Security: AO1

1) Verklaar/bespreek volgende termen
    a) bitlocker op windows

BitLocker is de gratis ingebouwde encryptietool van Windows 10. Hiermee kun je volledige schijven versleutelen. Bovendien biedt het programma bescherming tegen onbevoegde veranderingen in je besturingssysteem, zoals bijvoorbeeld malware op firmware niveau.

Systeemvereisten

BitLocker is alleen beschikbaar op computers die draaien op Windows Vista of 7 Ultimate, Windows Vista of 7 Enterprise, Windows 8.1 Pro, Windows 8.1 Enterprise, of Windows 10 Pro. De gratis versie van Windows 10 zit daar dus niet bij.

Bovendien moet je een opslagschijf hebben met minimaal twee partities en een Trusted Platform Module (TPM), een speciale chip die controles op je hardware, software en firmware kan uitvoeren. Wordt er een onbevoegde verandering aangetroffen, dan wordt je computer in een beperkte modus opgestart zodat kwaadwillenden weinig extra schade kunnen aanrichten.

    b) EFS op Windows

Het Encrypting File System (EFS) is een component van het NTFS-bestandssysteem op Windows 2000, Windows XP Professional en Windows Server 2003. (Windows XP Home bevat geen EFS.) EFS maakt transparante codering en decodering van bestanden mogelijk door geavanceerde , standaard cryptografische algoritmen. Elk individu of programma dat niet over de juiste cryptografische sleutel beschikt, kan de gecodeerde gegevens niet lezen.Versleutelde bestanden kunnen zelfs worden beveiligd tegen personen die fysiek in het bezit komen van de computer waarop de bestanden zich bevinden. Zelfs personen die geautoriseerd zijn voor toegang tot de computer en het bijbehorende bestandssysteem, kunnen de gegevens niet bekijken. Hoewel andere verdedigingsstrategieën moeten worden gebruikt en codering niet de juiste tegenmaatregel is voor elke dreiging, is codering een krachtige aanvulling op elke defensieve strategie. EFS is de ingebouwde bestandsencryptie tool voor Windows-bestandssystemen.

Elk defensief wapen, echter, als het verkeerd wordt gebruikt, kan schade aanrichten. EFS moet worden begrepen, op de juiste manier worden geïmplementeerd en effectief worden beheerd om ervoor te zorgen dat uw ervaring, de ervaring van degenen aan wie u ondersteuning biedt en de gegevens die u wilt beschermen, niet worden geschaad.Dit document zal

