

Oppgave 1. Generelt

Informasjonssikkerhet kort fortalt betyr å beskytte data og holde informasjon privat og sikret.

Daglig bruk av mobil og pc har blitt en del av livet vårt i det moderne samfunnet. Statistikken viser at det er ca 5 millioner mennesker som bruker internett. (Statista). Veksten på kriminalitet over internett har dermed også økt. Stadig flere blir utsatt for tyveri av personlig data eller penger. Hvordan skal vi beskytte oss mot slike trusler? For å redusere risikoen at du blir utsatt for angrep må vi bruke CIA modellen som står for Confidentiality, Integrity og Availability.

Confidentiality - Setter en begrensing på tilgang til informasjon, dette sørger for personvern.

Dette betyr at informasjon skal ikke bli avslørt av uautoriserte personer. Informasjon skal derfor holdes trygt og hemmelig, ved bruk av å kryptografi for å kryptere innholdet. Dette gjøres ved at informasjonen som blir kryptert kan kun leses dersom du har nøkkelen til å dekryptere den. Vi kan ved flere måter oppnå konfidensialitet.

- Encryption: når vi krypterer data trenger vi en kode som vi kaller for secret key. For å kunne dekryptere det tilbake til original stand må vi ha en dekrypterings kode, som eksempel kan være den samme secret key.
- Access Control: Dette kan være fra nøkkelkort eller adgangskode som kan identifiseres.
- Biometric: fingerprint eller iris scan som bruker mønstre til å gjenkjenne deg.

Integrity betyr at data skal være troverdig, originale data skal ikke ha blitt forandret uten riktig autorisasjon. Hvis pc har fått virus eller skadevare kan den stjele passord eller endre på filer. Man

kan ta hyppige kopier av filer, for å gjenopprette data dersom man skulle miste dem. Vi har metoder som sjekker om data ikke har blitt endret underveis.

- Checksum: en funksjon som gir et resultat for å kunne sammenligne med originale filen for endringer. Hvis filen har blitt endret med en karakter så vil svaret være annerledes.
- Metadata: vi må også beskytte metadata som inneholder informasjon om hvem som er eier, når det var lagd, når ble den sist brukt og hvem som har tilgang til dataen.

Availability betyr at det skal være lett tilgjengelig for autoriserte folk som skal jobbe med data.

Disse dataene skal lagres et sted som er robust og godt beskyttet med pålitelighet.

Vi kan bruke backup diskene til å lagre flere kopier av dataene eller ha USB minnepenn som er veldig praktisk å ha med.

- RAID1 en måte å ta backup på diskene, alle data blir kopiert over på to diskene, hvis den ene skulle gå tapt så har du fortsatt en backup av backup.

Oppgave 2. Konto hijacking og identitetstyveri

Hvis en hacker hadde fått seg tilgang til min konto ville han hatt fått veldig mye data om meg, alt fra personlige eiendeler, familien min, det sosiale. Epost er jo en viktig verktøy alle bruker i dag alt fra private til jobb, så man vet aldri hva en hacker kan komme seg frem til ved utpressing eller andre slags metoder for å oppnå målet. I de fleste tilfellene så er det sikkert PayPal konto, banker eller cryptocurrency wallet for å stjele pengene dine. Andre ting kan være bilder eller selge dataene videre til potensielle kjøpere.

Jeg tenker at hacker vil også bruke kontoen min til å sende phishing mails til mine kontakter i håp at de skal gå på fellen. Tiltak på det er vel å bli flinkere på å lage sterkere passord og multi-factor authentication som gir ekstra beskyttelse. En annen måte å beskytte seg er skille din private mail og den du bruker for alt andre ting på nett. Man kan f.eks. bruke maskerte mail tjenester eller når man skal registrere seg på en ny tjeneste kan man ha en kontroll på hvis de selger data om deg videre. Dette kan vi gjøre ved å skrive mymail+netflix@gmail.com hvis det strømmer inn reklamer så kan man blokkere hele domene.

Jeg tenker at hvis hacker har både kode og min BankID hadde jeg blitt utsatt for et kjempe stort brudd på personvern og sikkerheten min. Hacker kommer til å tømme kontoen eller hvitvaske penger. I det verste fall blir alt av kontoen min slettet når de gjør seg ferdige.

