IT Sikkerhet i Norsk arbeidsliv

av
Ole Edvard Hansen

Forelesningens 4 deler

1. Rikets tilstand: Sikkerhet i Norge og verden
2. Applikasjonssikkerhet og sikkerhetsrollen som utvikler
3. Pentesting i Norge
4. Spørsmål og tips

Rikets Tilstand

Sikkerhet i Norge og ute i verden

– Særlig alvorlig er politi- og lensmannsetatens mangler, men også arbeids- og velferdsetaten og Brønnøysundregistrene har kritikkverdige forhold, påpeker riksrevisor Per-Kristian Foss. (Bilde: Jacques Hvistendahl/DagbladetAll Over Press)

Riksrevisjonen refser norsk IKT-sikkerhet

– En rekke etater har alvorlige svakheter.

IT-sikkerheten til Statoil er aldri gransket

Til tross for at dataangrep mot oljesektoren er rekordhøyt, har IT-sikkerheten til Statoil aldri blitt gransket av myndighetene. Men nå skal IT-tabbene frem i lyset.

INGEN IKT-SJEKK: Ingen myndigheter har noensinne gått inn og gransket hvordan Statoil ivaretar IT-sikkerheten etter at selskapet flagget ut IT-driften av plattformer og landanlegg til India. Petroleumstilsynet har ikke fanget opp alvorlige IT-hendelser som har ført til evakuering, nedetid for data og produksjonsstans.
FOTO: HOMMEDAL, MARIT / SCANPIX

Anne Cecilie Remen
Journalist

Line Tomter
Journalist

MER OM NORGE

MER OM STATOIL

MER OM UTFLAGGING AV IT-ARBEIDSPLASSER

Oppdatert i dag, for 6 timer siden

Omstridt kinesisk selskap Huawei leverer til Norge

Det kinesiske selskapet Huawei leverer det nye 4G-mobilnettet som Telenor åpner onsdag. Huawei har møtt stor skepsis i andre land.

PST frykter at fremmede makters data- og internettbaserte etterretning vil kunne ramme norske mål hardere.
FOTO: TIM CHONG / REUTERS

Kilde: **NTB**

MER OM INTERNETT, PC OG MOBIL

Oppdatert 10.10.2012, kl. 06:23

Uproblematisk for Telenor

Telenors kommunikasjonsdirektør Torild Lid Urbarri opplyser at Huawei kun er én av flere leverandører til det nye 4G-nettet og at kineserne oppfyller Telenors krav.

Heller ikke samferdselsminister Marit Arnstad (Sp) har gitt uttrykk for skepsis. Da Huawei var tema i Stortinget, sa hun at hun har tillit til at Telenor har foretatt nødvendige risiko- og sårbarhetsanalyser.

Slik overtar utenlandske IT-selskap norske jobber

FORNEBU (NRK): Utenlandske IT-utviklere får oppdrag for rundt 30 milliarder kroner årlig. Viktig kompetanse og store penger forsvinner ut av Norge til land som India og Ukraina.

INTERNASJONALT MILJØ: Dataingeniør Kishore Mavuri og prosjektleder Venkatesha Prasad i det indiske selskapet TCS jobber sammen med Telenorsjefene Petter Schive og Terje Foyn Johannessen. Inderne har kompetansen Telenor etterspør og er i Norge på midlertidig arbeidstillatelse.
FOTO: ANNE CECILIE REMEN / NRK

Anne Cecilie Remen
Journalist

Line Tomter
Journalist

MER OM NORGE

MER OM NÆRINGSLIV

MER OM TELENOR

Publisert 28.04.2016, kl. 06:24

De store sliter, men i småbedriftene er situasjonen enda mer alvorlig...

