1. Popište jaké nebezpečí vás může potkat na síti

Na síti vás mohou potkat různá nebezpečí, mezi která patří:

Malware: škodlivý software, jako viry, červi, trojské koně, ransomware apod., který může poškodit nebo odcizit vaše data, infikovat systém nebo zpomalit počítač.

Phishing: podvodné techniky, které se snaží získat citlivé informace, jako jsou hesla, bankovní údaje, sociální zabezpečení, tím, že se vydávají za důvěryhodné entity.

Útoky na síťovou infrastrukturu: útoky, které cílí na infrastrukturu sítě, jako jsou směrovače, přepínače, firewally, s cílem narušit nebo přerušit provoz sítě.

Útoky na služby: útoky, které cílí na konkrétní služby, jako jsou webové servery, e-mailové servery, databáze, s cílem odcizit data nebo narušit provoz.

Únik dat: neoprávněné odhalení nebo odcizení citlivých dat, jako jsou osobní údaje, obchodní tajemství, bankovní informace apod.

Sociální inženýrství: manipulace s lidmi za účelem získání jejich citlivých informací nebo přístupu k systémům.

2. Popište základní pravidla chování v sítí.

Základní pravidla chování v síti zahrnují:

Používání silných a unikátních hesel pro přístup k účtům.

Pravidelné aktualizace a zabezpečování operačního systému a softwaru.

Ochrana přenosných zařízení (mobilní telefony, notebooky) heslem nebo šifrováním dat.

Otevírání a stahování pouze souborů a e-mailových příloh z důvěryhodných zdrojů.

Ochrana sítě pomocí firewallu a antivirusového softwaru.

Opatrné zacházení s citlivými informacemi a vyhýbání se jejich sdílení na nezabezpečených místech.

Monitorování a logování síťového provozu pro odhalování neobvyklých aktivit.

Pravidelná zálohování dat pro zajištění obnovení v případě ztráty nebo poškození.

3. Co je to SSH protokol a jak funguje.

SSH (Secure Shell) je síťový protokol, který slouží k zabezpečenému připojení a komunikaci mezi dvěma zařízeními. SSH umožňuje šifrování dat, autentizaci uživatele pomocí veřejných a privátních klíčů a vzdálené spravování zařízení. Funguje na principu asymetrického šifrování, kde je vytvořen pár veřejného a privátního klíče. Veřejný klíč je distribuován na server, zatímco privátní klíč je uložen na zařízení uživatele. Při připojení pomocí SSH jsou data šifrována pomocí veřejného a privátního klíče, což zajišťuje bezpečnou komunikaci.

4. Co je to DOS útok, popiš 2 způsoby DOS útoku?

DOS (Denial of Service) útok je typ útoku, který má za cíl přetížit nebo vyřadit z provozu služby nebo systémy, aby byly nedostupné pro legitimní uživatele. Existuje mnoho způsobů, jak provést DOS útok, zde jsou dva z nich:

Útok na vrstvu síťového připojení: útočník zaplavuje síťové spojení cílového serveru velkým množstvím neplatných nebo zfalšovaných paketů, čímž vyčerpává šířku pásma nebo systémové prostředky.

Útok na vrstvu aplikačních protokolů: útočník zasílá cílovému serveru velké množství požadavků na zpracování, jako jsou HTTP požadavky nebo žádosti o vytvoření připojení, čímž vyčerpává systémové prostředky a způsobuje přetížení.

5. Jak lze zaútočit na DNS, co může útočník způsobit?

Útoky na DNS (Domain Name System) mají za cíl narušit nebo poškodit fungování systému DNS. Útočník může provést různé typy útoků, jako jsou:

DoS útoky na DNS server: Útočník zaplavuje DNS server velkým množstvím požadavků, čímž vyčerpává jeho zdroje a způsobuje nedostupnost pro legitimní uživatele.

DNS cache poisoning: Útočník manipuluje s obsahem cache DNS serveru, aby přesměroval dotazy na nelegitimní adresy, což může vést k přesměrování uživatele na falešné webové stránky nebo k odcizení citlivých informací.

DNS spoofing: Útočník poskytuje falešné nebo zfalšované odpovědi na dotazy DNS, čímž může přesměrovat uživatele na nebezpečné webové stránky nebo sledovat jejich komunikaci.

6. Co je to spoofing a jak jej lze zneužít?

Spoofing je technika, při které útočník se vydává za legitimního uživatele nebo za jiného síťového uzlu. Útočník může zneužít spoofing pro různé účely, například:

IP spoofing: Útočník upravuje IP adresu zdrojového paketu, aby se zdálo, že pochází od jiného síťového uzlu. Tím se může vyhnout detekci a získat neoprávněný přístup nebo zneužít důvěřivost systému.