Hvis man tar høyde for dette tenker jeg at vi har en absolutt god grunn til å bli flinkere på å beskytte dataene våre, bruke anti-virus, trene opp sine nærmeste familiemedlem hvordan beskytte seg selv.

Oppgave 3. Skadevare

Worm	sprer seg og lager kopier av seg selv, som en smittebærer av en annen skadevare
Trojan	en “vanlig” hjelpeprogram som gjemmer en annen skadevare
Payload	nyttelast, f.eks. rootkit, gir deg adgang helt til kernel mode

Malware er av type programvare bygget for å utføre skader og utnyttelser. Det kan ha fra små til store konsekvenser i det verste fall katastrofale skader. Programvaren kjøres skjult i bakgrunnen og utfører oppgaver den ble designet til.

- Computer Worm vil kunne spre seg uten en host og lager kopier av seg selv. Den vil utnytte sårbarheter på maskiner som ikke har blitt patchet. Ormen vil kunne infisere andre

maskiner på samme nettverk som prøver å fortsette lage kopier av seg selv. På Windows vil den endre på regedit som gjør at ormen kjøres ved maskin start.

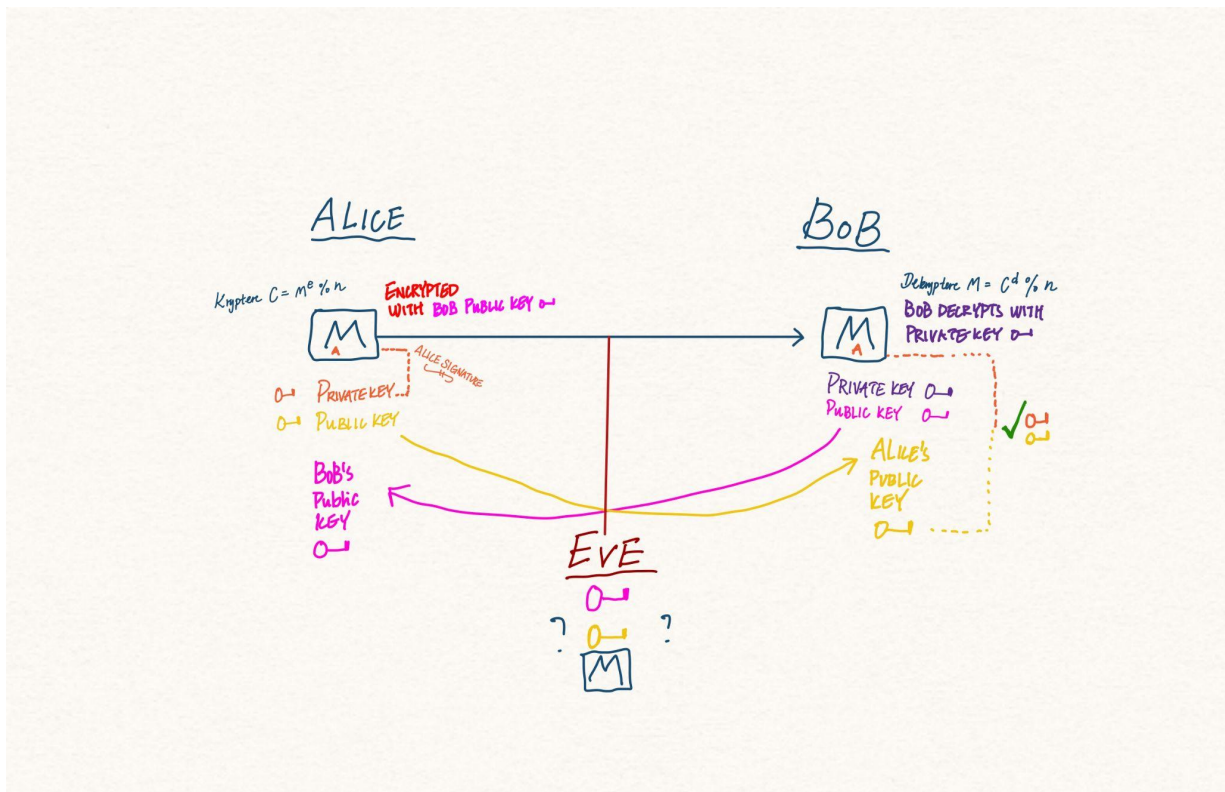
ILOVEYOU spredte seg over email når den blir åpnet. Inne på mailen var det en vedlegg som inneholdt ormen. Windows 2000 ble mest infisert av ormen fordi den skjulte extensions som standard LOVE-LETTER-FOR.YOU.TXT

