

# Conception and Implementation of Professional Laboratory Exercises in the field of ICS/SCADA Security

## Part II: Red Teaming and Blue Teaming

Maximilian Richter<sup>1</sup>, Klaus Schwarz<sup>2,3</sup>, Reiner Creutzburg<sup>1,2</sup>

<sup>1</sup>Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany

Email: maximilian.richter@th-brandenburg.de, creutzburg@th-brandenburg.de

<sup>2</sup>SRH Berlin University of Applied Sciences, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany

Email: klaus.schwarz@srh.de, reiner.creutzburg@srh.de

<sup>3</sup>The University of Texas at San Antonio, College of Engineering, 1 UTSA Circle, San Antonio, TX 78249-0669, USA

**Keywords:** open source intelligence, OSINT, cybersecurity, Advanced Google search, RiskIQ PassiveTotal, Censys, Shodan, Maltego, Red Team, Blue Team, cybersecurity training, big data

### Abstract

Industrial control systems are essential for producing goods, generating electricity, maintaining infrastructure, and transporting energy, water, and gas. They form the core of the critical infrastructure of modern industrial nations and are therefore of particular interest. Through the increased interconnectivity of formerly isolated ICS process environments and the use of standard IT technologies such as Ethernet, processes can be optimized and synergies leveraged.

However, ICS/SCADA also becomes the target of the same cyber-attacks as conventional IT systems. It is, therefore, necessary to combine the accumulated knowledge and experience of IT security with the classic Safety-First-mentality of ICS/SCADA-environments in order to avoid significant problems in the foreseeable future.

The new course was created for precisely this purpose. The approach of investigating the security of systems and organizations in Red and Blue Teams has long proven it is worth and is used worldwide.

This second part of the exercises describes the Blue Team action in case of an attack and beyond.

As opposed to Red Teaming, Blue Teaming is an independent group that develops defenses against Red Team activities to improve an organization's effectiveness and security and tests and improves them during a Red Team attack.

The present work aims to impart the interfacing knowledge; in the practical exercises of Blue Teaming, weaknesses of these hybrid infrastructures and systems are identified, and decisions are discussed on how to counteract possible attacks or even prevent them in advance. Throughout the course, students will participate in numerous practical exercises using the tools and techniques that form the basis of decision-making to prevent attacks on infrastructures, such as industrial control systems. A detailed accompanying theory precedes the exercises, and the

course is structured as follows:

#### Introduction

- ICS Cyber Kill Chain
- Types of information gathering

#### Blue Team Tools

- VirusTotal
- Dynamic malware analysis with any.run
- Checksum generation with Linux commands

#### Incident-Response Complex exercise: Part 1

- Preparation
- Detection & Analyses
- Containment

#### Incident-Response Complex exercise: Part 2

- Eradication
- Recovery
- Post Incident Activity

### Complex Exercises – Red Teaming in the ICS/SCADA environment

In this part, students will receive several complex exercises for individual stages of an attack on a target, from reconnaissance to taking over a target system and exfiltration of confidential documents. The goal is to understand the attacker's way of thinking and to know how an attacker proceeds in the individual phases of an attack and which tools are used.

### Accompanying theory

### ICS Cyber Kill Chain

In 2011, employees of the American defense company Lockheed Martin created a model for the classification of the individual phases of a cyber attack [16], which was intended to make decision-making and select the correct defensive reactions more transparent and more efficient. Based on this model, Robert Lee and Michael Assante wrote a document in 2015 describing the Industrial Control System Cyber Kill Chain (ICS) model [5], taking into account the specifics of an ICS environment, such as more stringent filtering of network communications and isolation from the Internet. This model serves to place the individual exercises in the context of a professional attack on companies with ICS infrastructures. The exercises to be performed are classified in the first stage of the kill chain since the complex exercise aims to gain access to a workstation and extract project data successfully.

#### Stage 1 : Cyber Intrusion Preparation and Execution - preparation and execution of a cyber attack

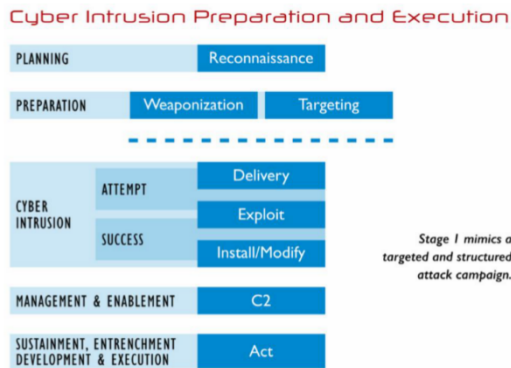


Figure 1. Level 1 of the ICS Cyber Kill Chain (from [5])

This stage of the kill chain aims to gather information about the company regarding the employees in decision-making positions, the IT systems used, and possible weaknesses with a subsequent attack and takeover of the network. In the planning phase (Planning), the target's reconnaissance is carried out to identify employees, IT systems, ICS technologies, and networks. Initially, information is collected from publicly available sources (Open Source Intelligence - OSINT), including a review of the organization's Internet presence, entries in job exchanges, social networks such as Twitter, LinkedIn, Facebook or Xing or targeted search queries with Google, Shodan and other specialized search engines. The advantage of this passive information gathering is that the target does not raise suspicion since many of the techniques used do not trigger warnings with conventional security solutions. Based on the information collected in this way, more targeted network scanning tools such as Nmap can then be used. However, this should be used with caution, especially in the ICS environment, since older devices, in particular, can be damaged by a scan. In the preparation phase, the information gathered is used to plan how the attack will be carried out. Decisive for this can be, for example, the operating systems used, open ports, or blackmailable employees of the target. The decision is also called targeting; to exploit the identified vulnerability is called weaponization. The next phase is the intrusion into the

target's IT infrastructure (cyber intrusion). Once the attack has been launched, ideally, the system is taken over (exploitation), and additional software is installed, and additional user IDs are created to provide a permanent gateway to the target's network. The communication takes place from the taken over system to a command server (Command&Control, short C2-Server). By this kind of connection, establishment firewalls and other security solutions can often be bypassed. In case the attack is detected, the change to an alternative C2-Server is much less expensive than changing the whole infrastructure of the attacker. With a permanent backdoor to the target's infrastructure, the collection of further confidential information and files to implement the second stage of the kill chain begins.

#### Stage 2: ICS Attack Development and Execution - development and deployment of advanced attacks on the ICS infrastructure

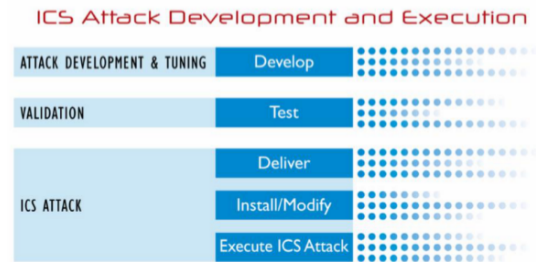


Figure 2. Level 2 of the ICS Cyber Kill Chain (from [5])

For this level, an attacker needs both technical expertise and financial resources. The information collected in the first stage is used to implement a laboratory setup that reflects the target's infrastructure. To prevent detection, the malware developed is tested and improved in this controlled environment. A further consideration is beyond this work's scope, as the following exercises focus on the first stage.

