ITS NW security

Weekly plans

UCL University college

Contact:
Morten Bo Nielsen <mbni@ucl.dk>

2022–05–27

UCL Erhvervsakademi og Professionshøjskole
Niels Bohrs Allé 1 . 5230 Odense M
Tlf. 6318 3000 . ucl.dk

Contents

List of Figures

1 Introduction

This document is a collection of weekly plans. It is based on the weekly plans in the administrative repository, and is updated automatically on change.

The sections describe the goals and program for each week of the second semester project.

2 Uge 6

Dette er første session. Så vi kommer til at bruge en del tid på at lære hinanden og faget at kende.

2.1 Mål for ugen

Practical and learning goals for the period is as follows

2.1.1 Praktiske mål

- Ingen

2.1.2 Læringsmål

- Den studerende ved hvad faget går ud på
- Den studerende kender til OSI modellen og strujtureret fejlfinding
- MON kender niveauet

2.2 Leverancer

- Diskussion på klassen

2.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

2.3.1 Mandag

Tidsplanen:

Time	Activity
8:15	MON introducerer faget
9:00	Vi snakker fagligt niveau
10:00	MON introducerer OSI modellen
10:40	MON introducerer fejlfinding
11:15	Gennemgang af lektier til næste gang
11:30	Vi slutter

2.4 Kommentarer

- Links om OSI modellen se her[1] og video her[2]

2.5 struktureret fejlfinding

- Root cause analysis
  - Fejlen er tydelig et sted, og så skal man følge kæden af data flow og processer tilbage til hvor den virkelige fejl er.
  - og dokumenterer undervejs
- YOLO
  - spreghagl, og når det virker igen så stopper man
  - uden at man kan reproducere eller ved hvad der var galt

2.6 Lektier til næste gang

Opgave 1+2

[1] https://www.comparitech.com/net-admin/osi-model-explained/
[2] https://www.youtube.com/watch?v=vv4y_uOneC0

3 Week 7

Vi skal snakke om hardware i dag.

3.1 Goals of the week(s)

Practical and learning goals for the period is as follows

3.1.1 Praktiske mål

None

3.1.2 Læringsmål

- Den studerende kan forklare OSI modellen og de tilhørende lag
- Den studerende kan placere hardware på de forskellige lag i OSI modellen.
- Den studerende kan benchmarke båndbredde
- Den studerende kan forklare konceptet “bottlenecks” og dets relevans i IT sikkerhed

3.2 Deliverables

None

3.3 Schedule

Below is the tentative schedule, which may be changed depending on input from the students.

3.3.1 Mandag

Tidsplanen:

Time	Activity
8:15	Dagens plan

Time	Activity
8:30	Lektier: OSI. 15 min i grupper, 15 min på klassen
9:00	Lektier: Fejlfinding. 15 min i grupper, 15 min på klassen
9:45	MON gennemgår CIA og flaskehalse
10:30	Speed tests og iperf
11:15	Lektier til næste gang
11:30	Vi slutter

Gennemgang af lektier:

- Der laves mindre grupper, hvor I sammenligner det som I har lavet
- Vi tager de bedste eksempler på klassen.

3.4 Kommentarer

3.4.1 CIA links

- deepwatch[3]
- forcepoint[4]
- comptia security+ youtube[5]

Og det skal sammen holdes med data at rest, in transit og in process.

3.4.2 Bottlenecks

- Start altid ved
  - Netværk
  - CPU
  - RAM
  - Disk I/O
- Der er altid en flaskehals et sted, ellers ville alting gå uendeligt hurtigt
- Kan man udnytte en flaskehals, er der potentiale for et denial-of-service angreb

[3] https://www.deepwatch.com/blog/cia-in-cybersecurity/
[4] https://www.forcepoint.com/cyber-edu/cia-triad
[5] https://www.youtube.com/watch?v=y3goanmMj3s

  - DDOS fra Cloudflare - https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/ (Vendor site!)

- vi vender tilbage til dette når vi snakker monitorering
- Tænk i at data flyder mellem processeringsenheder (som vi snakkede om i sidste uge), og at der på vejen er begrænsninger.

3.5 Lektier til næste gang

Opgave 1+2+3

4 Week 8

Netværk er en vigtig del af netværks- og kommunikations sikkerhed. I denne uge ser vi på hvordan man organiserer sig fysisk og logisk med netværk.