Basisfeiten over EFS

- EFS-codering vindt niet plaats op toepassingsniveau, maar op bestandssysteemniveau; daarom is het coderings- en decoderingsproces transparant voor de gebruiker en voor de toepassing. Als een map is gemarkeerd voor codering, wordt elk bestand dat is gemaakt in of verplaatst naar de map, gecodeerd.Toepassingen hoeven EFS niet te begrijpen of EFS-gecodeerde bestanden niet anders te beheren dan niet-versleutelde bestanden. Als een gebruiker probeert een bestand te openen en over de sleutel beschikt om dit te doen, wordt het bestand zonder extra inspanning van de kant van de gebruiker geopend. Als de gebruiker niet over de sleutel beschikt, wordt het foutbericht 'Toegang geweigerd' weergegeven.
- Bestandsversleuteling gebruikt een symmetrische sleutel, die vervolgens zelf wordt gecodeerd met de openbare sleutel van een coderingspaar voor openbare sleutels. De bijbehorende persoonlijke sleutel moet beschikbaar zijn om het bestand te kunnen ontsleutelen. Dit sleutelpaar is gebonden aan een gebruikersidentiteit en wordt beschikbaar gesteld aan de gebruiker die het gebruikers-ID en wachtwoord heeft. Als de persoonlijke sleutel is beschadigd of ontbreekt, kan zelfs de gebruiker die het bestand heeft gecodeerd het niet decoderen. Als er een herstelagent bestaat, kan het bestand mogelijk worden hersteld.Als sleutelarchivering is geïmplementeerd, kan de sleutel worden hersteld en het bestand worden gedecodeerd. Zo niet, dan kan het bestand verloren zijn. EFS is een uitstekend bestandscoderingssysteem - er is geen "achterdeur".
- Bestandsversleutelingssleutels kunnen worden gearchiveerd (bijvoorbeeld geëxporteerd naar een diskette) en op een veilige plaats worden bewaard om te zorgen dat de sleutels kunnen worden hersteld als de toetsen beschadigd raken.
- EFS-sleutels worden beschermd door het wachtwoord van de gebruiker. Elke gebruiker die de gebruikers-ID en het wachtwoord kan verkrijgen, kan zich als die gebruiker aanmelden en de bestanden van die gebruiker decoderen. Daarom moeten een sterk wachtwoordbeleid en een sterke gebruikerseducatie een onderdeel zijn van de beveiligingspraktijken van elke organisatie om de bescherming van EFS-gecodeerde bestanden te waarborgen.
- EFS-gecodeerde bestanden blijven niet versleuteld tijdens transport als ze worden opgeslagen in of worden geopend vanuit een map op een externe server. Het bestand wordt gedecodeerd, doorloopt het netwerk in leesbare tekst en wordt, als het is opgeslagen in een map op het lokale station die is gemarkeerd voor codering, lokaal versleuteld. EFS-gecodeerde bestanden kunnen gecodeerd blijven tijdens het doorkruisen van het netwerk als ze worden opgeslagen in een webmap met behulp van WebDAV. Deze methode voor opslag op afstand is niet beschikbaar voor Windows 2000.
- EFS maakt gebruik van FIPS 140-geëvalueerde Microsoft Cryptographic Service Providers (CSP-componenten die coderingsalgoritmen bevatten voor Microsoft-producten).

c) Hoe zou je dit op een linux systeem implementeren?

Schijfencryptie op een linux systeem:

Alle schijfversleutelingsmethoden werken op zo'n manier dat zelfs als de schijf gecodeerde gegevens bevat, het besturingssysteem en de toepassingen het "zien" als de corresponderende normaal leesbare gegevens zolang de cryptografische container (dwz het logische deel van de schijf die de de versleutelde gegevens) is "ontgrendeld" en gemount.
Hiervoor moet een aantal "geheime informatie" (meestal in de vorm van een sleutelbestand en / of wachtwoordzin) door de gebruiker worden verstrekt, waaruit de eigenlijke versleutelingssleutel kan worden afgeleid (en gedurende de duur in de kernelsleutelring worden opgeslagen). van de sessie).

Als je helemaal onbekend bent met dit soort operaties,
lees ook het gedeelte #How the encryption works hieronder.

De beschikbare methoden voor schijfversleuteling kunnen op basis van hun werkingslaag in twee typen worden verdeeld:

Stacked filesystem encryption

Gestapelde bestandsysteemencryptieoplossingen worden geïmplementeerd als een laag die bovenop een bestaand bestandssysteem wordt gestapeld, waardoor alle bestanden naar een codering worden geschreven-
actieve map wordt on-the-fly gecodeerd voordat het onderliggende bestandssysteem ze op schijf schrijft en ontsleuteld wanneer het bestandssysteem ze van schijf leest. Op deze manier worden de bestanden in gecodeerde vorm opgeslagen in het hostbestandssysteem (wat betekent dat hun inhoud, en meestal ook hun bestands- / mapnamen, worden vervangen door willekeurige
op zoek naar gegevens van ongeveer dezelfde lengte), maar anders dan dat ze nog steeds bestaan in dat bestandssysteem als ze zouden zonder encryptie, zoals normale bestanden / symlinks / hardlinks / etc.