### Types of information retrieval

#### Analysis of network recordings for reconnaissance

Network recordings have a high value for attackers because they contain information about the installed programs and hierarchies without active interaction with the IT systems. This is especially true for ICS systems since the protocols used to send their information unencrypted, and it is recognizable whether the respective system is a master or a slave. After an analysis, actual results are detailed network plans of the ICS infrastructure, including possible master servers, historians or other important ICS components, possible authentication tokens, and control data packages for use in later MITM attacks. Possible tools for analysis are Wireshark and GrassMarlin; their operation is discussed in detail in the following chapter. Use of search engines to discover ICS services on the Internet Errors in the configuration and administration of ICS systems can cause these systems to be accessible from the Internet. Web-based HMI interfaces, in particular, can be found by search engines such as Google or Shodan and thus pose a risk for the entire ICS environment of the person concerned.

## Obtaining information from other public sources

Through their activities on the Internet, companies and their employees disclose information that an attacker can use. Employee entries in social networks such as LinkedIn and Xing reveal possible business partners and technologies used. Furthermore, companies in these networks share new cooperations and projects for advertising purposes. This can provide conclusions about ICS systems and contact persons who are ideal targets for a social engineering attack. Especially dangerous is the insight into these persons' private lives by using their real names in networks like Facebook, Instagram, or Twitter; these profiles provide information about friends and relatives, which can be used as a means of pressure [17]. Detailed advertisements on job boards can provide information about current weaknesses regarding a lack of qualified personnel, hardware and software used in the ICS area, internal team structures, and job titles for convincing phishing mails. The company's website's investigation can also provide IP addresses, email addresses, published publications, and technical information from press releases. One possible tool to facilitate this collection of information is Maltego, the use of which is explained in the following chapter.

## Red Team Tools/Tools

### Note:

In general, the students have to keep in mind that the bold characters of the commands indicate the respective shell, so \$ stands for the hacker VM's standard command line. Students are advised to NOT copy the bold characters when they customize the commands to do the job.

### Nmap

Nmap, short for "Network Mapper," is a free, open-source network scanner that can be used to discover IT systems on networks. The program is available for macOS, Windows, and Linux systems. [18] Possible information includes IP addresses, open/closed ports, assumptions about the operating systems used, whether the device is behind a packet filter. The operation is done either from the command line or via Zenmap, a graphical user interface installed separately. The active scanning of systems provides much important information about used services and programs within a network. However, in ICS networks, unplanned use is not recommended, as the scanning methods used by Nmap can lead to failures and damage to the ICS systems. A passive analysis of the network traffic should first be performed to determine concrete target IPs, and also, the number of scans per second should be reduced to minimize the risk.

### Maltego

According to the manufacturer Paterva, Maltego is an interactive data mining tool for generating graphs [19]. The main application is to collect information from public sources or the support of forensic investigations. A powerful feature is connecting to other sources such as search engine APIs or importing and processing imported data from other forensic tools. In the complex exercise, the operation is limited to using the transformations and the manual entry of information. Objects can be dragged and

dropped from the left bar into the working environment. In order to call up the transformation menu, one only has to right-click on the target object. Figure 3 shows an example mindmap of the TH Brandenburg website with the website object's transformation menu.



Figure 3. User interface of Maltego (source: own screenshot)

### Shodan

According to its statement [20], Shodan is the first search engine for devices connected to the Internet. Researchers can use search filters to find specific manufacturers, types of systems, services, or open ports. Unlike Google, an index of the individual web pages is not created; instead, the service banners and headers are indexed. A banner is a kind of figurehead, which the respective service presents on request. Shodan is exciting for the ICS sector because by filtering by manufacturer name or specific ports of the individual ICS protocols, critical systems can be detected connected to the Internet without planning. The use of Shodan may be prohibited in some countries, and the search results may also include productive devices, so further interaction without prior authorization is not recommended. Figure 4 shows that even a simple search for Siemens HMIs could generate 82 possible hits.

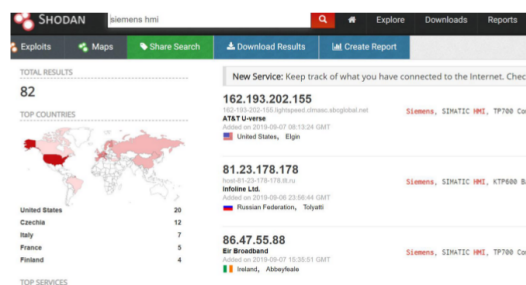


Figure 4. Result of a Shodan search for Siemens Simatic HMIs (Source: own screenshot)

### Google Hacking

Google Hacking is the creative use of the search parameters of the Google search to get exciting results. [21] The advantage

is that the target does not need to be called directly by the attacker, so this approach is more inconspicuous than an active scan with a crawler like Dirbuster. Search queries can include strings displayed in web-based HMI interfaces, error messages indicating vulnerabilities, or types of documents on a specific web page. [21] There is a Google Hacking Database, which provides ready-made examples in regular order to find current vulnerabilities.

### theHarvester

A tool for collecting emails, names, domains, IP addresses, and other information is theHarvester; Christian Martorella of Edge Security Research wrote it. It is free of charge and requires only a Python3 installation to run on all operating systems. By default, the interfaces of various free search engines are used to collect the information, but students can also use other commercial search services by adding valid keys. [24] In figure 5 a part of a scan of the TH-Brandenburg domain is visible. Google was used as a source. Only the first 300 results should be displayed, but this is optional.

```
control@ctp:~$ theharvester -d th-brandenburg.de -b google -l 300
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correct
.....
theHarvester Ver. 3.0.6
  Coded by Christian Martorella
  Edge-Security Research
  cmartorell@edge-security.com
.....
[+] found supported engines
[+] Starting harvesting process for domain: th-brandenburg.de
[+] Searching in Google:
  Searching 0 results...
  Searching 100 results...
  Searching 200 results...
  Searching 300 results...
  Searching 400 results...
  Searching 500 results...
Harvesting results
No IP addresses found

[+] Emails found:
-----
katrin.sens@th-brandenburg.de
info@th-brandenburg.de
upl@th-brandenburg.de
claudia.hoenisch@th-brandenburg.de
dana.voigt@th-brandenburg.de
annegrat.seyerleinklog@th-brandenburg.de
```

Figure 5. Scan of the TH-Brandenburg domain (Source: own screenshot)

### Wireshark

Wireshark is the most used network protocol analysis tool worldwide [25]. It is developed by the Wireshark community and is a free open source software available for Unix/Linux, macOS, and Windows systems. Students can record network traffic and records, mostly in .pcap format, import, and analyze. For many communication protocols, filters and so-called dissectors are available. These serve to break down the data packets into their layers in order to facilitate the analysis. Attackers and defense attorneys use Wireshark and IT administrators to get a better overview of a network. It is operated via the graphical user interface. The input area for display filters can be filtered by protocols, IP addresses, ports, and other characteristics. After a filter has been applied, all corresponding data packets can be seen in the middle. In the lower field, the selected packet is broken

down into its layers. Display filters also affect other statistics; for example, under Statistics-> Protocol Hierarchy, only the filtered packets are included. This is demonstrated in figure 6 for the Modbus/TCP protocol.