Subnets er en praktisk og sikkerhedsmæssig indeling af netværket.

4.1 Goals of the week(s)

Pratical and learning goals for the period is as follows

4.1.1 Praktisk mål

- Den studerende har vmware workstation kørende, og har en Kali live

4.1.2 Læringsmål

- Den studerende kan forklare fordele og ulemper ved forskellige topologier
- Den studerende kan forklare segmentering, og dets relation til sikkerhed og netværksperformance
- Den studerende kender til hvordan netværksenheder bruges

4.2 Leverancer

Ingen

4.3 Schedule

Below is the tentative schedule, which may be changed depending on input from the students.

4.3.1 Mandag

Tidsplanen:

Time	Activity
8:15	Lektier: Hardware specs
8:45	Lektier: Båndbredde check
9:30	segmentering og subnets
10:45	vmware og kali
11:15	lektier til næste gang
11:30	Frokost

4.4 Kommentarer

- Online companion til dagen er her[6]
- Baggrundsmateriale om IP adresser kan finder her[7]

4.5 Lektier til næste gang

- installer vmware[8]
- installer kali live[9]
- sæt en router op[10]
  - og brug wireshark/tcpdump til at checke indkomne vs. outgoing ip pakker.

[6] https://moozer.gitlab.io/course-networking-security/02_segmentation/
[7] https://moozer.gitlab.io/course-networking-basisc/03_IP/
[8] https://moozer.gitlab.io/course-networking-security/Bonus/install_vmware/
[9] https://moozer.gitlab.io/course-networking-security/Bonus/kali_on_vmware/
[10] https://moozer.gitlab.io/course-networking-basisc/05_more_routing/setup/#importing-router-1h

5 Uge 9

Sidste uge snakkede vi om netværks topologi og hvordan man strukturere sit netværk for at få redundans og (lidt) sikkerhed.

Denne uge ser vi på hvordan man rent praktisk indretter sig med IP adresser, routere og VLANs.

5.1 Mål for ugen

Pratical and learning goals for the period is as follows

5.1.1 Praktiske mål

- Den studerende har en minimal Debian headless server og en openbsd router.

5.1.2 Læringsmål

- Den studerende kan designe et netværk ud fra simple specifikationer
- Den studerende kan designe et IP layout for et simpelt netværk
- Den studerende kan forklare forskellene på fysiske og virtuelle enheder (interfaces, servere, LANs)
- Den studerende kan forklare hvad netflow er og hvad det kan bruges til

5.2 Leverancer

Ingen

5.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

5.3.1 Mandag

Tidsplanen:

Time	Activity
8:15	Lektier: vmware, router, kali og virtuelle maskiner generelt
9:15	Ip layouts og netbox
10:15	netflow og ntop
11:15	lektier til næste gang
11:30	Frokost

5.4 Kommentarer

- Online companion til dagen er her[11]

5.5 Lektier til næste gang

- IPAM
  a. papir+blyant øvelse.
     Lav en IP subnet oversigt over dine device og de tilhørende interne og eksterne netværk
  b. Set netbox op og dokumentér dit netværk
     Jeg hjælper gerne.
     Gå evt. i gruppe med en diplomer for de har nok eet halvstort netværk. . .
  c. Se på det IPAM dokumentation som firmaet allerede har, og forhold dig til det.
- Set up netflow[12]

6 Uge 10

Dagen emne er netværkstrafik og hvordan man analyserer det. Data skal samles op og vi ser på lidt tools til at arbejde med det.

Det forventes at den studerende har en grundlæggende forståelse for forskellige netværksprotokoller på forhånd, såsom DNS og HTTP.

[11] https://moozer.gitlab.io/course-networking-security/03_network_layer/
[12] https://moozer.gitlab.io/course-networking-security/03_network_layer/netflow/#netflow-using-ntopng

6.1 Mål for ugen

Pratical and learning goals for the period is as follows

6.1.1 Praktiske mål

Ingen.

6.1.2 Læringsmål

- Den studerende kan forklare TLS
- Den studerende kan bruge relevante analyse værktøjer til at undersøge netværkstrafikken.

