

Task 9: Detecting security flaws and vulnerabilities

Goal:

- Be able to identify some common security flaws in your operating systems and network infrastructure
- Understand and apply computer security best practices for preventing various attacks

Recommended reading:

Chapter 22 – *Security* and security sections of Chapter 17 – *DNS*, Chapter 20 – *Electronic Mail* and Chapter 14 – *TCP/IP Networking* of the labs book

Steps:

- 1) Try to find (not exploit!) different kinds of vulnerabilities in the systems of the group with the closest subsequent group number (modulo (number of groups plus 1)) referred later as target group. The focus is on configuration errors, but you could also check for software vulnerabilities and social engineering tricks if you like. Note that you should not break the systems of your colleagues or do any unethical operations. The goal is just to identify possible security flows in their systems and communicate your findings to them. You should at least perform the following checks:
- 2) Use network port scanner tool and identify what services are running on the machines of your target group. Try to identify the version of their operating system and the concrete software that is running on particular port e.g. Postfix or Sendmail on port 25. Save the command that you used to invoke the tool and its output.
- 3) Read up on what is *open DNS resolver* and why it is a bad idea to have your DNS server configured that way. Test if the DNS server of your target group is configured as open DNS resolver. Save the steps you took to verify your findings.
- 4) Read up on what is *open mail relay* and why it is a bad idea to have your mail server configured that way. Test if the mail server of your target group is configured as open mail relay. Save the steps you took to verify your findings.
- 5) Check if the remote logins with the user *root* are enabled on the target group server and gateway machines. Save the steps you took to verify your findings.
- 6) Read up on attacks based on specific ICMP messages – in particular ICMP redirect and ICMP echo request to IP broadcast addresses. Test if the ICMP broadcast is enabled for the network of your target group. If you find an easy way i.e. this is optional, test if ICMP redirect is enabled on any of the target group machines. Save the steps you took to verify your findings.
- 7) Make sure that the vulnerabilities mentioned above are not present on your own systems.
- 8) Compile a report containing all the information from steps 2 – 6 above and all other checks you performed (if any) and vulnerabilities you found. For each one of these steps specify what approach and tools you used to check your target group machines. Include any output and command line parameters used when invoking these tools. Specify your group number and send the report to you lab assistant no later than October 19.

Sample final exam questions:

- 1) How an attacker can use the information provided by a network port scanner tool?

- 2) What is open mail relay?
- 3) What is open DNS resolver?