HELT UBESKYTTET: Jarl Salomonsen fikk sjokk da han så en av Lofotnetts servere ligge tilgjengelig for alle på nett. På serveren lå det sensitiv kundeinformasjon og passord. Foto: Øistein Norum Monsen / Dagbladet

«Det er et forferdelig sjokk - og trolig kroken på døra»

Selskapet solgte dataløsninger for flere millioner kroner, men kundenes passord lå åpent på Internett.

Meanwhile, in the rest of the world

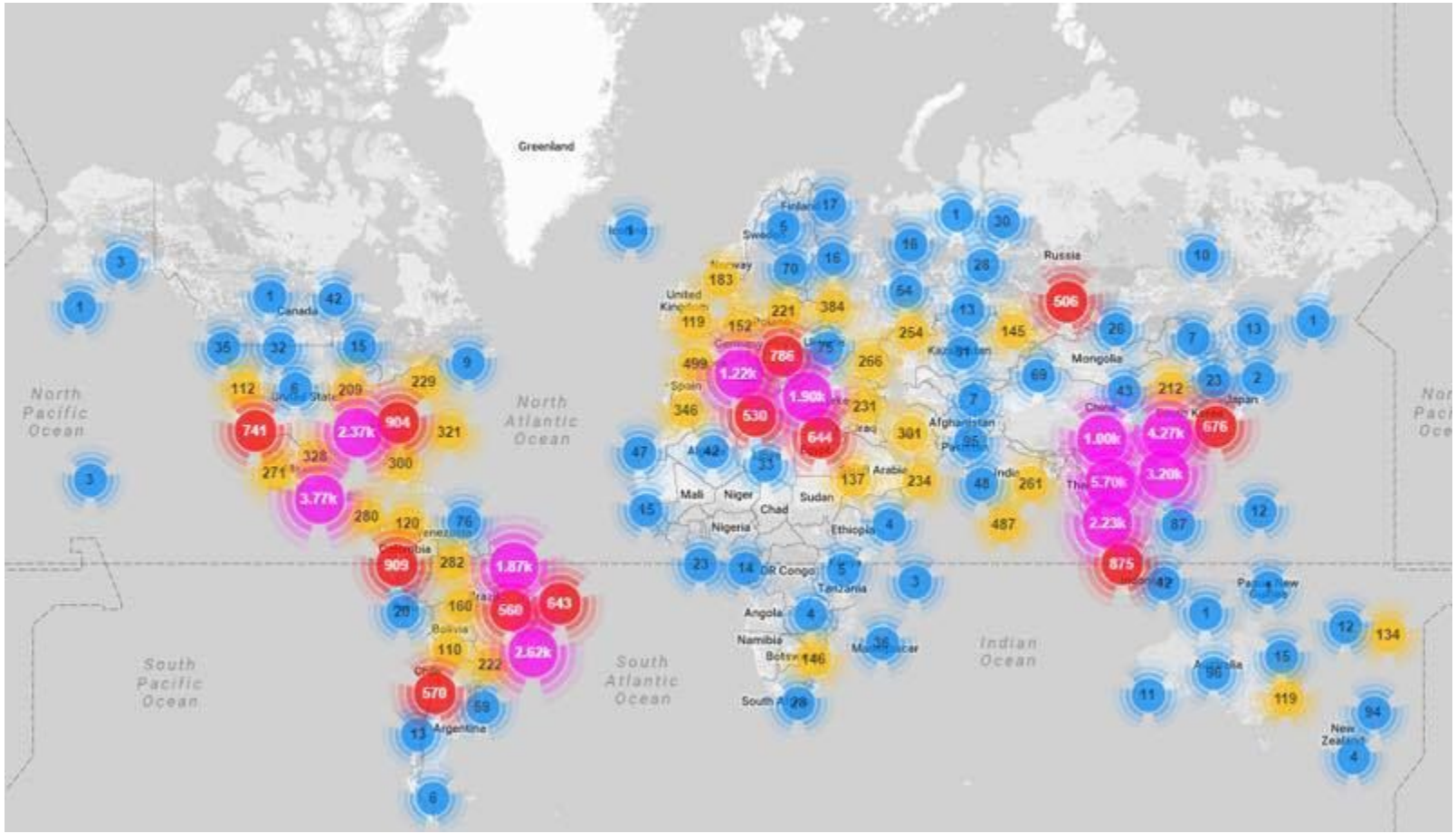
THE DENVER POST

BUSINESS > TECHNOLOGY

60% of small companies that suffer a cyber attack are out of business within six months.