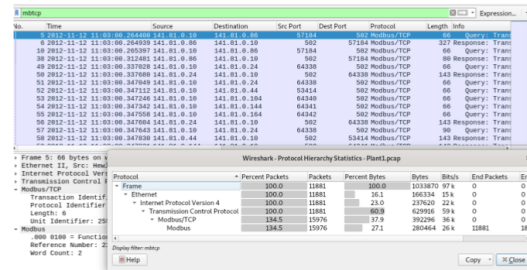


Figure 6. Filtering of Plant1.pcap by Modbus/TCP packets (Source: own screenshot)

Inexperienced operators can click together Display Filters with the Expression Builder, as demonstrated in figure 7.

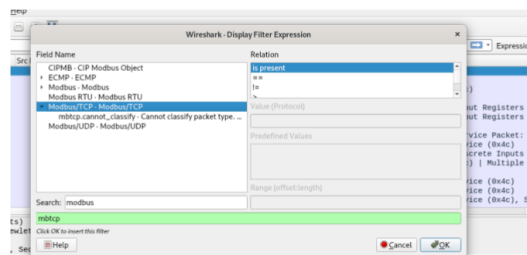
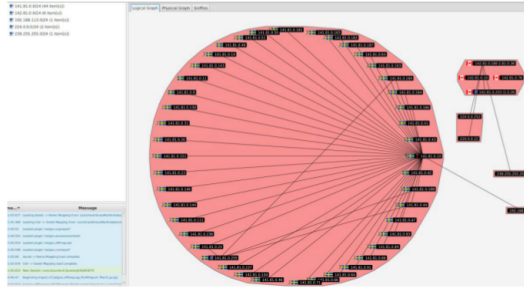


Figure 7. Using the Expression Builder to create a Display Filter for Modbus/TCP (Source: own screenshot)

### GrassMarlin

GrassMarlin is an open-source tool for the graphical representation of networks in the ICS/SCADA area. It was developed by the US National Security Agency (NSA) and can be obtained free of charge from their GitHub; it is available for Linux and Windows systems. [26] GrassMarlin is operated via a graphical user interface, via File->Import Files..., students need to call up the submenu for importing the network recording. With Add Files, the student selects the .pcap file and then selects import Selected to complete the process. Students can see the CIDR notation networks on the left side of the interface, and on the right side, a graphical layout, is situated which enables the student to move around and improve the clarity. With a right-click, the student can open the context menu in the submenu Group. After selecting a filter, the student needs to select Run Layout on All Nodes Now from the context menu to update the graph. Figure 8 shows a filter by the network, including the subnets on the left side.

Another essential function appears in the context menu when the cursor is over an object, View Details for <Name of Object>. Here all recognized information, according to which the filters work, is displayed for this element. This can be very helpful when searching for specific systems like Master Servers or Historians.



**Figure 8.** The GrassMarlin user interface (source: own screenshot)

### Metasploit Framework (MSF)

According to the software's website, the Metasploit Framework (MSF) is the most widely used penetration testing framework. [28] Such a framework can be imagined as a collection of individual tools and exploits that have been given a common user interface and a common database. The Metasploit framework is developed by Rapid7 and is open source and free of charge; only the business support is charged. The general approach is to search for a suitable exploit, enter the target and other required parameters, and then attack the selected payload. Such a scenario is explained within the complex exercise and can be understood by the students. Before starting the MSF, it should be ensured that the PostgreSQL database is started so that automatically obtained information is stored. After a successful exploit, a special shell is provided on the target system, the so-called Meterpreter Shell, which has a Linux-like syntax and is used for interaction. Using a few commands, far-reaching rights can be obtained on the target system, and a permanent backdoor can be set up. [29]

### John the Ripper

John the Ripper is a free, open-source tool for cracking passwords. [30] It is available for Windows, Linux, and macOS and was written by Alexander Peslyak. It is already installed in the hacker VM and is accessed via the Metasploit framework. The operation is explained during the exercise.

### Exercise 1 - Reconnaissance with public sources (OSINT)

The fictitious company eLSFoo was created by the company eLearnSecurity and is used for exercises in their course Penetration Testing Professional, the tasks however were created by the author; only the website and all persons and profiles were created by eLearnSecurity. [18]

### Collecting information with Maltego

#### Tools needed:

- A web browser
- Maltego (already installed in the hacker VM)
- theHarvester (already installed in the hacker VM)
- Accounts for Twitter and LinkedIn to have access to profiles (fake profiles are quite sufficient)

**Scenario:** The order is given to attack the company eLSFoo, but the client has asked to act as inconspicuously as possible and not

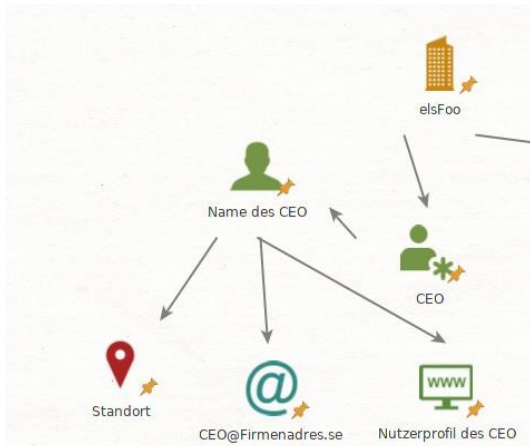
take any steps that would indicate an attack. The starting point is the website [www.elsfoo.com](http://www.elsfoo.com). The task is to use Maltego to create a mind map with the required information and send it to the client. All further information will also be entered manually into the Maltego interface upon receiving. Maltego needs to be started in the Hacker VM by clicking on Activities in the upper left corner and searching for the program. A free user account is required to use the Community Edition (CE). The link for registration can be found after selecting the CE. After successful registration, confirmation on all other windows is needed with the Next button. After that, the setup wizard can be closed. Now an empty graph should be visible; after closing the Run View window in the left menu bar, all available objects will be displayed. After that, a website object needs to be dragged into the desktop, and the text needs to be changed to [www.elsfoo.com](http://www.elsfoo.com), the starting point. Also, a Company object needs to be created and labeled with eLSFoo; after that, an arrow onto the Web page object needs to be dragged in position to represent that the Web page belongs to the company.