6.2 Leverancer

Ingen

6.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

6.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier: IPAM
8:45	Lektier: netflow
9:15	pause :-)
9:30	om at sniffe trafik
10:00	TLS, kryptering og den slags
10.30	pause
10:45	tcpdump og wireshark - på klassen
11:30	Frokost
12:15	netflow, wireshark and pcaps

Tidspunkt	Aktivitet
13:30	lektier til næste gang
13:45	the end

6.4 Kommentarer

- Online companion til dagen er her[13]
- wirehark intro[14]
- wireshark test pakker[15]
- tcpdump BPF examples[16]

6.5 Lektier til næste gang

1. Protokoller
    1. Find to-tre protokoller fra wiresharks eksempler som du genkende
    2. Forstå hvad der foregår, evt. vha. google
    3. Tag noter, og vis det næste gang
2. Lokal net/firma net
    1. Start wireshark og saml noget data op
    2. Gem PCAPS
    3. Se på det: er der ukendte protokoller? ukendte ip adresser? andet interessant?
    4. Dyk ned i 2-3 streams, og forstå hvad der foregår.
    5. Tag noter, og vis det næste gang
3. Lav SSL dump opgaven herfra[17]

[13] https://moozer.gitlab.io/course-networking-security/04_packets/
[14] https://www.varonis.com/blog/how-to-use-wireshark
[15] https://wiki.wireshark.org/SampleCaptures
[16] https://hackertarget.com/tcpdump-examples/
[17] https://moozer.gitlab.io/course-networking-security/04_packets/tls_protocol/

7 Uge 11

Monitorering er en hjørnesten i al sikkerhed. Vi ønsker at have så meget synlighed i vores netværk som muligt, for at opdage anomalier - og for at fikse ting i driften som er forkerte.

Der er meget overlap mellem drift og sikkerhed, se f.eks. denne artikel[18].

7.1 Mål for ugen

Pratical and learning goals for the period is as follows

7.1.1 Praktiske mål

- Den studerende har en monitoreringsserver kørende med grafana, prometheus mv.

7.1.2 Læringsmål

- Den studerende kan forklare de tre forskellige typer af monitorering
- Den studerende kan forklare hvilke data der er tilgængelige fra hvilke typer enheder
- Den studerende kan udføre simpel fejlfinding ud fra monitorering

7.2 Leverancer

Ingen

7.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

7.3.1 Mandag

Tidsplanen:

[18] https://medium.com/anton-on-security/stealing-more-sre-ideas-for-your-soc-e2fe6836fe9a

Tidspunkt	Aktivitet
8:15	Lektier: wireshark protokoller
8:45	Lektier: wireshark sniffing og analyse
9:15	Lektier: ssldump
9:45	a quick primer on monitoring
10:15	Pause så kan kan checke teknikken
10:30	Ekstern gæst (online) om hvordan grafana & friends bliver brugt
11:45	Frokost/MON er til møde
12:35	More monitoring
13:30	lektier til næste gang
13:45	the end

7.4 Kommentarer

- Online companion til dagen er her[19]

7.5 Lektier til næste gang

- lav opgaven her[20]

8 Uge 12

Der er meget at snakke om når vi snakker web og DNS. Privacy, confidentiality og integrity blandt andet.

8.1 Mål for ugen

Practical and learning goals for the period is as follows

8.1.1 Praktiske mål

Ingen

[19] https://moozer.gitlab.io/course-networking-security/05_monitoring/
[20] https://moozer.gitlab.io/course-networking-security/05_monitoring/software/

8.1.2 Læringsmål

- Den studerende kan forklare DNS og issues i forbindelse med CIA
- Den studerende kan forklare design elementer i almindelig web server setups
- Den studerende kan udføre passive dns opslag og forklare relevansen.

8.2 Leverancer

Ingen

8.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

8.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier: grafana, prometheus og loki
9:30	DNS gennemgang
10:30	Passive DNS highlight
11:30	Frokost/MON er til møde
12:15	APIs, WAF, proxy, http/s
13:30	lektier til næste gang
13:45	the end

8.4 Kommentarer

- DNS oversigt. se her[21]
- DNS er meget problematisk på forskellige måder
  - see f.eks. her[22] fra uncensoreddns.org.

[21] https://moozer.gitlab.io/course-networking-basisc/06_domain_name_system/
[22] https://blog.uncensoreddns.org/blog/39-the-unfriendly-internet-turning-off-cleartext-lookups-in-se

  - Skal it afdelingen bestemme over DNS? paul vixie[23]. Spoiler: han er sur.
  - Mere DNS kryptering (https://www.youtube.com/watch?v=pjin3nv8jAo)
    * DNS over TLS, DNS over HTTPS
  - encrypted dns fra cloudflare[24]. Note: vendor link
  - Er centralisering af dns servere en god ting? 8.8.8.8, 1.1.1.1 og de andre store
  - data in transit, confidentiality, integrity?