- Brain er en computer virus på floppy disk. Viruset lagde en kopi av seg selv når den blir kjørt deretter bytter på boot loader (boot) for floppy disker så viruset kjører istedenfor. Virus krever host og for å kunne spre seg må det begå en menneskelig handling.
- WannaCry en ransomware hvordan den spredte seg er ukjent men antakeligvis via phishing spam mails og fra der spredte seg selv til andre på globalt nivå. Ransomware er først og fremst ute etter penger. Programmet krypterer alt på disk og utpresser brukere for penger mot “dekryptering”. Programmet inneholder en bakdør som blir gjemt av Trojan (EternalBlue), nyttelasten er å kjøre WannaCry.
- Stuxnet er en kompleks malware som inneholder alle typer i seg. Den endrer også på regedit og vil starte opp selv etter reboot replikerer seg selv og sprer videre. Drivere som “mrxnet.sys” og mrxcels.sys” er trojaner som gjemmer resten av nyttelasten. Rootkit “wtr4132.tmp” og “wtr4141.tmp” er rootkits med verifisert digital signatur som gir adgang til kernel mode. (Symantec Response, p.30)

Vi har mange typer av malware og i tabellen er det klassiske kjennetegn som klassifiserer hver av disse.

Oppgave 4. Kryptering

I RSA kryptering så handler dette om asymmetrisk key exchange. Du har en Private key og en Public key. Private key beholder du for å dekryptere og signerer, Public key bruker du for å kryptere meldinger og verifisere. For å kunne verifisere meldingen ikke er forfalsket må vi bruke signatur.



Vi starter ut i fra at Alice og Bob genererer hvert sitt nøkkelsett. De veksler Public key med hverandre. Alice sender nå en melding og krypterer med Bob sin Public key $c = m^e \pmod n$. Bob får denne krypterte meldingen og dekrypterer med sin Private key $m = c^d \pmod n$. Meldingen kan kun dekryptere med Bob sin Private Key. I samme meldingen som Alice sender til Bob, inneholder det Alice sin digital signatur, med andre ord så krypterer Alice meldingen også med sin Private Key. Hvis Bob bruker Alice sin Public Key og det gir en match med signaturen må den komme fra og kun Alice. Vi bruker da egen Private Key som signatur sender

til mottaker som verifiserer og hverandres Public Key for å sende meldinger for så dekryptere med egen Private Key.

Oppgave 5. Kryptering (utregning)

Alice's public key: $n = 3233$, $e = 17$ & private key: $n = 3233$, $d = 2753$

Bob encrypts message: $c = m^e \bmod n$

Alice decrypts message: $m = c^d \bmod n$ – **$1759^{2753} \% 3233 = 68$**

c	1759	2160	1992	690	1632	2235	1992	1859	2680	2790
m	68	117	32	107	97	110	32	82	83	65
ASCII	D	u		k	a	n		R	S	A

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	 	Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	\$	68	44	104	D	D	100	64	144	d	d