#### Tasks:

1. A transformation (right-click on an object) needs to be used to get the IP address belonging to the website. It is advised to take note of the IP address.
2. A transformation needs to be used to find the domain belonging to the website. It is advised to take a note of the found domain.
3. A transformation needs to be used to determine the email addresses belonging to the website. It is advised to take note of the addresses.
4. A transformation on the [elsfoo.com](http://elsfoo.com) domain object needs to be used to display the DNS server names (note: zone transfer). It is advised to take a note of the names.
5. It needs to be checked if all discovered DNS servers belong to the already known IP address, and if not, it is advised to take a note of the other IP address with the corresponding domain.
6. IP address ranges can usually be assigned to a specific region; this can be used to determine the web server's data center location. It needs to be determined using a transformation of the network areas (Netblock), and the location data (city/country) belonging to the found IP addresses. (Note: Routing Info)
7. A transformation needs to be used to display external links on the company website. Which social network can be discovered among the external links? For that reason, a double click on the object is used to search under Properties for possible links, for company profiles, and user accounts. It is advised to list them. After that, the [www.sitemaps.org](http://www.sitemaps.org)-Object and the [www.w3.org](http://www.w3.org)-Object needs to be deleted for better clarity.
8. Information about influential employees is of enormous value for successful social engineering or phishing attacks. The links found and the company website now need to be researched. It is advised to name the Chief Executive Officer (CEO) and the Chief Information Officer (CIO). Are there other C-level members of the company eLSFoo and/or secretaries of the management level? The student is advised to find evidence in the social networks or on the company

website. It is advised to name their roles and, if visible, their names.

- In Maltego, a person object needs to be created for each employee discovered. After that, the information found with that employee needs to be associated. All other information in figure 9 will be collected in later tasks and is only for orientation.



**Figure 9.** Illustration xxx Template for structuring the collected information of an examined person (source of own screenshot)

- While viewing LinkedIn profiles, it needs to be noticed that not all information is available, even if students are logged in. This is because LinkedIn restricts the information displayed when there are no shared contacts.
- The Google search function needs to be used by the student with the option to filter by document type to find possible MS Office documents and PDFs (.docx, .xlsx, .pptx, .pdf).
- Students should now start the hacker VM terminal and analyze the domain elsfoo.com with Google as a data source.

### Find Remote Access through Shodan and Google

#### Tools needed:

- A web browser
- A (free) Shodan account

**Scenario:** During this exercise, students will visit websites that may be used in production or used as honeypots. Students are made aware to DO NOT attempt to log in or use other techniques they have learned. Neither the author nor the TH-Brandenburg or any other entity will take responsibility for possible damages.

#### Tasks:

- A first step to find vulnerabilities for certain ICS/SCADA products is a Google search for security bulletins from manufacturers, security companies, or organizations such as ICS-CERT. Students need to use the following search terms: "Siemens HMI Vulnerability" and "S7-1200 Vulnerability". It is advised to note the name of a Siemens Security Advisory (abbreviation is sufficient).

- Students need to find out which keywords appear on the login page of web-based HMI, and after that can find Internet-connected systems with Google. It is advised to search Google for Simatic HMI Miniweb.
- In a fictitious attack scenario, the next step would be to search for valid access data for the discovered HMI interface. As with regular IT products, it is also common in the ICS/SCADA environment, default user name, password combinations. Unfortunately, these are rarely changed, so lists of these default credentials are usually very effective. Students are advised to find such a list using Google and enter a possible password for Simatic S7 PLCs or a Siemens WinCC HMI.

### Analysis of ICS network recordings with Wireshark

#### Tools needed:

- Wireshark (is already installed in the Hacker-VM)
- Hacker VM
- the exercises folder (found in the hacker VM under /home/control/)

**Scenario:** In the previous exercise, the students have already collected much important information with the help of publicly available sources (OSINT), which can be useful when attacking a target. In this section, the planning phase continues, but with inside information available. The ControlThings Platform provides the analysis file, and the exercises with Wireshark were inspired by one of the tasks from SANS410 [7] but modified by the author to reflect the students' level of knowledge. In this exercise, students will gain temporary access to a facility where ICS systems are part of a social engineering exercise. Students will complete successfully attach a network sniffer and will be able to create and exfiltrate network recordings. Their task is to extract as much information as possible from the collected data to plan further attacks on the ICS infrastructure.

#### Tasks:

- How large is the provided pcap file in the File Browser?
- Now, students need to open the recording with Wireshark for the following tasks. How many packages are in this .pcap file?
- Students are advised to open the overview of the network recording distribution into the individual protocols under Statistics->Protocol Hierarchy. The question is here, Which ICS protocols the student can find.
- Students are advised to note the number of packets for each ICS protocol.
- Which of the IP addresses probably belongs to a master server? Students are advised to keep in mind that in a master-slave setup of the ICS protocols, only the master can initiate connections, and it causes much traffic. Students are now advised to use the IPv4 tab under Statistics->Endpoints and Statistics->Conversations and give a short reason for their answer.
- Students are advised to name the IP addresses of the slaves and assign them to the individual ICS protocols. Students

need to use the display filters of the individual protocols and the IPv4 tab under Statistics->Conversations.

7. Students are now advised to make sure that no display filter is active, and then need to open the Input/Output Graph under Statistics->I/O Graph. A rapid increase and decrease in the amount of bytes transferred can be observed in the middle of the network average. Students are advised to add more graphs using the ICS logs' display filters from the last task. Is one of the ICS logs responsible for this deflection?
8. Students now are advised to open the TCP tab under Statistics -> Endpoints and sort by bytes, what can be found out about the sender with the most bytes? Students are advised to create a graph in the I/O graph with the corresponding port as a display filter. Is this the reason for the traffic spike? What kind of essential system within the OT infrastructure can it be? Name the port and the IP address.

### Analysis of ICS network recordings with GrassMarlin

#### Tools needed:

- GrassMarlin (is already installed in the Hacker-VM)
- Hacker VM
- The exercises folder (found in the hacker VM under /home/control/)

Scenario: The student is advised to continue the analysis of the collected network recordings from the previous exercise. The goal is to get a picture as accurate as possible of the geographical and logical division of the ICS devices into individual subnets.

#### Tasks:

- The student is advised to open GrassMarlin and import the Plant1.pcap file in the home/control/exercises folder/Grassmarlin\_
- If the student encounters any problems, the student is advised to look at the accompanying theory, there the most common bug fixes can be found.
- Students are advised to group by the individual net areas and note them down. If individual countries could be assigned to the net areas, students are advised to write them down.
- Students are now advised to use the grouping by category to identify possible HMI and PLC. Not all PLC devices are necessarily tagged PLC; therefore, students need to check other groups' metadata for recognized ICS protocols.
- GrassMarlin can help to visualize the relationships between known systems quickly. Therefore Students need to use the filter to get an overview of possible masters, slaves, and servers. Students are advised to note down the master and server's IP addresses, due to the number of slaves a quantity is sufficient.

## Complex exercises – Blue Teaming in the ICS/SCADA environment

### Accompanying theory

### Incident Response Process

The Incident Response process is used to handle security incidents and ensures a structured approach to optimize resources. The following figure shows the cyclical nature of the process, so ideally, there will be continuous improvement. Compared to classical IT security, however, there are some changes in ICS/SCADA security, which are explained in the individual phases' descriptions.

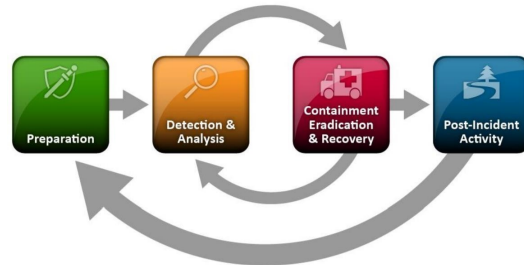


Figure 10. Incident Response Lifecycle according to NIST SP800-61 [31]

#### Preparation (Preparation)

The preparation phase is particularly critical since many decisions are made here that contribute significantly to containing the damage and solving the problem. These decisions include clarifying responsibilities within the organization for individual business units and IT systems, selecting the members of the incident response team (IR team), and the threshold, but one situation is declared a security incident. The IR team needs the full support of the organization's management. In this phase, network plans are updated, systems are upgraded, staff training is provided, checklists and work instructions are created for critical activities, such as creating forensic images or restoring systems from backups [32]. The planning of communication paths away from the company infrastructure in the form of separate smartphones and the establishment of a war room for coordinated work in an emergency are recommended by the American NIST [31]. This can be a dedicated room or a conference room that the IR team can block in an emergency. A unique feature of ICS/SCADA security is proprietary communication protocols and the increased use of legacy systems with insufficient or no security functions. Therefore, the IR team must pay particular attention to establishing accurate baselines of network traffic at the lower levels of the Perdue model and correctly plan and implement the ICS systems' isolation. The ability to distinguish legitimate network traffic from potentially harmful traffic is critical for the next phase [7].

#### Detection & Analysis

In this phase, it is clarified whether a detected event is a security incident. This correct assessment requires an experienced IR team and good preparation. The time frame between the attacker's intrusion and the affected person's detection has improved enormously in recent years. In 2014 the average detection time of data leaks (data breaks) was 205 days; in 2018, this number could be reduced to 78 days (see [33], [34]). When reviewing information, it is important to recognize possible connections and ensure that the investigation does not alter possible

evidence at an early stage. Therefore, the creation of forensic copies and complete documentation of activities is necessary. Of great value is the use of the ticket system of the IT helpdesk, the information gained from this can help determine the time frame and narrow down the affected user groups. Many attacks on the ICS/SCADA area start as regular cyber-attacks to secure access to the control level. Therefore, affected organizations need to view detected IT security incidents from the perspective that they are only the first step in a larger attack. Critical infrastructure operators are significantly affected as they are increasingly becoming the target of such attacks as cyberwar activities expand globally. Especially the activities of state actors in sabotage and industrial espionage have increased in recent years [34].

Containment, Eradication & Recovery

The analysis results are incorporated into decisions regarding the elimination of malware, the containment of damage, and the recovery of systems and processes. Additional information is collected and fed back into the analysis process to close the incident. The goal of containment is to stabilize systems and processes. This can be achieved by temporarily isolating the affected network or systems. Further activities include changing local passwords on the systems and physically securing the affected server and office rooms, and IT systems. For example, affected client systems of employees should be recovered and forensically secured as quickly as possible. IP addresses that are suspected to be C2 servers should be blocked at least temporarily (blacklisting). An advantage of ICS networks is the possibility to block all unknown connections (whitelisting) for the duration of the investigation; thus, even data leaks not initially detected can be prevented. [7] Eradication aims to identify and eliminate the causes of the problem. [35] The risk of inadequate analysis can mean that not all attacker backdoors can be found, and subsequently restored systems can be directly reinfected. Detected samples of the malware can be examined both statically and dynamically. The static malware analysis examines the binary without executing it, while the dynamic analysis sets up an isolated test environment to study the behavior when it is run. After removing the detected malware and cleaning the systems, a vulnerability analysis should be performed, for example, with a scanner like Nessus 8. This way, it can be determined whether the vulnerability has been closed successfully and whether there might be others. For ICS systems and networks, it is essential to use these scans in a very targeted manner, as the network scans can cause damage the devices. During the recovery, it is essential not to restore any infected system states. Therefore it is essential to have an isolated backup system that checks the data during the backup. Alternatively, an installation with the original installation disks and a new installation of all updates can be carried out, but this process can be very time-consuming, so a backup is preferable. After the systems have been restored, they should be monitored for a certain period to prevent incomplete removal and re-infection.

Post Incident-Activity (Follow-up of the security incident)

After a security incident has been dealt with, a report must be prepared, firstly for management and possibly third parties in-

involved, and secondly in the event of a police investigation or insurance. This report is compiled from information gathered during a Lessons Learned Meeting. The following list contains several questions that should be clarified in this meeting (according to NIST800-61 [31]):

- What happened when?
- What information should have been known earlier?
- Which activities were unnecessary or not useful?
- What can be improved so that such an attack cannot occur in the future?

The identified improvement potentials flow into the preparation phase and thus ensure a continuous improvement process.

**Blue Team Tools/Tools**

**VirusTotal**

VirusTotal is an Internet service for scanning links, files, or hash values for malware, using "over 70 antivirus scanners and URL/domain blacklisting services" [36]. The service was purchased by Google in 20129 and is free for non-commercial use.

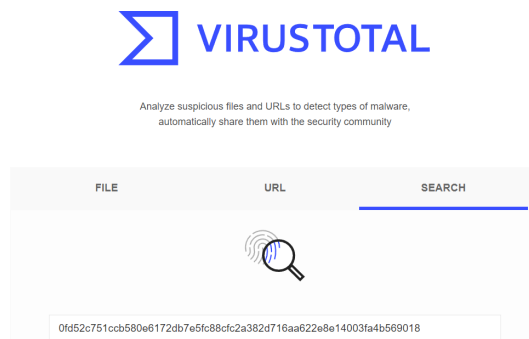


Figure 11. Search mask of VirusTotal (Source: own screenshot)

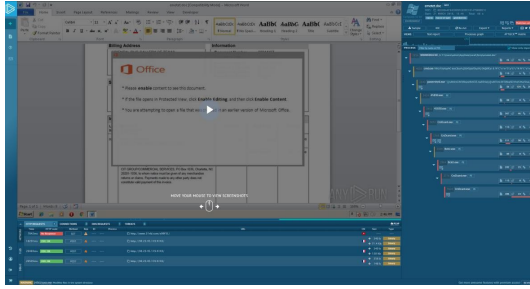
The operation is via the website or the programming interface, but only the regular web interface is needed for the following exercise. When uploading files, please note that they are shared with Google and the cooperating IT security service providers, so uploading confidential documents is not recommended. This risk can be circumvented by using a suspicious file to generate the hash value and inserts it into the VirusTotal search mask. An example of such a search is shown in figure 11.

**Dynamic malware analysis with Any.Run**

For dynamic analysis of malware, the student usually needs a lab environment, and must make sure that the VM used to execute the malware is isolated from the Internet. However, providers of analysis VMs can be accessed via the browser, where students only pay for their own hosted environment. The Any.Run service offers such an interactive online malware analysis service, and there is also a limited free version, which is sufficient for student purposes. [37] The student can either upload a file or search for a hash value to check if an analysis has already been performed. Search engines can find these analyses like Google.