- Passive DNS. Farsight[25] er dem jeg kender
  - Vi ville have brugt dnsscout som eksempel, men booo[26]
  - En video[27] om det
  - Måske er [security trails(https://securitytrails.com/corp/api)] relevant Hvor kommer data fra, og hvad kan det bruges til?

- API
  - hvis du selv laver dem så brug swagger[28] (official example site[29])
  - Mandatory OWASP link[30] - som I nok har set før?
  - Design
    * Web application firewall - WAF:
      · cloudflare[31] (vendor link)
      · nginx har ACL'ere[32] og en paid WAF.
      · Et eksempel på modsecurity[33].
      · Denne[34] ser interessant ud.
      · Og lidt mere[35]
      · Disclaimer: Jeg er ikke hård til WAF'er.
    * reverse proxies[36] - vendor link
      · Load balancing,
      · ssl offloading, ACME/let's encrypt

[23] https://www.youtube.com/watch?v=ZxTdEEuyxHU
[24] https://blog.cloudflare.com/dns-encryption-explained/
[25] https://www.farsightsecurity.com/
[26] https://www.farsightsecurity.com/dnsdb-community-edition/
[27] https://info.farsightsecurity.com/hubfs/DNSDB%2020%20Flexible%20Search.mp4
[28] https://swagger.io/
[29] https://petstore.swagger.io/
[30] https://owasp.org/www-project-top-ten/
[31] https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application-firewall-waf/
[32] https://docs.nginx.com/nginx/admin-guide/security-controls/controlling-access-proxied-tcp/
[33] https://www.netnea.com/cms/apache-tutorial-7_including-modsecurity-core-rules/#step_4_triggering_alarms_for_testing_purposes
[34] https://coreruleset.org/documentation/
[35] https://www.feistyduck.com/library/modsecurity-handbook-free/online/index.html
[36] https://www.cloudflare.com/en-gb/learning/cdn/glossary/reverse-proxy/

        * web cache, e.g. varnish[37]
    - hvor krypterer vi?
        * data in transit, integritcy confidentiality

- Disclaimer om cloudflare.
    - De er store, og laver mange gode ting, inkl. teknisk dokumentation.
    - De er også et kommercielt firma som leverer netværksydelser, så et passende niveau af kildekritik er på sin plads.
    - Deres dokumentation plejer at være meget sober sammenlignet med andre virksomheder.

8.5 Lektier til næste gang

- opret en konto på security trail, free tier, og se hvad den siger om domæner du interesserer dig for
    - ucl.dk har f.eks. 255 underdomæner

9 Uge 13

Vi er ca. halvvejs, så denne og næste uge vil være en form for recap.

Denne og næste uge tager vi trappen fra lag 1 til applikations laget, og snakker CIA.

9.1 Mål for ugen

Practical and learning goals for the period is as follows

9.1.1 Praktiske mål

Ingen

[37] https://varnish-cache.org/

9.1.2 Læringsmål

- Den studerende kan forklare sikkerhed på lag 1 og 2, vha. CIA.
- Den studerende kan beskrive almindelige angreb på lag 1 og 2.

9.2 Leverancer

Ingen

9.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

9.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier: securitytrail
9:30	Sikkerhed og problemer på lag 1-2
10:30	MACsec og 802.1x
11:30	Frokost
12:15	wireless, måske demo, måske kun snak
13:15	lektier til næste gang
13:30	the end

9.4 Kommentarer

- Sikkerhed på lag 1-2
- 802.1x
  - "den sædvanelige" som man bruger til Network Access Control (NAC)
  - Man connecter til en port, logger ind, og bliver tildelt et vlan
  - Dette burde bare virke som klient med windows, mac, linux mv.