ASCII ▼

To

Text ▼

68 117 32 107 97 110 32 82 83 65

Du kan RSA

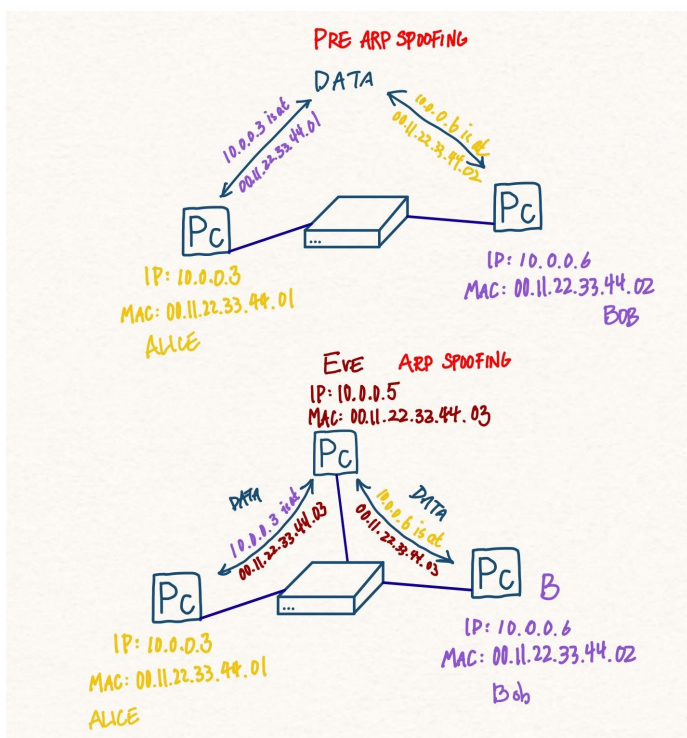
Oppgave 6. Nettverk

ARP står for Address Resolution Protocol som oversetter IP adresser til MAC adresser. Alle enheter må ha en MAC adresse som er den fysiske adressen for enheten. MAC adresser brukes for å identifisere seg selv i et nettverk. Når en enhet vil kommunisere med en annen på samme lokalt nettverk trenger vi MAC adressen til mottakeren.

Vi kan slå opp i switch tabellen med en `arp -a` command for å se alle enheter som er koblet på nettverket. Når du sender ut arp pakken er det en forespørsel til alle på lokale nettverket.

Maskinene svarer tilbake og identifiserer seg selv med MAC adressen sin.

Eve er også på samme nettverk og være man-in-the-middle for å utføre ARP spoofing. Det vil si at Eve vil kunne se alt av dataene mellom Alice og Bob.



```
C:\Users\Administrator>arp -a

Interface: 136.129.3.15 --- 0x10
Internet Address      Physical Address      Type
136.129.3.130         00-90-0f-0f-47-8d    dynamic
136.129.3.135         00-90-0f-0f-47-9d    dynamic
136.129.3.140         00-90-0f-0f-48-51    dynamic
136.129.3.145         00-90-0f-0f-48-53    dynamic
136.129.6.2           00-1d-9c-c8-be-2a    dynamic
136.129.255.255       ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.252          01-00-5e-00-00-fc    static
239.192.128.224       01-00-5e-40-80-e0    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 10.0.100.1 --- 0x13
Internet Address      Physical Address      Type
10.0.100.96           00-03-2d-23-ba-51    dynamic
10.0.100.255          ff-ff-ff-ff-ff-ff    static
```

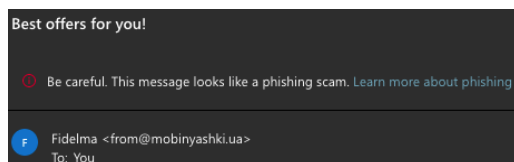
networkencyclopedia

Oppgave 7. Phishing

Phishing er en homofon for fish hvor angriper bruker avanserte verktøy for å skanne lekket domener for offer. Angriper forsøker å lure brukere for personlig informasjon som brukernavn og passord. Man får ofte spam mails og hvis du trykker på linkene vil dataen din bli lekket i det verste tilfelle infiserer du enheten din med skadevare. Andre typer som Whaling er målrettet mot store selskaper og organisasjoner for informasjon og penger. Angriperen vil f.eks. sende epost og endrer på DNS i host filen ved bruk av Social Engineering Attack som lurer deg til en falsk side og stjeler alle informasjonene.

Ansatte må trenes opp av spesialister mot phishing i kjennetegn på typiske phishing mails.

Hvordan ansatte skal forsvare ved å inspisere URL, ikke bare trykk på link. Installere antivirus og anti-ransomware på maskinene. Selskaper kan sette strengere krav ved deling av informasjon på sosiale medier. Eventuelt kan man sette på filter slik at alle mailer som kommer utenfor nettverket blir flagget, dette minsker risikoen.



Oppgave 8. Hjemmekontor

Det har blitt vanlig å jobbe hjemmefra. Mange som synes det er helt greit andre ikke så mye og vil tilbake til den normale hverdagen. Det kan være en risiko for mange ansatte som velger å jobbe hjemme men ser bort fra sikkerheten. Bruker ansatte jobb PC eller hjemme PCe til å bearbeide dataene. Hvordan holde sensitiv informasjon konfidensiell hjemme fra.