Simple steps can help you avoid a hack that could destroy your fortunes

Mirai Botnetet som kræsjet store deler av USA tidligere i høst



Du retweetet

Jeremiah Grossman @jere... · 21.10.2016

Are we onboard with software manufacturer liability yet, or does the entire internet have to go down or someone die first?

282 378

NEW YORK POST

BUSINESS EXCLUSIVE

Verizon wants $1B discount on Yahoo deal after reports of hacking, spying

By Claire Atkinson

October 6, 2016 | 6:02pm

]HackingTeam[

The Shadow Brokers dump more intel from the NSA's elite Equation Group

PLA unit 61398

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu

Wen Xinyu

Sun Kailiang

Gu Chunhui

Wang Dong


Toolkit

Hvordan holde seg oppdatert om generell sikkerhet?

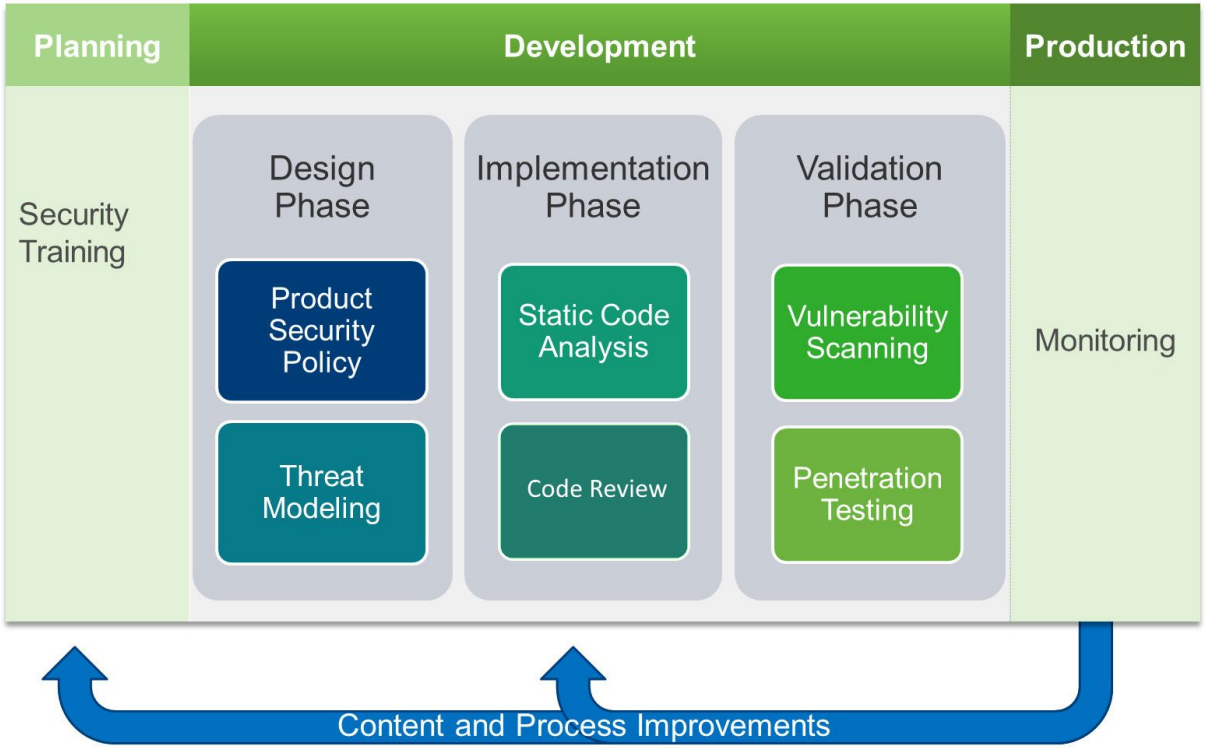
Nasjonal Sikkerhetmyndighets' blogg - Øverste myndighet for sikkerhet i Norge
https://www.nsm.stat.no/om-nsm/mediebrief-fra-nsm/