    - linux guide[38]
  - Authentication modes from juniper[39]
    - Obs: Der er flere modes og fall back til enheder som ikke kan 802.1x
  - Lidt fra VMware[40]

- IEEE 802.1AE (MACsec)
  - Krypteret trafik mellem L2 enheder.
  - From juniper[41]
  - from zindagitech[42]
  - Quick intro from phil anderson[43]
  - I am so not an expert in this

- Angreb
  - DHCP, 802.1x, VLAN, MAC spoof, mv
  - ettercap[44] er en gammel kending. Der er også en Fun with ettercap[45]
  - Mht. Wireless ville jeg starte ved aircrack-ng[46]. Og en guide[47], og en demo[48]

Det kan være forstyrrende, socialt uacceptabelt, brud på den lokale IT politik, og måske kriminelt at lege med denne slags. Slå hjernen til.

9.5 Lektier til næste gang

- Leg med ettercap
  - Genskab “Fun with ettercap” DNS delen
  - er det nemt? svært?
  - hvordan beskytter man sig imod det?

[38] https://www.uio.no/english/services/it/network/student-residential-network/instructions/nm/
[39] https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/802-1x-authentication-switching-devices.html
[40] https://www.vmware.com/topics/glossary/content/network-access-control.html
[41] https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/understanding_media_access_control_security_qfx_ex.html
[42] https://zindagitech.com/what-is-ieee-802-1ae-macsec-how-does-it-work/
[43] https://www.youtube.com/watch?v=u-nisjfHhtQ
[44] https://www.ettercap-project.org/
[45] https://pentestmag.com/article-fun-ettercap/
[46] https://www.aircrack-ng.org/
[47] https://nooblinux.com/crack-wpa-wpa2-wifi-passwords-using-aircrack-ng-kali-linux/
[48] https://www.youtube.com/watch?v=uKZb3D-PHS0

- Leg med aircrack
  - Aflyst dit eget netværk derhjemme eller sæt et op til lejligheden.
  - er det nemt? svært?
  - hvordan beskytter man sig imod det?

10 Uge 14

Denne og sidste er en form for halvvejs recap, hvor vi går ISO modellen igennem og snakker CIA.

10.1 Mål for ugen

Practical and learning goals for the period is as follows

10.1.1 Praktiske mål

Ingen

10.1.2 Læringsmål

- Den studerende kan forklare sikkerhed på lag 3 og 4, vha. CIA.
- Den studerende kan beskrive almindelige angreb på lag 3 og 4.

10.2 Leverancer

Ingen

10.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

10.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier: ettercap og aircrack
9:30	Tunneller - sikkerhed og design tanker
10:30	BGP, TCP/UDP issues
11:30	Frokost
12:15	Firewall regler - demo og diskussion
13:15	lektier til næste gang
13:30	the end

10.4 Kommentarer

- Sikkerhed på lag 3-5
- På lag 3 har vi forskellige tunneler
  - ikke krypterede e.g. gre, 4in6, 6in4. See RFC2003[49] for the general idea.
  - krypterede, aka. VPN, såsom wireguard[50], openvpn[51], PPTP, L2TP/IPSec, [SSTP] (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/70adc1df-c4fe-4b02-8872-f1d8b9ad806a#:~:text=SSTP%20is%20a%20mechanism%20t
    (VPN over HTTPS - why not?)
- BGP[52] issues
  - "Accidental reroute" from US to china[53] and from Europe to China[54]
  - Facebook outage in 2021[55]
- Connection hijacking[56]. It is a variation on MITM.
  - More from tutorialspoint[57]
- UDP amplification attacks

[49] https://datatracker.ietf.org/doc/html/rfc2003
[50] https://www.wireguard.com/
[51] https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn
[52] https://www.juniper.net/documentation/us/en/software/junos/bgp/topics/topic-map/bgp-overview.html#:~:text=BGP%20is%20an%20exterior%20gateway,complete%20route%20to%20each%20destination.
[53] https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet
[54] https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-th
[55] https://www.techtarget.com/searchnetworking/feature/3-lessons-from-the-2021-Facebook-outage-for-ne
[56] https://www.greycampus.com/opencampus/ethical-hacking/network-or-tcp-session-hijacking
[57] https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tcp_ip_hijacking.htm

  - Since UDP is connectionless, this is a real problem, see e.g. uncensoreddns blog[58] on why they stop unencrypted DNS.
  - From cloud flare, DNS[59] and NTP[60]

- Firewall rules
  - pf on openbsd[61]
  - iptables on linux[62]
  -
  - Some Juniper[63] devices can do “selective stateless”.