Det er lurt å implementere passord på alle jobbrelaterte enheter. Det finnes mange trusler i dag og det kommer til å bli enda mer i fremtiden. De fleste av oss vil nok ikke være et mål som andre folk eller organisasjoner er spesifikt ute etter med mindre du er en høyt profilert person. Men det betyr ikke at vi skal ikke være obs på våre handlinger.

Vi kan være mer bevisste på det vi gjør, aktsom på valgene vi tar. Det er mindre sannsynlighet for at du blir skal bli en offer hvis du ikke har alt av informasjon i det åpne, som f eks sosiale medier. Lite informasjon om deg på internett minsker naturligvis vektorene som utfører skade mot deg. Vi vil faktisk være en av de største trusselen mot egen personvern og sikkerhet. Alle kan ta feil på et tidspunkt, men hvis vi implementer CIA modellen passer det utmerket for oss som holder oss oppdatert innenfor informasjonsteknologi. Hvis vi følger noen prinsipper ut ifra modellen kan vi aktivt beskytte oss mot trusler.

Trusler som omgår mange av oss er e post, spammet med phishing lenker som er ute etter bankkortet ditt eller passordene dine og andre skadevare mot deg og dine enheter. Hvis det er mail fra banken din kan man like godt logge seg inn fra ny fane enn å trykke på linken som ble sendt til deg. Det har blitt vanlig på nettsider når man lager passord skal være en minstestandard på en rekke betingelse. Vi kan lage et kompleks passord, men kan vi opprettholde denne standarden over tid, ikke minst hvordan skal vi huske på alle forskjellige tjenester vi bruker. Vi kan nettopp benytte password manager som genererer tilfeldige og sterke passord for oss. For å gjøre det enda mer sikker kan vi implementere tokens f eks Google's authentication.

Antivirus vil være det minstekravet i dag for å regne som "godt" beskyttet i det store trusselbildet.

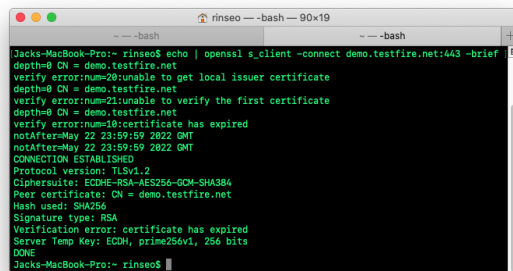
Oppgave 9. Praktisk SSL analyse

Jeg bruker commando `echo | openssl s_client -connect demo.testfire.net:443 -brief`

`echo |` = print melding og avbryt kobling med ny linje

`s_client -connect host:port` = tester kobling med SSL/TLS mot host på port 443(https)

`-brief` = ekskluderer info



Protocol version: TLSv1.2

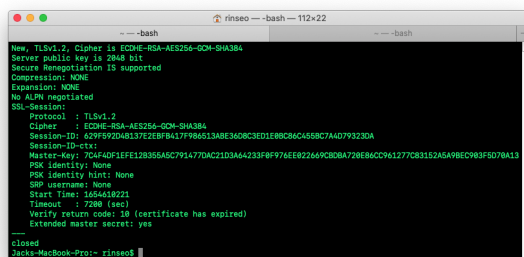
Ciphersuite:

`ECDHE-RSA-AES256-GCM-SHA384`

Hash: SHA256

Type: RSA

Verification error: Certificate has expired



Jeg kjører følgende commands:

`openssl s_client -connect demo.testfire.net:443 -tls1_2`

Er en flag for TLS versjon

Vi kan se at det brukes `Diffie-Hellman for Public Key exchange` RSA brukt som algoritme

`AES256 standard 256 bit key GCM som metode` `SHA384 Hash symmetrisk algoritme`

SSL/TLS over HTTP gjør data som sendes mellom klient og vert kryptert. Vi forestiller at det er

Eve som avlytter trafikken som strømmes, men uten å ha tilgang til private key er det så å si

umulig å dekryptere meldingen. Klienten vil i dette tilfellet sende en forespørsel (3-way