De manier waarop het wordt geïmplementeerd is om de map te ontgrendelen die de onbewerkte gecodeerde bestanden opslaat in het hostbestandssysteem ("lagere map"),
het is op zichzelf geplaatst (optioneel met een speciaal gestapeld pseudo-bestandssysteem) of optioneel op een andere locatie ("bovenste map"), waar dezelfde bestanden vervolgens in leesbare vorm worden weergegeven - totdat het opnieuw wordt gedeactiveerd of het systeem wordt uitgeschakeld.

Beschikbare oplossingen in deze categorie zijn eCryptfs en EncFS.

Block device encryption

Versleutelingsmethoden voor apparaatversleuteling werken daarentegen onder de bestandssysteemlaag en zorgen ervoor dat alles dat naar een bepaald blokapparaat (dwz een hele schijf

of een partitie of een bestand dat als een virtueel loopback-apparaat fungeert) is gecodeerd . Dit betekent dat terwijl het blokapparaat offline is,
de volledige inhoud ziet eruit als een grote klodder van willekeurige gegevens, zonder enige manier om te bepalen welk soort bestandssysteem en welke gegevens het bevat. Toegang tot de gegevens gebeurt opnieuw door de beschermde container (in dit geval het blokapparaat) op een speciale manier op een willekeurige locatie te monteren.
De volgende "block device encryption" -oplossingen zijn beschikbaar in Arch Linux:

loop-AES
loop-AES is een afstammeling van cryptoloop en is een veilige en snelle oplossing voor systeemversleuteling. Loop-AES wordt echter beschouwd als minder gebruikersvriendelijk dan andere opties, omdat het niet-standaard kernelondersteuning vereist.
dm-crypt
dm-crypt is het standaardapparaat-mapper encryptie-functionaliteit geboden door de Linux-kernel. Het kan direct worden gebruikt door diegenen die graag volledige controle hebben over alle aspecten van partitie en sleutelbeheer. Het beheer van dm-crypt wordt gedaan met het cryptsetup userspace-hulpprogramma. Het kan worden gebruikt voor de volgende soorten codering van block-devices: LUKS (standaard), gewoon, en heeft beperkte functies voor loopAES- en Truecrypt-apparaten.

- LUKS, standaard gebruikt, is een extra laag die alle benodigde installatie-informatie voor dm-crypt op de schijf zelf opslaat en partitie en sleutelbeheer abstraheert in een poging om het gebruiksgemak en de cryptografische beveiliging te verbeteren.
- eenvoudige dm-crypt-modus, omdat het de oorspronkelijke kernelfunctionaliteit is, wordt de extra laag niet gebruikt. Het is moeilijker om dezelfde cryptografische sterkte ermee te gebruiken. Daarbij zijn de langere toetsen (wachtzinnen of sleutelbestanden) het resultaat. Het heeft echter andere voordelen, beschreven in de volgende vergelijkingstabel.

Bestandencryptie op een linux systeem:

GnuPG is een volledige en gratis implementatie van de OpenPGP-standaard zoals gedefinieerd door RFC4880 (ook bekend als PGP). Met GnuPG kunt u uw gegevens en communicatie versleutelen en ondertekenen. Het beschikt over een veelzijdig sleutelbeheersysteem en toegangsmodules voor allerlei soorten openbare sleutelfolders. GnuPG, ook bekend als GPG,
is een opdrachtregelprogramma met functies voor eenvoudige integratie met andere toepassingen. Een schat aan frontend-applicaties en bibliotheken zijn beschikbaar. Versie 2 van GnuPG biedt ook ondersteuning voor S / MIME en Secure Shell (ssh).

