lots of information and it must be analyzed to provide any benefit.
- Powerful machines are not necessary to establish the honeynet. The Georgia Tech Honeynet did not use state of the art machines and it functioned as intended. Everything we needed to establish our honeynet was already available on campus.

Source: *Know Your Enemy: Honeynets in Universities Deploying a Honeynet at an Academic Institution*

Honeypot vs NIDS

NIDS

- + See all traffic
- — see and need to process ALL TRAFFIC
- + Known and understood by management

Honeypot

- + See only attack traffic
- + Few false positives
- + Require less ressources

Counter Attacks

- General rule, never *hack back*
- Usually not the real source of the attacks
- End up attacking random innocent victims
- Unintended consequences – hacking back medical equipment? SCADA or ICS?
- Ethically not sound

Coordinating Response

- **Definition 27-8** A *computer security incident response team* (CSIRT) is a team established to assist and coordinate responses to a security incident among a defined constituency
- Constituency may be a company, an organization, a sector (academic institutions), or even broader
- Morris internet worm lead to the formation of the Computer Emergency Response Team (CERT/CC) coordination center at Carnegie Mellon University
  `https://en.wikipedia.org/wiki/CERT_Coordination_Center`
- The main danish CERT/CSIRT is `https://www.cert.dk/en` unfortunately it only covers forskningsnettet the National Research and Educational Networks (NREN) in Denmark!
- In Denmark we also had GovCERT, which is now part of Center for Cyber Security (CfCS)
- There is an internet standard document about Incident Response
  Expectations for Computer Security Incident Response `https://www.ietf.org/rfc/rfc2350.txt`

Digital Forensics – Computer Forensics

- **Definition 27-9** *Digital forensics* is the science of identifying and anlyzing entities, states, and state transitions of events that have occurred or are occurring.
-
-
-
-

Exercise

Now lets do the exercise

??

which is number **??** in the exercise PDF.

Exercise

Now lets do the exercise

??

which is number **??** in the exercise PDF.

For Next Time

Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools