Certificate of Advanced Studies

Linux Cyber Security

Organizations today are increasingly turning to Linux as a platform of choice for large enterprise infrastructure and small embedded systems. The network connectivity of Linux systems exposes them to hostile and malicious cyber attacks. The CAS Linux Cyber Security (LCS) teaches students the internals of Linux, how to harden Linux systems, and various types of attacks targeting Linux servers. The CAS LCS completes with a module on Linux forensics in the event of compromise or abuse.

Berner
Fachhochschule

Table of Contents

1 Environment

Organizations today are increasingly turning to Linux as a platform of choice for many organizations, product manufacturers, and service providers. Linux is being used for large supercomputers and clusters, for cloud and virtualization infrastructure, and for backend storage and database servers. Linux is used for Internet facing services, firewalls, and edge computing. In addition to scalable enterprise infrastructure, Linux is also used in small embedded devices and industrial control systems. Linux end-user distributions are also becoming attractive as desktop environments.

The network connectivity of Linux systems exposes them to hostile and malicious cyber attacks. The CAS LCS teaches students the internals of Linux, how to harden Linux systems, and various types of hacking attacks targeting Linux servers. The CAS LCS completes with a module on Linux forensics in the event of compromise or abuse.

2 Target audience

The CAS LCS is designed for IT and Cybersecurity professionals wanting to specialize in Linux systems and Linux Cyber security.

3 Career opportunities

The CAS LCS program will prepare students for career opportunities in a variety of organizations:

- Finance industry – Linux based payment systems and banking platforms
- Large enterprises using Linux – IT/Cyber security and CTI teams
- Product manufacturers and developers using Linux
- Firms with Linux based industrial control systems
- Consultancy firms with a focus on cyber security, needing Linux security experts
- Private boutique (specialized) security firms focused on Linux
- Companies with Linux based big data and artificial intelligence systems

4 Education goals

This continuing education program has practical learning objectives. Students completing the CAS-LCS will have deep understanding of how Linux works and how Linux can be hacked. Students will have the skills to securely harden Linux systems and perform digital forensics in the event of an incident.

5 Admission Requirements

Admission into the CAS LCS requires one of the following:

- a university degree or equivalent professional education degree in computer science, computer engineering, or related field

- professional experience in Cybersecurity, threat intelligence, digital forensics or IT investigation, and a related industry certification.

If applicant qualifications are unclear or inconclusive, further information (for example, a CV) or an interview may be requested.

6 Language, location, and contact

Modules are conducted in one-week fulltime periods and taught in English. Some modules may have pre-reading recommendations. Module assignments and exams are completed by the end of the week.

The location of taught classes is the Switzerland Innovation Park, Aarbergstrasse 46, in Biel/Bienne. More information can be found here: https://www.bfh.ch/en/about-bfh/locations-facilities/locations/biel-aarbergstrasse-46/

Some modules allow remote attendance, however, onsite attendance is strongly recommended (better teaching experience, building friendships with your student colleagues and teachers).

Please see the schedule for the latest dates and onsite availability.

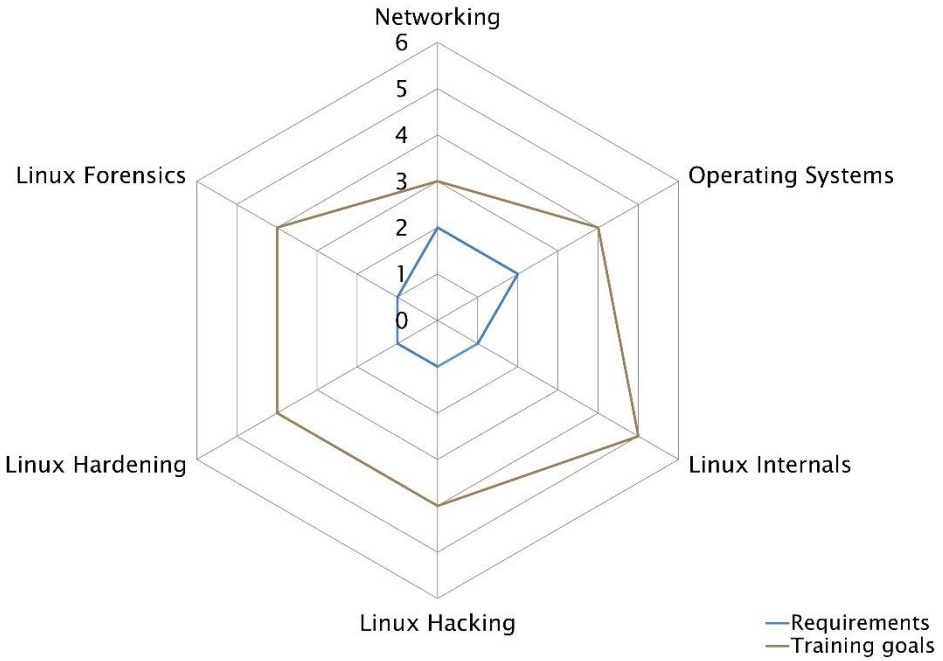
Contact with the administration can be made by post, telephone, or e-mail:

Postal address:
Bern University of Applied Sciences
School of Engineering and Computer Science
Continuing Education
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel/Bienne

Telephone: +41 31 848 31 11

E-mail: weiterbildung.ti@bfh.ch

7 Skills profile



Skill levels

1. Proficiency/knowledge
2. Comprehension
3. Application
4. Analysis
5. Synthesis
6. Appraisal

8 Course outline

Course / Teaching unit	Lessons	Hours	Lecturers
Linux Internals	40		Peter Eggimann
Linux Hacking	40		Ben Fehrenson
Linux Hardening	40		Andreas Mühlemann
Linux Forensics	40		Bruce Nikkel
Total	**160**		

The CAS comprises a total of 12 ECTS credits. For the individual courses, time for self-study, exam preparation, etc. must be taken into account as needed.

The student may choose an elective that is of interest from the list provided.

Please see the schedule for the latest dates and onsite availability.

9 Course descriptions

The individual modules that make up the CAS LCS program are described below. Some of the modules are shared with the MAS DFCI and CAS CTI programs. A module may include a variety of teaching methods such as lectures, seminars, case studies, practical labs, assignments, etc. To complete the CAS LCS students must successfully complete all four modules.

9.1 Linux Internals

Educational objectives	This module teaches the internals of Linux from a security perspective
Topics and content	– History and motivation for creating Linux – Linux kernel architecture, distributions, and desktops – Boot process: loaders, kernel and initramfs, systemd init – The shell, programs and daemons, systemd management, d-bus – Disks, partitions, and file systems – Linux Networking – Containers (cgroups, namespaces, docker, etc) – System administration
Course materials	Provided in Moodle

9.2 Linux Hacking

Educational objectives	This module teaches various methods and tools used to hack into Linux systems
Topics and content	– Vulnerability scanning, target reconnaissance – Penetration testing, ethical hacking, and red-team exercises – Denial of service attacks against Linux – Network stack abuse – Internet facing service exploitation – Privilege escalation – Kernel compromise (kernel modules, eBPF) – OWASP
Course materials	Provided in Moodle

9.3 Linux Hardening

Educational objectives	This module teaches students how to harden Linux systems to protect against cyber attacks using defensive configuration and secure system setup
Topics and content	– Security models: DAC, MAC, users/groups – Linux security features: SELinux, Apparmor – Stripping down: systemd, network listeners, daemons, d-bus activation – Defensive kernel settings and networking configuration, firewalling – Secure remote access, login process, privilege escalation – File system permissions, ACLs – Containers and process isolation – Encrypted files systems, use of TPM – Secure disposal of decommissioned Linux systems
Course materials	Provided in Moodle

9.4 Linux Forensics

Educational objectives	This module covers the forensic acquisition and analysis of Linux systems, including forensic readiness, triage of live systems, and dead-disk forensics
Modules available	– Linux forensic readiness and incident response – Live analysis/triage of running Linux systems – Dead-disk forensics, forensic acquisition – Filesystem forensic analysis – Reconstructing system boot and initialization – Examination of installed software packages – Identifying network configuration artifacts – Log and journal analysis – Forensic aspects of time and location – Reconstructing user activity, desktops, and attached peripherals
Course materials	Provided in Moodle

10 Proof of proficiency

To gain the 12 ECTS credits, students must demonstrate proficiency by successfully completing all coursework (examinations, project work), in accordance with the following list:

Proof of proficiency	Weighting	Type of qualification	Student pass rate
Linux Internals	2.5	Final exam	0 – 100 %
Linux Hacking	2.5	Final exam	0 – 100 %
Linux Hardening	2.5	Final exam	0 – 100 %
Linux Forensics	2.5	Final exam	0 – 100 %
Total weighting / Pass rate	10		0-100%
ECTS grade			**A – F**

Each student can achieve a pass rate of 0 to 100% for each proof of proficiency. The weighted sum of the pass rates per topic and the weighting of the topic results in an overall pass rate between 0 and 100%.

The overall pass rate is converted into an ECTS grade A to E, as defined in the study regulations. An overall pass rate below 50% is awarded a grade F, “unsatisfactory”.

11 Organisation

CAS supervisor:
Prof. Dr. Bruce Nikkel
E-mail: bruce.nikkel@bfh.ch
Threema: DC2JN4YK
Mobile: +41 79 255 6316

CAS administration:
Miriam Patwa
Phone: +41 31 848 58 68
E-Mail: miriam.patwa@bfh.ch

Note: Changes may be made to content, learning objectives, lecturers and required proficiency levels. The lecturers and the Head of Studies are authorized to make adjustments to a CAS on the basis of current developments in a subject area, the specific previous knowledge and interests of the students, or for didactic and organizational reasons.

Bern University of Applied Sciences
School of Engineering and Computer Science
Continuing Education
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel/Bienne

Tel. +41 31 848 31 11
E-Mail: weiterbildung.ti@bfh.ch

bfh.ch/ti/weiterbildung
bfh.ch/cas-lcs