Figure 12 shows the user interface; the window shows individual screenshots of the desktop during the malware execution,



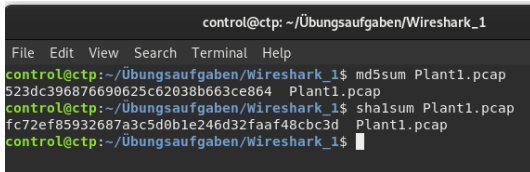


**Figure 12.** The graphical user interface of Any.Run (source: own screenshot)

which helps for a first assessment. In the lower half of the interface, divided into several tabs, there is different information regarding network communication to double-click on individual entries to open a detailed view. In the right half of the user interface, the student can find the individual processes with their children in a hierarchical structure, especially PowerShell processes can often find network connections to C2 servers.

### Checksum generation with Linux commands

Hash values or also checksums are used for integrity checks. Functions are applied which calculate a value from a file. If another hash value is generated from this file with the same procedure, one must assume that it has been changed. This check is used for data transfer or backup systems. Another use case is, however, necessary for IT security. By generating and exchanging hash values of detected malware, the risk of accidental infection can be reduced. The same applies to checking confidential data on portals such as VirusTotal or Any.Run. Figure 13 shows the generated MD5 and SHA1 checksums of the file Plant1.pcap.



**Figure 13.** Example of checksum generation in the command-line (source: own screenshot)

### Incident-Response Complex Exercise: Part 1

**Scenario:** In a fictional scenario, students are advised to be a member of the global ICS security team of a large pharmaceutical company. The group has production sites, offices, and research facilities worldwide. Students are appointed to the Incident Response Team to contribute their professional expertise in the ICS/SCADA area.

#### Tasks:

1. Their task is now to check the current (simplified) network plan of their site and to correct any deviations from the distribution specified by the Perdue model. To do this, draw lines to reposition the elements and note the changes in key points.

2. The students were advised to briefly describe the Control System DMZ's primary task and how this task is performed.

Control System DMZ's primary task is to control the data flows between the business and control zones. This separation is enforced using a two-firewall solution, one between the DMZ and the business zone and the other between the DMZ and the control zone. Unidirectional gateways are another way to control the data streams, as they use data diodes at the hardware level to prevent the backflow of data.

3. The supervisor has asked the students to procure and install a hazardous gas measurement device within the production areas, isolating the device from the rest of the ICS infrastructure. What type of system is this? (Note: the exact term is being searched for) It is a Safety Integrated System (SIS), or more precisely, a Safety Monitoring System.

#### Explanation:

Safety Instrumented Systems (SIS) are devices and systems that monitor specific parameters and intervene if deviations are too large to prevent man and machine damage. These systems are usually isolated from the rest of the ICS infrastructure to minimize the chances of failure. Deviations are detected by the safety monitoring systems, including leakage warning devices, fire detectors, radiation meters, or gas detectors.

### Detection & Analysis

#### Tools needed:

- Search engine of the students choice

#### Scenario:

The CSO (Chief Security Officer) has called an emergency meeting. A recent security assessment has revealed suspicious looking traffic, the following facts are currently known:

Outgoing IP (belongs to the company network):	192.168.123.123
Target IP:	132.148.9.244
Port:	TCP443
Further information:	Traffic occurs from Monday to Friday, between 02:00 and 10:00 CEST

1. The student is advised to consider suspects about the times and whether it can be made an initial guess about the country of origin of the attack. The time frame looks like a regular working week, where the times coincide with regular office hours in a time zone that is +6 or +7 before CEST, including countries like China or North Korea.
2. What kind of traffic is it, could the content of the communication be read by simply recording it? (Note: Port)
3. What kind of malware could generate this traffic
  - (a) Virus
  - (b) Worm
  - (c) Remote Access Trojan (RAT)
  - (d) Ransomware

## Containment

### Scenario:

While checking the IP address, students discover that this is used company-wide to assign IP addresses dynamically, several host systems have been identified that communicate with the malicious site. These systems are located in different locations worldwide.

1. How could these systems have been infected with the malware?
  - (a) (Spear)Phishing Mail to senior staff
  - (b) USB stick by a single inside perpetrator
  - (c) Watering Hole attack through the website of a local canteen
2. Which of the following actions should be taken to contain the damage? (multiple answers are possible)
  - (a) Blacklisting of the target IP
  - (b) Moving the affected systems into the analysis
  - (c) Formatting of the affected systems
  - (d) Implementation of a Lessons Learned Meeting

### Incident Response Complex Exercise: Part 2

#### Tools needed:

- The Hacker VM
- A Terminal (Available in the Hacker VM)
- A Browser (for VirusTotal and any.run)

#### Scenario:

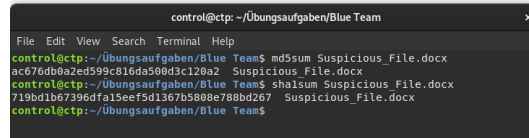
Based on the latest findings, the fictional student based IR team has decided to declare the current events a security incident, but at this point, security authorities' involvement is not considered necessary. The responsible IT departments at the respective branch offices have moved in the infected host systems and equipped the employees with replacement devices. Within a few hours, the suspicious traffic will again be generated by the new devices. In a fictitious scenario, the student is instructed to imagine that during an investigation by the IT security team, phishing emails specifically tailored to three affected individuals were discovered in their email inboxes with a Microsoft Word document attached. The affected file will be provided to the student in the process.

#### Tasks:

1. As it cannot be excluded initially, the file is not an important internal document, a direct upload to services like VirusTotal is not recommended. To avoid a possible loss of data, decide to create a hash value of the suspicious file before the check and use it to start the analysis.
2. Students are advised to create the MD5 and SHA-1 hash value from the file Suspicious.File.docx. The file can be found on the hacker VM in the folder /home/control/exercise tasks/Blue Team.

Figure 14 shows the output of a checksum generation:

#### ATTENTION:



```
control@ctp: ~/Übungsaufgaben/Blue Team
File Edit View Search Terminal Help
control@ctp:~/Übungsaufgaben/Blue Team$ md5sum Suspicious.File.docx
ac676db0a2ed599c816da50d3c120a2 Suspicious.File.docx
control@ctp:~/Übungsaufgaben/Blue Team$ sha1sum Suspicious.File.docx
719bd1b67396dfa15ee75d1367b5880e788bd267 Suspicious.File.docx
control@ctp:~/Übungsaufgaben/Blue Team$
```

**Figure 14.** Output of the checksum generation of the suspicious file (Source: own screenshot)

The sample given is real malware; students are advised not to call any domain they find during their investigation.

3. Students are advised to examine the MD5 checksum provided by VirusTotal and answer the following questions:
  - What type of document is it? It is a Word document.
  - What is the name of the author of the document?
  - What is the name of the Word document? (.doc)
  - How big is the file?
  - Which domain(s) were contacted, what could they be?
  - Are there any executable files (.exe) suspected concerning this sample?
4. Students are now advised to search the MD5 value on Google to find any.run VM where the malware they are looking for has been executed.
5. Which domains are being accessed, and what are the corresponding IP addresses?
6. Students are now advised to find out which Microsoft program they see in the graphical representation of the executed malware.
7. What process was used to call the domains?
8. What kind of malware is it?
9. What is the IP address of the C2 server? If the IP can be assigned to one of the detected domains, the domain should be noted.
10. What kind of malware is it?
11. **BONUS:** What is the name of the malware?
12. What is the IP address of the C2 server?