Brian Krebs' blogg - Den kanskje aller dyktigste sikkerhets-reporteren
http://krebsonsecurity.com

Binni Shah's Twitter Feed - Sikkerhetsindustriens beste kunnskaps-hvelv
https://twitter.com/binitamshah

Applikasjonssikkerhet og sikkerhetsrollen som utvikler

Sikkerhet i utviklingssyklusen



Del I: Trening

Hva må sikres?

All Input is Evil

- Hacking skjer ved manipulasjon av input
- Input kommer fra mange kilder
  - Database
  - Fysisk Nettverk
  - Trådløst Nettverk
  - Tastatur
  - USB og liknende
- Tastaturtasting, filnedlasting, videostreaming, bildevisning over nett, åpning av filer på filshare, bluetoothtilkoblinger - alt dette er input og output.
- Input må valideres og vaskes
- Mye av dagens input er basert på tillit - at vi stoler på den som har laget software/hardware, eller den som benytter et system.
  - Historien har vist oss at det ikke er så klokt.

Autentisering og Autorisering

- Tilgangskontroll er en viktig del av moderne applikasjonsutvikling
  - Det er også noe mange ikke helt får til
  - Kan bruke eksterne autentiseringstilbydere
- Autorisasjon er kunsten om å gi systemtilganger basert på brukere, brukergrupper eller brukerroller.
  - Ofte hårete og komplisert - mange velger å bruke katalogtjenester slik som AD eller LDAP integrert inn i applikasjonen, andre bruker CRUD matriser.

Data må beskyttes fra spionasje

- Selv om hackere ikke klarer å hacke seg inn i et system, så kan de avlytte det
- Nettverkstrafikk må krypteres - TLS/SSL
- Data må krypteres
  - Enveiskryptering
  - Toveiskryptering
  - Kryptering som er sikker i dag, kan være utdatert om 5 år

Strukturer datasystemer i sikre soner

- Gjør alt dere kan for å sikre datasystemer…
- Men gå ut ifra at noen vil klare å bryte seg inn.
  - Det finnes to typer bedrifter:
    - De som vet de har blitt hacket
    - De som ikke vet det enda
- “Vi kjører på lukket nett” er en vanlig argumentasjon for bedrifter som ikke vil investere i sikkerhet (legemiddelindustrien, med mer)
  - Dette stemmer, helt inntil noen kobler seg på lukket intranett med infisert hardware / USB eller kobler opp ruter innenfor lukket sone. Menneskelig faktor vil ALLTID påvirke.
- Ikke nok med perimeterforsvar.
  - Anta at folk kommer forbi første linje, også i miljøer som kjører i lukkede nett
  - Strukturer datasystemene deres i vanntette skott / sikre soner
  - Bruk mye tid på å sikre løsninger som går ut mot internett og sett dem opp (gjerne som proxy) i en ekstern sone.

Del II: Utvikling

- Designfasen
  - Bestem produktets sikkerhetsskop. Hva skal det og skal det IKKE forholde seg til?
  - Kjør trusselmodellering / riskomodellering på ulike use caser
- Implementasjonsfasen
  - Kjør statisk kodeanalyse kontinuerlig - på byggserver
  - Gjennomfør vennligsinnet Code Review.
    - Husk at Code Review er til for å hjelpe hverandre - ikke for å hovere.
- Valideringsfasen
  - Kjør sårbarhetsscannere på systemet
  - Utfør pentrasjonstester

Del III: Monitorering

- Overvåkning av et system i produksjon er viktig, og avdekker ofte feil som ikke ble oppdaget under utvikling
- Fra et sikkerhetsperspektiv så er monitorering viktig for å avdekke hvordan angripere brøt seg inn i applikasjonen
  - Husk at selv de beste applikasjoner kan inneholde sårbarheter. Monitorering er viktig.
- Lagre loggene et sted som ikke er tilgjengelig for resten av applikasjonen.
  - Viktig å ikke lagre dem i samme database
  - Viktig å ikke lagre dem på applikasjonsserveren

NSMs veiledning for oppsett av systemovervåkning:

https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-11_systemovervaking_ved_bruk_av_elk-stakken.pdf


Toolkit

Verktøy og teknikker for applikasjonssikkerhet

Trusselmodellering - Gjennomgang av applikasjonen i designfasen.
Eksempelprogram: Microsoft Threat Modelling Tool
https://www.microsoft.com/en-us/download/details.aspx?id=49168

Best practices og god metode - Dette er kunnskap om hva som skaper sikkerhetshull, og hvilke deler av applikasjonen som må sikres.
Må læres, oppdateres og repeteres jevnlig.

Code Reviews - Gjennomgang av kode sammen med andre utviklere, med formål å avdekke blant annet sikkerhetsavvik

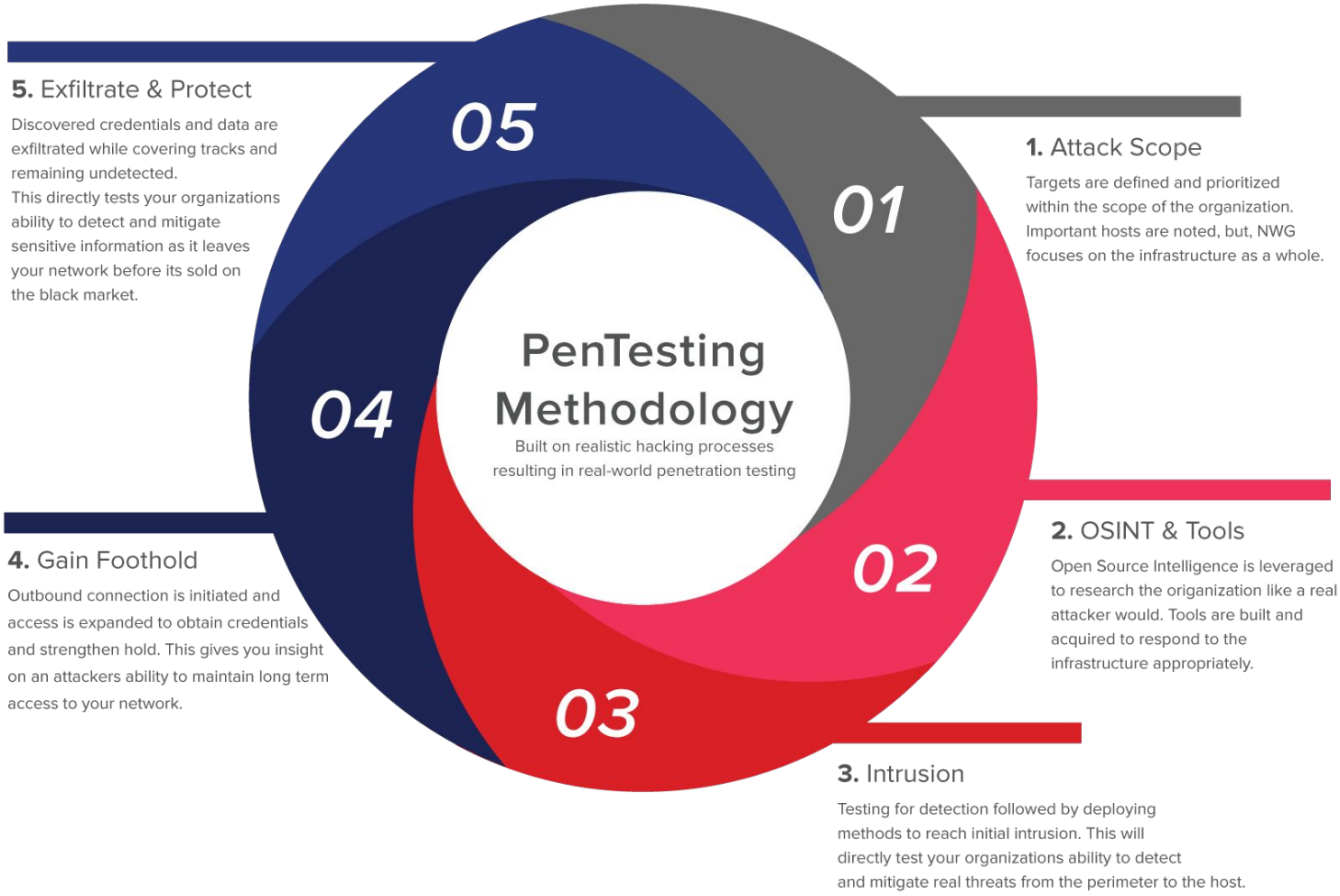
Statisk kodeanalyse - Scanning av kodebase med verktøy, som foreksempel Visual Studio Code Analysis eller FxCop (på Microsoft-baserte prosjekter).
https://fxcopinstaller.codeplex.com

