Ethical Hacking

...and how to not get kicked out of LiU

LINKÖPINGS UNIVERSITET

#whoarewe

Linköping University Incident Response Team (LiU IRT)

David Byers
Head of IT infrastructure

Information security lead @ LiU
PhD in software security

Christopher Gilmore-Ellis
Team member

Incident responder
Penetration tester
Microsoft master

Karl-Johan Karlsson
Team member

MSc in Digital Forensics
Automation engineer
Open-source savant

The Rules

Using IT resources

LiU:s IT-resurser får användas till sådant som inte bryter mot svensk lag, mot ingångna avtal, eller mot universitetets policy och regelverk, inklusive dessa regler.

Det är inte tillåtet att dölja, eller försöka dölja, sin egen eller någon annans identitet vid användning av LiU:s IT-resurser gentemot LiU utom i de fall det är uttryckligen tillåtet. Användning av VPN-tjänster och anonymiseringsnätverk är tillåtet.

Det är inte tillåtet att använda LiU:s IT-resurser för att förtala, förolämpa, förnedra eller kränka andra.

Du får inte använda IT-resurserna på ett sätt som stör andra användare, till exempel genom att förbruka en för stor del av tillgänglig kapacitet.

Du får inte göra LiU:s IT-resurser tillgängliga för någon utanför LiU utan skriftligt medgivande från IT-direktören.

LiU:s IT-resurser får inte användas för affärsverksamhet utan skriftligt medgivande från IT-direktören.

Användare av LiU:s IT-resurser är skyldiga att följa anvisningar från IT-direktören, IT-säkerhetsgruppen och systemadministratörer med ansvar för resurserna.

- Don’t break the law, rules, policies, or agreements
- Don’t hide your identity from LiU
- Don’t use our stuff to be an ***hole
- Don’t mess things up for others
- Don’t share our stuff with your friends and family
- Don’t run your business using our stuff
- Follow instructions from security people

Authorisation and security

Behörigheter till nät och andra IT-resurser är personliga och får inte upplåtas till någon annan.

Lösenord ska hållas hemliga och väljas så att de är svårgissade. Ingen från LiU kommer att kontakta dig och begära dina inloggningsuppgifter.

Du får inte uppge ditt lösenord till någon annan. Det är inte tillåtet att begära att någon annan ska uppge sitt lösenord.

Det är inte tillåtet att använda annan användares inloggningsuppgifter oavsett om denne själv lämnat ut inloggningsuppgifterna eller inte.

Du förväntas agera på ett säkert sätt. Skydda din utrustning och dina och andras uppgifter. Om du agerar på ett sätt som leder till säkerhetsproblem kan din tillgång till IT-resurser tillfälligt spärras för att underlätta avhjälpning av problemet.

Om du ansluter privat utrustning till LiU:s nätverk så måste du underhålla den så att den inte utgör ett hot mot LiU:s IT-säkerhet. Till exempel ska operativsystem och all programvara hållas uppdaterad, och datorn ska ha ett uppdaterat skydd mot skadlig programvara.

- Don’t let anyone else use your access
- Use strong passwords everywhere
- Don’t tell anyone your password or ask theirs
- Don’t use anyone else’s identity
- Act securely and protect your stuff
- Keep your stuff secure and updated

Keeping your stuff secure

Do

Regularly update your system

Run *good* antimalware software

Use an ad blocker and a content blocker

Use a password manager

Use multi-factor authentication

Change file associations on Windows

Create a separate admin account

Enable virtualisation-based security (Windows)

Don’t

Don’t download stuff from dodgy sites

Don’t install a residential proxy or free vpn

Don’t run malicious or deceptive software

Don’t enable macros in Office

Don’t ignore warnings from your operating system

Don’t always have administrator privileges

Don’t allow privilege elevation without authentication

Don’t experiment with malware on a normal system

Authorisation and security (continued)

Det är inte tillåtet att försöka skaffa sig högre behörigheter i LiU:s IT-system än man har rätt till. Det är inte heller tillåtet att använda LiU:s IT-resurser i syfte att skaffa sig behörigheter man inte har rätt till i andra system.

Om du upptäcker svagheter, fel eller störningar som kan påverka säkerhet eller tillförlitlighet i LiU:s IT-system, eller om du upptäcker att någon bryter mot dessa regler, ska du anmäla detta till LiU:s IT-säkerhetsgrupp (IRT).

Don’t try to hack our stuff*

Don’t use our stuff to hack anyone else*

Tell us about vulnerabilities you find

You guys are no fun at all

Reporting vulnerabilities

Do

Check security.txt before doing anything at all

Figure out who you should send the report to

Be clear, concise, and provide details

Use a secure and reasonably anonymous address

Be patient and understanding

Keep records of your communication

Don’t

Don’t use what you find for personal gain

Don’t report trivial stuff as if it was critical

Don’t be pushy or obnoxious

Don’t be oblivious law, politics, and policy

Don’t make a public disclosure too soon

Don’t access information you don’t have to

E-mail

Du förväntas regelbundet kontrollera epost till din studentmailadress.

Det är inte tillåtet att, utan skriftligt tillstånd från IT-direktören, göra massutskick, skicka reklam, enkäter eller liknande via epost till personer som inte samtyckt på förhand.

Check your mail!

Don’t be a spammer

Monitoring

För att LiU ska kunna fullgöra sina skyldigheter gentemot sina avtalspartners, studenter, medarbetare och samhället i stort övervakas LiU:s IT-resurser i viss utsträckning.

Systemadministratörer har rätt att övervaka system och nätverk, inklusive ta del av nätverkstrafik och lagrade data, för att säkerställa en tillförlitlig drift och godtagbar säkerhetsnivå i LiU:s IT-system.

Systemadministratörer har rätt att rensa i brevlådor, lagringsutrymmen och liknande om de missköts eller är inaktiva, efter att ha informerat berörd individ.

Systemadministratörer har rätt att tillfälligt stänga av IT-resurser vid akut driftssituation eller grundad misstanke om lagbrott.

IT-direktören och IT-säkerhetsgruppen har rätt att utestänga enskilda personer från användning av IT-resurser vid grundad misstanke om brott mot LiU:s regelverk.

We have to monitor our systems

We can and do monitor them

System administrators can do stuff to your stuff

System administrators can kick you off

Security people can do even more

Getting in to trouble

Om du bryter mot de här reglerna kan din tillgång till LiU:s IT-resurser begränsas. Begränsningen upphör normalt när du försäkrar att du inte längre bryter mot reglerna. Vid upprepade brott mot reglerna kan begränsningen kvarstå under en längre period, som bestäms av IT-direktören. I samband med sådan åtgärd delges information om möjligheter att överklaga eller få begränsningen lättad eller hävd.

Misstänkta lagbrott kan komma att polisanmälas.

If you break these rules, your access to LiU's IT resources may be restricted. The restriction normally ends when you assure that you are no longer breaking the rules. In case of repeated violations of the rules, the restriction may remain for a longer period, which is determined by the IT director. In connection with such action, information is shared about opportunities to appeal or to have the restriction eased or lifted.

Suspected violations of the law may be reported to the police.

How much trouble can I really get in to

TSIT 14: Digital Forensics and Incident Response

www.liu.se

LINKÖPINGS UNIVERSITET