### Recovery

**Scenario:** In a fictional scenario, the students' team has successfully replaced the affected systems, and no further communication attempts to the detected C2 server were detected. Investigations have not yet identified any infected devices within the control zone. However, since it is malware that Windows systems can reproduce itself very aggressively within networks, caution is advised.

#### Tasks:

1. Many engineering workstations use Windows operating systems as a basis, why is this particularly critical?
2. What can make the system recovery work much more comfortable?
  - Backups
  - Original Installation Disks
  - Packet Filter
  - Antivirus program

## Post Incident Activity

**Scenario:** In a fictive szenario the student is advised to imagine that the IR Team has successfully recovered the affected systems, and the monitoring systems no longer report any suspicious traffic. The student and his IR team declare the security incident closed. This time the cyberattack was detected early enough and could not spread into the control zone.

### Tasks:

1. In a fictional szenario, the student is advised to specify, what type of attacker poses the greatest threat to a company in terms of industrial espionage.
  - State Actors (APT)
  - Script Kiddies
  - Terrorist Organizations
  - Petty criminals

## Evaluation

The Open Source intelligence course created in this thesis has already been evaluated in several practical sessions with 20 test persons. The result is predominantly positive feedback; the participants thoroughly enjoyed the topic and the exercises' structure. The exact structure and sequence of the exercises are also convincing. The participants further stated that the exercises' extent and the available teaching material are appropriate to the requirements. All participants also praise the high practical part of the exercises. During the evaluation, the course always included all 11 practical exercises. On 14 training dates, a total of 64 contact hours of teaching were provided in 2 weeks (see Table in Appendix).

## Summary and Outlook

The complex exercises in the area of Red Teaming in ICS/SCADA environments gave the students a practical understanding of the ICS Cyber Kill Chain's theoretical steps. They put themselves in the attacker's role, spied out their target, checked for vulnerabilities, and finally carried out a successful cyber attack. They can now detect suspicious activities in networks and public spaces and have learned how dangerous entries in social media can be. Furthermore, the vulnerability of Windows in ICS environments was practically demonstrated, and within a few commands, the system could be taken over by the critical HMI software. The Blue Teaming exercises provided a hands-on examination of each stage of security incident handling, requiring both organizational and analytical skills as decisions had to be made and pattern recognition was required. Furthermore, there was a short digression into malware analysis, both static with VirusTotal and dynamic with Any.Run. The exercises showed that the ICS/SCADA area faces similar problems as IT did 20 years ago. Insufficiently secure protocols and outdated devices and operating systems pose a significant danger to operators. However, the findings of IT security can be used as a basis for securing ICS systems. It can be assumed that the networking of ICS/SCADA systems will continue to increase; the BSI comes to a similar conclusion in its Management Report on IT Security 2018. Mainly due to the implementation of Industry 4.0, the importance of effective defense against cyber attacks will continue to increase. The market for security solutions for ICS infrastructures is already being

tapped by renowned providers such as Kaspersky [12] or Checkpoint [13]. Efforts are underway to develop secure communication protocols in the ICS environment; a current example would be the IEC6235114 standard within the energy sector. A survey conducted by the SANS Institute [15] in 2019 showed that almost 40% of the companies surveyed expect their ICS/SCADA systems to be highly threatened by cyber attacks, while a further 12% even assume a very high threat. The human factor (62%) is considered by far the most significant risk factor. [38]. This shows that a rethinking in the minds of the affected employees must occur since it is usually not the inside perpetrator in the foreground but the improper networking and operation of the ICS systems. Further possibilities to deepen the ICS/SCADA security knowledge gained in this thesis would be the participation in the SANS ICS410: ICS/SCADA Security Essentials course and the study of further reading within the ControlThings-Platform.

## References

- [1] A. Berg and T. Haldenwang, "Bitkom: Wirtschaftsschutz in der Industrie," 13. September 2018. <https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf> (last access February 22, 2021)
- [2] N. Falliere, L. O Murchu and E. Chien, "W32.Stuxnet Dossier," Februar 2011. [https://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf) (last access February 22, 2021)
- [3] BSI, "Die Lage der IT-Sicherheit in Deutschland 2014," 15. Dezember 2014. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?blob=publicationFile> (last access February 22, 2021)
- [4] BSI, "Die Lage der IT-Sicherheit in Deutschland 2018," 2018. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?blob=publicationFile&v=6> (last access February 22, 2021)
- [5] M. Assante and R. Lee, "SANS Institute: The Industrial Control System Cyber Kill Chain," Oktober 2015. <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297> (last access February 22, 2021)
- [6] NIST, "National Institute of Standards and Technology Special Publication 800-82r2 Guide to Industrial Control System (ICS) Security," Mai 2015. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf> (last access February 22, 2021)
- [7] J. Searle, "Kurs: SANS ICS410: ICS/SCADA Security Essentials," SANS, 2018
- [8] E. Knapp, "Industrial Network Security - Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", Syngress, 2011, ISBN: 978-1-59749-645-2
- [9] P. Ackerman, "Industrial Cybersecurity - Efficiently secure critical infrastructure systems", Packt Publishing, 2017, ISBN: 978-1-78839-515-1
- [10] DHS, "Department of Homeland Security Recommended Practice: Improving Industrial Control Sys-