Verktøy og teknikker for applikasjonssikkerhet

OWASP- Open Web Application Security Project er et onlinesamfunn som gir ut gratis verktøy og artikler om hvordan man skal sikre applikasjoner.
Mange, spesielt økonomer, hevder at det holder å sikre applikasjonene for OWASP Top 10 sårbarheter (tja).
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Pluralsight - Pluralsight er et online treningsnettsted som betaler instruktørene sine riktig godt, og som derfor har kursvideoer av høy kvalitet. Det lønner seg å overbevise bedriftsledelsen om å opprette en konto der.
https://app.pluralsight.com/library/courses/owasp-top10-aspdotnet-application-security-risks/table-of-contents

Penetrasjonstester-rollen


05
01
04
02
03
PenTesting Methodology
Built on realistic hacking processes resulting in real-world penetration testing
5. Exfiltrate & Protect
Discovered credentials and data are exfiltrated while covering tracks and remaining undetected.
This directly tests your organizations ability to detect and mitigate sensitive information as it leaves your network before its sold on the black market.
1. Attack Scope
Targets are defined and prioritized within the scope of the organization. Important hosts are noted, but, NWG focuses on the infrastructure as a whole.
4. Gain Foothold
Outbound connection is initiated and access is expanded to obtain credentials and strengthen hold. This gives you insight on an attackers ability to maintain long term access to your network.
2. OSINT & Tools
Open Source Intelligence is leveraged to research the origanization like a real attacker would. Tools are built and acquired to respond to the infrastructure appropriately.
3. Intrusion
Testing for detection followed by deploying methods to reach initial intrusion. This will directly test your organizations ability to detect and mitigate real threats from the perimeter to the host.

Sluttrapporten

Sluttrapporten utarbeides mens dere er i gang - Det er viktig å dokumentere hva dere har testet, og hvilke funn dere har gjort

1. Del 1 av rapporten er en generell intro
2. Del 2 av rapporten inneholder konklusjoner og grafer - til ledelsen
3. Del 3 av rapporten går i dybden teknisk
    a. Hva har blitt testet?
    b. Hvilke funn har blitt gjort?
    c. Hvilke råd gir dere til bedriften?