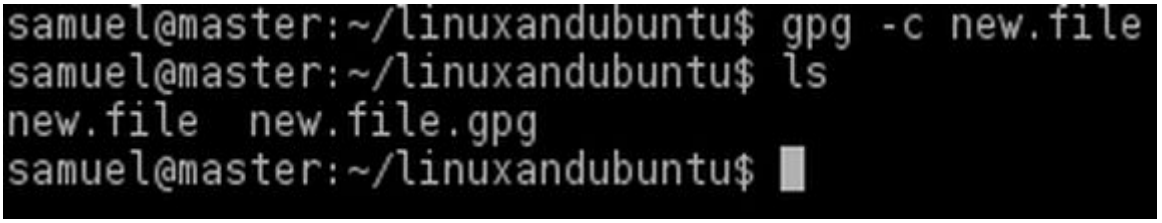
Hoe GnuPG te gebruiken?

Het eerste dat je moet doen voordat je GPG gebruikt, is door het te installeren. GnuPG is beschikbaar voor elk besturingssysteem, zelfs als u het op Mac OSX of Windows kunt gebruiken.

Sommige Linux-distro's hebben standaard GnuPG geïnstalleerd, maar als je distro het niet geïnstalleerd heeft, kun je het door de pakketbeheerder halen of het vanuit de broncode compileren.

voorbeeld:

Ik heb een bestand gemaakt met de naam "new.file" en ik wil het coderen, dus ik moet gpg gebruiken als de volgende manier -



U kunt zien dat ik nu het versleutelde bestand "new.file" heb.
gpg "en als ik de inhoud ervan wil zien zonder het te decoderen, kan ik het niet doen.

Als een bestand is gecodeerd, kan elke gebruiker de inhoud ervan alleen zien als hij het wachtwoord kent. Dus ik ga het ontsleutelen met behulp van de volgende opdracht:

Dit is niet de beste manier om een bestand te versleutelen, omdat het gebaseerd is op het gebruik van een symmetrische sleutel.
GPG heeft een betere manier om te coderen met behulp van asymmetrische sleutels.

Ik denk dat GnuPG de beste manier is om bestanden te coderen in Linux om drie redenen:

1. Het ondersteunt asymmetrische sleutels.
2. Het ondersteunt de RSA- en DSA-algoritmen.
3. Het is gratis.

d) Voor welke andere onderdelen/systemen zou je nog encryptie kunnen gebruiken?

- Encryptie voor chatdiensten die end-to-end-encryptie gebruiken om berichten te versleutelen.
- USB flash drive encryptie zodat belangrijke en gevoelige data bij diefstal of verlies niet kan worden bekeken.

2) Geef mij een kort overzicht van enkele software producten/methoden (gratis of betalend) die per onderstaand deel kan gebruikt worden om je te beschermen. En dit zowel voor windows als linux.

	Windows	Linux
a) Virus	comodo, Windows Defender	eset, sophos

b) Malware	BitDefender Antivirus Free Edition	ClamAV
c) Surfen	Web of Trust (MyWOT), expressvpn	Tails, whonix, vpn: NordVPN
d) Firewall	comodo, ESET Smart Security (Shareware), Windows Firewall.	ClearOS

3) Welke combinatie van software zou jij voorstellen om te gebruiken op een
   a) Windows gebaseerde computer

een antivirus en firewall zoals die van comodo en een betrouwbare browser met de extensie web of trust geinstalleerd + een virtueel particuliere netwerk van bv. expressvpn.

   b) Linux gebaseerde computer

opensource antivirus engine voor detecteren van trojans, virussen, malware en andere bedreigingen zoals die van ClamAV + een virtueel particuliere netwerk van bv. NordVPN + als firewall ClearOS.

bronnen;

https://computertotaal.nl/artikelen/pc/de-ingebouwde-encryptietool-van-windows-10-gebruiken/

https://technet.microsoft.com/en-us/library/cc700811.aspx

https://wiki.archlinux.org/index.php/GnuPG#Installation

http://www.linuxandubuntu.com/home/ways-to-encrypt-files-in-linux
https://wiki.archlinux.org/index.php/Disk_encryption#Available_methods