10.5 Lektier til næste gang

- Det er påske. Lad os sige at vi reviewer hvad vi har lavet so far.
  - Kig ugerne igennem.
  - Formuler et spørgsmål per uge
  - Fremhæv en ting per uge som er cool, interessant, eller som på anden vis kan fremhæves.

11 Uge 17

Vi får besøg fra crowdsec[64] idag

11.1 Mål for ugen

Practical and learning goals for the period is as follows

11.1.1 Praktiske mål

Ingen

[58] https://blog.uncensoreddns.org/blog/39-the-unfriendly-internet-turning-off-cleartext-lookups-in-se
[59] https://www.cloudflare.com/en-gb/learning/ddos/dns-amplification-ddos-attack/
[60] https://www.cloudflare.com/en-gb/learning/ddos/ntp-amplification-ddos-attack/
[61] https://www.openbsd.org/faq/pf/example1.html
[62] https://www.cyberciti.biz/tips/linux-iptables-examples.html
[63] https://www.juniper.net/documentation/us/en/software/junos/flow-packet-processing/topics/topic-map/security-packet-based-forwarding.html#:~:text=An%20SRX%20device%20operate%20in,on%20a%20per%2Dpacket%20basis.
[64] https://crowdsec.net/

11.1.2 Læringsmål

- Den studerende kan forklare formålet med dynamisk opdaterede firewalls, eg. vha. crowdsec
- Den studerende kan starte virtuelle maskiner i skyen

11.2 Leverancer

Ingen

11.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

11.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier: gennemgang af tidligere uger Spørgsmål, udeståender og highlights
10:00	Crowdsec kommer
12:00	Frokost
12:45	Intro til Digital ocean og cloud
13:15	lektier til næste gang
13:30	the end

11.4 Kommentarer

- Online companion til dagen er her[65]

11.5 Lektier til næste gang

- Spin up en DO cloud server

[65] https://moozer.gitlab.io/course-networking-security/06_internet/

  - Se øvelsen her[66]
  - Husk at slukke for den igen.

12 Uge 18

Vi vil dykke mere ned i certifikater og hvordan man tænker når de skal bruges.

12.1 Mål for ugen

Practical and learning goals for the period is as follows

12.1.1 Praktiske mål

Ingen

12.1.2 Læringsmål

- Den studerende kan forklare hvad PKI er og hvad det bruges til
- Den studerende kan oprette og bruge certifikater
- Den studerende kan forklare konceptet ssl interception og hvordan det implementeres

12.2 Leverancer

Ingen

12.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

[66] https://moozer.gitlab.io/course-networking-security/06_internet/exposed_server/

12.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier: DO spinup, auth logs
9:15	Certificates 101
10:00	MDAM om praktik
10:30	Easy-rsa
11:15	Frokost
12:00	NGFW og mitmproxy
13:15	lektier til næste gang
13:30	the end

12.4 Kommentarer

- Links to come.
- Basic certifikat koncepter:
  - x509, private key, certificate, signing requests, revocation, self-signed, certificate chains, PKI
  - openssl tool
- Easy-rsa[67] demo
- mitmproxy[68]. Installation script is here[69]

12.5 Lektier til næste gang

- Test easy-rsa
  1. Opret en easy-rsa pki
  2. Opret en ny vm med en webserver
  3. Opret et certifikat til webserveren
  4. tilføj certifikatet til webserveren
  5. check at det virker vha. browser og/eller curl

[67] https://easy-rsa.readthedocs.io/en/latest/
[68] https://mitmproxy.org/
[69] https://gitlab.com/-/snippets/2309755

13 Uge 19

I denne uge vil vi snakke om hvordan angribere arbejder, når de kompromiterer et netværk, og hvordan vi kan gøre det sværere for dem vha. segmentering.

13.1 Mål for ugen

Practical and learning goals for the period is as follows

13.1.1 Praktiske mål

Ingen

13.1.2 Læringsmål

- Den studerende kan forklare og bruge netværkssegmentering i design fasen
- Den studerende kan forklare almindelige sikkerhedstiltag på netværksniveau (L1-L4)
- Den studerende kan forklare brugen MITRE att&ck framework

Se også uge 8

13.2 Leverancer

Ingen

13.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

13.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier: PKI and web server
9:15	The cyber kill chain
10:00	Lateral movement
11:15	Frokost
12:00	MITRE att&ck.
13:15	lektier til næste gang
13:30	the end