Toolkit

Nyttige verktøy for pentestere - Del I - OSInt

Open Source Intelligence - OSInt er verktøy og teknikker for å enumerer en organisasjons angrepsflate

Google - https://www.google.com

LinkedIn - https://www.linkedin.com

Facebook - https://www.facebook.com/ / http://graph.tips

FOCA - https://www.elevenpaths.com/labstools/foca/index.html

Shodan - https://www.shodan.io

Nyttige verktøy for pentestere - Del II - Systemer

Kali Linux - Kali Linux er en Linuxdistro med viktige verktøy preinstallert

Metasploit - Metasploit er et rammeverk skrevet i Ruby. Det er open source, og har egen repo på Github. Metasploit er et automatisert rammeverk for alle ledd av pentesting-syklusen - https://github.com/rapid7/metasploit-framework/

Burp - Som dere allerede vet så er Burp Suite den desidert beste proxyen for pentesting av web-applikasjoner - https://portswigger.net/burp/

Nessus eller nExpose - Nessus og nExpose er sårbarhetsscannere som kan kjøre vulnerability scans av systemer. Scanningen har flere moduser og rapporten som genereres er veldig god -
http://www.tenable.com/products/nessus-vulnerability-scanner/nessus-professional
https://www.rapid7.com/products/nexpose/download.jsp

Du retweetet

the grugq @thegrugq · 07.02.2015

Give a man an 0day and he'll have access for a day, teach a man to phish and he'll have access for life.

3 522 3 839

Nyttige verktøy for pentestere - Del III - Phishing

Phishing er en variant av social engineering som angriper mennesker istedenfor systemer

Social-Engineering-Toolkit (setoolkit) - Skrevet av Dave Kennedy (Rel1k) - https://www.trustedsec.com/social-engineer-toolkit/

Browser Exploitation Framework (BeEF) - Laget av Wade Alcorn og Michelle Orru - http://beefproject.com

Veil - Veil er et rammeverk for mutasjon av angreps-payloads (skjuler kjent malware fra antivirus-motorer) - https://www.veil-framework.com/
(Brukes i kombo med setoolkit og/eller metasploit)

Nyttige verktøy for pentestere - Del IV - Persistence

Persistence får man når installerer diverse software på vertsmaskinen etter å ha brutt seg inn.

Det er vel heller tvilsomt at kunden ønsker at du skal opprette persistence, men du kan jo legge igjen proof i form av en textfil inne på administrators domenekontroller eller documentfolder (hvis du kommer så langt).

For å få god persistence er det viktig å eskalere privileges:

Mimikatz - https://github.com/gentilkiwi/mimikatz - Get the Golden Ticket!

Windows Credentials Editor - (Windows 8 siste versjon som dette funker på) http://www.ampliasecurity.com/research/windows-credentials-editor/

Spørsmål og tips

Hvordan blir hverdagen som sikkerhetsansvarlig i ulike typer bedrifter*?

Offentlig / Statlig
- Underlagt sikkerhetsloven
- Riksrevisjonen følger med som hauker
- Lydhøre ovenfor NSM
- Stort fokus på sikkerhet
- Stort sikkerhetsbudsjett

Privat - Konsern / Storbedrift
- Underlagt sikkerhetsloven
- Har av og til dyktige sikkerhetsarkitekter
- Verdsetter sikkerhetsekspertise
- Sikkerhet i annen rekke etter produktutvikling
- Sikkerhet viktig i anbudsfasen

Offentlig / Kommunalt
- Underlagt sikkerhetsloven
- Liten IT driftsavdeling med lav kompetanse
- Sikkerhetsoppgaver tilknyttet brukerstøtte og oppsett av antivirus, brannmur, patching osv.

Privat - Liten / Mellomstor bedrift
- Underlagt sikkerhetsloven, men vet det ikke
- Har sjelden sikkerhetskompetanse
- Sikkerhet er overlatt til tilfeldighetene
- Har med stor sannsynlighet blitt hacket, uten at de vet det.

*(gjelder ikke rene sikkerhetsfirmaer)

Spørsmål?