- tem Cybersecurity with Defense-in-Depth Strategies,” September 2016. [https://www.us-cert.gov/sites/default/files/recommended\\_practices/NCCIC\\_ICS-CERT\\_Defense\\_in\\_Depth\\_2016\\_S508C.pdf](https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf) (last access February 22, 2021)
- [11] T. Wiens, “S7 Communication (S7comm),” 13. Mai 2016. <https://wiki.wireshark.org/S7comm> (last access February 22, 2021)
- [12] EU, “Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern,” 08 Dezember 2008. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32008L0114> (last access February 22, 2021)
- [13] K. Fowler, “Data Breach Preparation and Response: Breaches are Certain, Impact is Not”, Syngress, 2016, ISBN: 978-0-12-803451-4
- [14] C. Bodungen, B. Singer and e. al, “Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions”, McGraw-Hill Education, 2017, ISBN: 978-1-25-958972-0 (E-Book)
- [15] J. Searle, “ControlThings I/O,” <https://www.controlthings.io/home> (last access February 22, 2021)
- [16] Velocio, “Produktbeschreibung: Velocio Ace PLC,” <http://velocio.net/ace/> (last access February 22, 2021)
- [17] E. Hutchins, M. Cloppert and R. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain,” <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf> (last access February 22, 2021)
- [18] eLearn-Security, “Kurs: PTPv5 Penetration Testing Professional,” 2018
- [19] Nmap-Community, “Nmap Overview and Introduction,” <https://nmap.org/> (last access February 22, 2021)
- [20] Maltego, “Maltego CE,” <https://www.paterva.com/buy/maltego-clients/maltego-ce.php> (last access February 22, 2021)
- [21] Shodan, “What is Shodan?” <https://help.shodan.io/the-basics/what-is-shodan> (last access February 22, 2021)
- [22] J. Long, “The Google Hacker’s Guide: Understanding and Defending Against the Google Hacker,” <http://pdf.textfiles.com/security/googlehackers.pdf> (last access February 22, 2021)
- [23] OTW, “SCADA Hacking: Finding Vulnerable SCADA Systems using Google Hacking,” (September 08, 2019). <https://www.hackers-arise.com/single-post/2016/07/05/SCADA-Hacking-Finding-Vulnerable-SCADA-Systems-using-Google-Hacking> (last access February 22, 2021)
- [24] GoogleGuide, “Search Operators,” [http://www.googleguide.com/advanced\\_operators\\_reference.html](http://www.googleguide.com/advanced_operators_reference.html) (last access February 22, 2021)
- [25] C. Martorella, “Github Page: theHarvester,” <https://github.com/laramies/theHarvester> (last access February 22, 2021)
- [26] Wireshark, “About Wireshark,” <https://www.wireshark.org> (last access February 22, 2021)
- [27] NSA, “National Security Agency: GRASSMARLIN User Guide Version 3.2,” <https://github.com/iadgov/GRASSMARLIN/raw/master/GRASSMARLIN%20User%20Guide.pdf> (last access February 22, 2021)
- [28] Rapid7, “Metasploit - Getting Started,” <https://metasploit.help.rapid7.com/docs> (last access February 22, 2021)
- [29] D. Kennedy, J. O’Gorman, D. Kearns and M. Aharoni, “Metasploit: The Penetration Tester’s Guide”, No Starch Press, 2011, ISBN: 978-1-59327-288-3
- [30] A. Peslyak, “John the Ripper password cracker,” <https://www.openwall.com/john/> (last access February 22, 2021)
- [31] “Simpsons Meme,” <https://imgur.com/a/WSFVBma> (last access February 22, 2021)
- [32] NIST, “National Institute of Standards and Technology Special Publication 800-61r2: Computer Security Incident Handling Guide,” August 2012. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (last access February 22, 2021)
- [33] R. Lee, “Kurs: SANS ICS515: ICS Active Defense and Incident Response,” SANS, 2018
- [34] Mandiant, “M-Trends 2015: A View from the Frontlines,” 2015. <https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf> (last access February 22, 2021)
- [35] FireEye, “M-Trends 2019: FireEye Mandiant Services Special Report,” 2019. <https://content.fireeye.com/m-trends> (last access February 22, 2021)
- [36] K. A. Monnappa, “Learning Malware Analysis - Explore the concepts, tools, and techniques to analyze and investigate Windows malware”, Packt Publishing, 2018, ISBN: 978-1-78839-250-1.
- [37] VirusTotal, “How it works,” <https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works> (last access February 22, 2021)
- [38] Any.RUN, “What is ANY.RUN,” <https://app.any.run/docs/> (last access February 22, 2021)
- [39] B. Filkins and D. Wylie, “SANS 2019 State of OT/ICS Cybersecurity Survey,” Juni 2019. [https://radiflow.com/wp-content/uploads/2019/06/Survey\\_ICS-2019\\_Radiflow.pdf](https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf) (last access February 22, 2021)
- [40] BSI, “Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2019,” 01 Januar 2019. [https://www.allianz-fuer-cybersicherheit.de/ACS/DE/./downloads/BSI-CS\\_005.pdf?blob=publicationFile](https://www.allianz-fuer-cybersicherheit.de/ACS/DE/./downloads/BSI-CS_005.pdf?blob=publicationFile) (last access February 22, 2021)
- [41] P. Kobes, Leitfaden Industrial Security - IEC 62443 einfach erklärt, VDE Verlag GmbH, 2016, ISBN: 978-3-8007-4166-3 (E-Book)
- [42] J. Luttgens and M. Pepe, Incident Response & Computer Forensics, Third Edition, McGraw-Hill Education, 2014, ISBN: 978-0-07-179868-6
- [43] OTW, “SCADA Hacking: Finding SCADA Systems using Shodan,” 30. Juni 2016. <https://www.hackers-arise.com/single-post/2016/06/30/Hacking-SCADA-Finding-SCADA-Systems-using-Shodan>. (last access February 22, 2021)
- [44] A. Soullie and A. Torrents, “Brucon 0x07 ICS Workshop: Pentesting ICS 101”, Oktober 2015.
- [45] D. Vukadinovic, “Was ist der Unterschied zwischen HTTP und HTTPS?,” 26. Juni 2018. <https://www.globalsign.com>

[com/de-de/blog/unterschied-zwischen-http-und-https/](https://www.infund.com.ar/data/servicios/Automation.jpg)  
(last access February 22, 2021)

- [46] “Stock Image einer HMI”. <http://www.infund.com.ar/data/servicios/Automation.jpg> (last access February 22, 2021)
- [47] Schwarz, Klaus; Franziska Schwarz, Reiner Creutzburg: “Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT)”. Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020, <https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-278>
- [48] Schwarz, Klaus; Reiner Creutzburg: “Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 1: RiskIQ PassiveTotal”. Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
- [49] Schwarz, Klaus; Reiner Creutzburg: “Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 2: Censys”. Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
- [50] Schwarz, Klaus; Reiner Creutzburg: “Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego”. Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
- [51] Schwarz, Klaus; Reiner Creutzburg: “Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego”. Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)
- [52] Schwarz, Klaus: “Conception and Implementation of Professional Laboratory Exercises in the Field of Open Source Intelligence (OSINT) for use in English and German Training Market for Security Authorities”. Master Thesis, Technische Hochschule Brandenburg, Department of Computing and Media, April 2020
- [53] Kant, Daniel; Reiner Creutzburg: ‘Investigation of risks for Critical Infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan’. Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020 <https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253>
- [54] Pilgermann, Michael; Thomas Bocklisch; Reiner Creutzburg: “Conception and implementation of a course for professional training and education in the field of IoT and smart home security”. Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms

& Applications Conference (MOBMU) 2020 <https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-277>

## Author Biography

*Maximilian Richter received his M.Sc. degree in Computer Science from Technische Hochschule Brandenburg (Germany) in 2020. His research interests include IIoT/OT Security, Active Defense, Threat Intelligence and Cyber War. He currently works as a SOC Analyst in the financial sector.*

*Klaus Schwarz received his B. Sc. and M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017 and 2020, respectively. His research interests include IoT and Smart Home Security, OSINT, Mechatronics, Sensorics, Embedded Systems, Artificial Intelligence, and Cloud Security. As a faculty member, he is developing a graduate program in Applied Mechatronic Systems with focus on Artificial Intelligence at SRH Berlin University of Applied Sciences.*

*Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019 he is a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.*

**JOIN US AT THE NEXT EI!**

IS&T International Symposium on

# Electronic Imaging

SCIENCE AND TECHNOLOGY

*Imaging across applications . . . Where industry and academia meet!*



- **SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •**
- **INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •**

[www.electronicimaging.org](http://www.electronicimaging.org)