13.4 Kommentarer

- Cyber kill chain
  - jeg har altid fundet den som værende meget militært inspireret
  - by csoonline[70]
  - by computer.org[71]
  - video by the ciso perspective[72]
- Lateral move
  - lateral movement fra trend micro[73]
  - Common techniques[74]
  - Crowdstrike's take on it[75] - Reklameagtig, men har nogle gode tanker.
  - Lateral move on MITRE tactics[76]
  - CIS 20 CSC (version 8)[77]: A lot of the controls are applicable to this:
    - 3.3 Configure Data Access Control Lists
    - 6 access control management
    - 16.8 separate production and non-production systems
  - video om flat vs. segmented networks[78]
- MITRE att&ck frameowrk

[70] https://www.csoonline.com/article/2134037/what-is-the-cyber-kill-chain-a-model-for-tracing-cyberat
html
[71] https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can
[72] https://www.youtube.com/watch?v=II91fiUax2g
[73] https://blog.trendmicro.com/cyberattack-lateral-movement-explained/
[74] https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/
post-exploitation-techniques/lateral-movement-techniques/
[75] https://www.crowdstrike.com/epp-101/lateral-movement/
[76] https://attack.mitre.org/tactics/TA0008/
[77] https://www.cisecurity.org/controls/
[78] https://www.youtube.com/watch?v=Xjo9UG90E0o

  - for reference: MITRE homepage[79]
    * they run e.g. cve.org[80]
  - MITRE att&ck website[81]
  - Design ang philosophy[82]
  - The mandatory getting started[83]
  - a bit by trellix[84]
  - Examples:
    * non standard port[85]
    * network segmentation[86]
    * Loss of availability[87]
    * out-of-band communications[88]
    * DNS datasource[89] - se også referencen

13.5 Lektier til næste gang

1. Kig på listen af angrebsteknikker og udvælg 2-3 teknikker
   - søg evt. inspiration i artikler eller andet på nettet om hvordan et angreb har forløbet
2. Undersøg de tilsvarende mitigation teknikker
   - Forklar hvordan man ville sætte mitigation op i et rigtigt system
3. Undersøg de tilsvarende detection teknikker
   - Forklar hvordan man ville sætte detection op i et rigtigt netværk

14 Uge 20

Aktiv monitorering kender vi at scanne. Dette er ofte støjende og nemt at opdage. Det er også et godt værktøj for en adminsitrator, som ønsker at vide hvad der er på deres netværk.

[79] https://www.mitre.org/
[80] https://www.cve.org/
[81] https://attack.mitre.org/
[82] https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy
[83] https://attack.mitre.org/resources/getting-started/
[84] https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
[85] https://attack.mitre.org/techniques/T1571/
[86] https://attack.mitre.org/mitigations/M1030/
[87] https://attack.mitre.org/techniques/T0826/
[88] https://attack.mitre.org/mitigations/M0810/
[89] https://attack.mitre.org/datasources/DS0038/#Passive%20DNS

14.1 Mål for ugen

Praktiske og læringsmål for ugen er som følger

14.1.1 Praktiske mål

(ingen)

14.1.2 Læringsmål

- Den studerende kan aktiv monitorering og scanne med passende værktøjer
- Den studerende kan forklare attack surface, og interne vs. eksterne tools.

14.2 Leverancer

- Ingen

14.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

14.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Lektier fra sidst: Mitra att&ck
9:15	Scanning, sniffing og attack surfaces
10:15	Intern scanning
11:15	Frokost
12:00	Scannere på internettet: whois, ssllabs, shodanhq, security trail
13:20	lektier
13:30	the end

14.4 Kommentarer

- I kender allerede til passive og aktive handlinger, sniffing og så videre
  - Mitre active scanning[90]
  - CIS critical controls[91]: e.g control 1: inventory, eller control 7: Continuous Vulnerability Management
- Attack surface
  - alle programmer, services og enheder som kan angribes, ie. det hele. Traditionelt set kun det der vender mod internettet, men det er ved at ændre sig.
    - vi vil have fokus på netværksdelen
  - fra okta[92]
  - fra fortinet[93]
  - kombiner attack surface og attack vectors med lateral movement
    - tænk intern og ekstern attack surface, og attack surface på alle enheder.
  - Hvordan afhænger dette af lokaliteten i netværket?
- Interne tools
  - nmap[94] er uundgåelig
    - nmap intro[95]
    - eksempler fra phoenixnap[96]
    - flere eksempler fra cyberciti[97]
    - en oldie but goodie[98]
    - nse examples fra redhat[99]
  - sslscan[100]: en af mine personlige favoritter
    - den er 10 år gammel, men stadigt valid :-)
  - openvas[101]/nessus virker mere som “system sikkerhed” tools
    - download en VM hvis I vil teste[102]