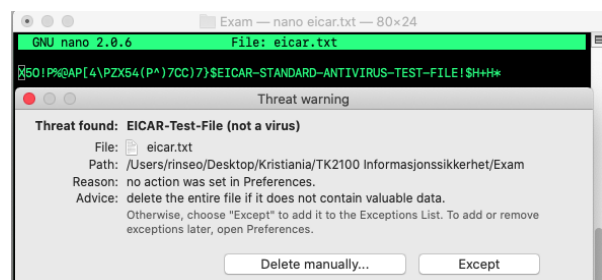
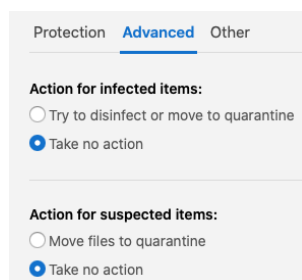
handshake) og velger den mest sikret Hash funksjon(SHA256). Hash skal sjekke for kollisjon

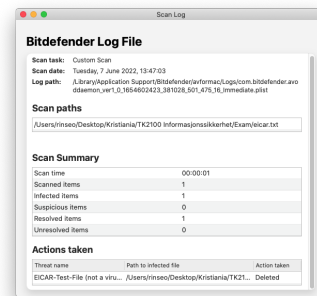
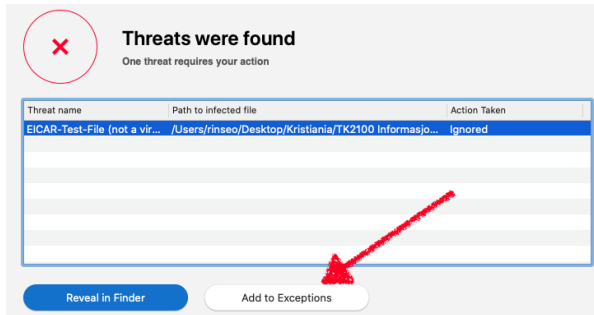
hvis data har blitt endret selv med én karakter vil digest(resultat) ikke samsvare.

Hosten her har ikke fornyet sin sertifikat og klienten kan dermed ikke verifisere hvem host egentlig er. Trafikken vil ikke være kryptert. De fleste sårbarheter man finner i TLSv 1.2 er pga støtte for legacy versjoner av algoritmer hvor brukere prøver med f eks POODLE – protokoll for å nedgradere versjoner. For å nevne noe eldre versjoner så skal man ikke bruke MD5 som har kun 128 bit og mange svakheter. Dagens standard er minimum 256 bit. Andre ting kan være argument eNULL i parameter hvor det er ingen kryptering som skjer og da viser absolutt alt i klar tekst.

Oppgave 10. Praktisk anti-virus

Først går jeg inn på Bitdefender og skruer av autopilot på håndtering av virus, ellers vil AV skanne min enhet for filer som har samme mønster som kjennetegner til å være virus så slette det. Jeg lager en ny tekstfil med navn *eicar.txt* som inneholder 68 karakter strengen i nano. Så høyreklikker på filen og skanner for virus. Bitdefender har oppdaget mønsteret i filen som er verifisert virus for test. Den inneholder ingen skade. Jeg skruer autopilot tilbake og Bitdefender har nå fjernet filen, jeg inspiserer loggen fra handlingen at filen har blitt riktig fjernet.





Kilder

Statista. *Global Digital Population of April 2022*.

<https://www.statista.com/statistics/617136/digital-population-worldwide/>

Network Encyclopedia. *arp commands* <https://networkencyclopedia.com/arp-command/>

ILOVEYOU <https://en.wikipedia.org/wiki/ILOVEYOU>

Brain. *Computer Virus* [Brain \(computer virus\) - Wikipedia](#)

EternalBlue <https://en.wikipedia.org/wiki/EternalBlue>

W32.Stuxnet Dossier Version 1.4 (February 2011). *Nicolas Falliere, Liam O Murchu, and Eric Chien* <https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en>

Ciphersuite. https://ciphersuite.info/cs/TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384/

OpenSSL. *-tls1_2*. https://www.openssl.org/docs/man1.0.2/man1/openssl-s_client.html

POODLE. *downgrade attack*. <https://crashtest-security.com/downgrade-attack/>