[90] https://attack.mitre.org/techniques/T1595/
[91] https://www.cisecurity.org/controls/cis-controls-navigator/
[92] https://www.okta.com/identity-101/what-is-an-attack-surface/
[93] https://www.fortinet.com/resources/cyberglossary/attack-surface
[94] https://nmap.org/
[95] https://nmap.org/book/man.html
[96] https://phoenixnap.com/kb/nmap-command-linux-examples
[97] https://www.cyberciti.biz/security/nmap-command-examples-tutorials/
[98] https://www.youtube.com/watch?v=M-Uq7YSfZ4I
[99] https://www.redhat.com/sysadmin/nmap-scripting-engine
[100] https://www.kali.org/tools/sslscan/
[101] https://www.openvas.org/
[102] https://www.greenbone.net/en/testnow/

        * architecture[103]

- Internet baserede scannere
  - noget kører kontinuert, andre on demand
  - hvorfor køre det via en internet service og ikke direkte hjemmefra?
  - whois: whois on ucl.dk[104]
  - ssllabs[105]: test af ucl.dk[106]
    * sslscan gør det samme.
  - security trails
    * De har en ASI platform[107]
    * Vi har allerede snakket om denne
  - shodanhq

Links: * CIS CSC20 #3 Continuous Vulnerability Management[108] * Vulnerability management[109] - (kildekritik: afsender ikke vetted)

OBS! (med udråbstegn): Vi laver aktive ting på netværket ofte mod servere og services der kører. Så slå hjernen til og lav ikke en `hail mary` ting, hvis det ikke virker i første forsøg. Vi har mulighed for at forstyrre netværket og services - hvis vi vil være destruktive, så skal det være med vilje.

Der er ting som jeg synes er relevante, men som ikke er spot on * Reconnaisance på ipv6 netværk: RFC 7707[110] og RFC 9099[111] * Openscap: wikipedia[112], getting started[113], howto[114]

14.5 Lektier til næste gang

1. Se emnelisten igennem
2. Sammenlign med Jeres noter
3. Skriv to-tre sætninger til hver om hvad I vil snakke om i 5'ish minutter
4. Vi snakker om det på mandag

[103] https://greenbone.github.io/docs/latest/background.html#architecture
[104] https://mxtoolbox.com/SuperTool.aspx?action=whois%3aucl.dk&run=toolpage
[105] https://www.ssllabs.com/ssltest/
[106] https://www.ssllabs.com/ssltest/analyze.html?d=ucl.dk&latest
[107] https://securitytrails.com/corp/attack-surface-intelligence
[108] https://www.cisecurity.org/controls/continuous-vulnerability-management/
[109] https://www.dnsstuff.com/network-vulnerability-scanner
[110] https://tools.ietf.org/html/rfc7707
[111] https://datatracker.ietf.org/doc/html/rfc9099
[112] https://en.wikipedia.org/wiki/Security_Content_Automation_Protocol
[113] https://www.open-scap.org/getting-started/
[114] https://www.youtube.com/watch?v=6ehIeAxzXSY

15 Uge 21

Aktiv monitorering kender vi at scanne. Dette er ofte støjende og nemt at opdage. Det er også et godt værktøj for en adminsitrator, som ønsker at vide hvad der er på deres netværk.

15.1 Mål for ugen

Praktiske og læringsmål for ugen er som følger

15.1.1 Praktiske mål

- De studerende har en god forståelse for eksamensemne og proceduren

15.1.2 Læringsmål

- ingen

15.2 Leverancer

- Ingen

15.3 Tidsplan

Nedenfor er den foreløbige tidsplan, som vil ændre sig afhængigt af input fra de studerende (m.fl.)

15.3.1 Mandag

Tidsplanen:

Tidspunkt	Aktivitet
8:15	Vi snakker eksamen
?	the end

Vi stopper når vi er færdige.

15.4 Kommentarer

ingen

15.5 Lektier til næste gang

Det er op til Jer. Næste “gang” er eksamenen :-)

16 Additional resources

None at this time