E-mail spoofing: Útočník mění odesílatele e-mailu tak, aby se zdálo, že pochází od jiné osoby nebo organizace. Tím může vést k sociálnímu inženýrství nebo podvodu.

ARP spoofing: Útočník posílá falešné ARP odpovědi, aby se vydával za jiný síťový uzel. Tím může přesměrovat provoz na svůj systém a provádět odposlechy nebo další útoky.

7. Jak se lze bránit zjištění hesla?

Pro ochranu před zjištěním hesla je důležité dodržovat několik bezpečnostních postupů:

Používání silných a unikátních hesel: Hesla by měla obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků. Je také důležité mít pro každý účet jiné heslo.

Dvoufaktorová autentizace: Místo pouhého hesla se používá kombinace něčeho, co uživatel ví (heslo) a něčeho, co uživatel má (například SMS kód na mobilním telefonu).

Používání šifrování: Při komunikaci přes nezabezpečené sítě, jako je veřejné Wi-Fi, je vhodné použít šifrované spojení, například pomocí protokolu HTTPS nebo VPN.

Pravidelná změna hesel: Hesla by měla být pravidelně měněna, aby se minimalizovalo riziko jejich odhalení nebo zneužití.

Ochrana proti odposlechu: Je důležité používat zabezpečené kanály komunikace, jako je šifrovaný e-mail nebo šifrované chatování, aby se minimalizovalo riziko odposlechu hesla.

8. Jaké jsou možnosti anonymizace?

Možnosti anonymizace zahrnují:

Použití VPN (Virtual Private Network): VPN umožňuje vytvořit šifrovaný tunel mezi zařízením uživatele a VPN serverem, který maskuje IP adresu uživatele a chrání jeho identitu při komunikaci přes internet.

Použití anonymního prohlížeče: Existují speciální prohlížeče, jako je Tor, které maskují IP adresu uživatele a směřují jeho provoz přes více serverů, aby bylo obtížné zjistit jeho skutečnou identitu.

Ochrana soukromí na sociálních sítích: Uživatelé mohou nastavit své profily a příspěvky jako soukromé, omezit sdílení osobních informací a používat pseudonymy namísto skutečných jmen.

9. Co je dobré filtrovat na firewallu a co by se filtrovat nemělo?

Filtrované obsahy na firewallu by měly zahrnovat:

Nebezpečný nebo škodlivý provoz: Firewall by měl filtrovat provoz, který je známý jako nebezpečný, jako jsou útoky typu DoS, malware nebo phishingové webové stránky.

Nepovolený přístup: Firewall by měl filtrovat přístup z neznámých nebo nedůvěryhodných zdrojů a blokovat neoprávněné pokusy o přístup ke zdrojům v síti.

Nevhodný obsah: Firewall by měl umožnit filtrování webového obsahu na základě kategorií, jako jsou hazardní stránky, pornografie, násilí apod., aby se minimalizovalo riziko exponování uživatelů nevhodnému obsahu.

Některé věci, které by se filtrovat neměly, zahrnují:

Legitimní provoz: Firewall by neměl blokovat legitimní provoz a služby, které jsou nezbytné pro běžnou činnost organizace.

Aktualizace a zabezpečení: Firewall by neměl blokovat aktualizace softwaru, antiviru nebo jiného zabezpečovacího softwaru, které jsou nezbytné pro udržení bezpečnosti systému.

Oprávněný přístup: Firewall by neměl blokovat oprávněný přístup zaměstnanců nebo uživatelů k potřebným zdrojům v síti.

10. K čemu všemu se dá použít v bezpečnosti HASHování (stačí 3 použití)?

Hashování je proces převodu vstupních dat (textový řetězec, soubor) na pevně dlouhý a jedinečný výstup, který je známý jako hash. Hashování se používá pro různé účely v bezpečnosti, jako jsou:

Ověření integrity dat: Hashování umožňuje ověřit, zda se data nezměnila od okamžiku, kdy byla vytvořena hash hodnota. Porovnáním hash hodnoty původních dat s vypočítanou hash hodnotou lze zjistit, zda došlo ke změnám.

Ukládání hesel: Hashování se často používá k ukládání hesel uživatelů. Namísto ukládání samotných hesel jsou uloženy jejich hash hodnoty. Při ověřování hesla se porovnává hash hodnota uložená v databázi s vypočítanou hash hodnotou zadaného hesla.

Digitální podpisy: Hashování se používá při vytváření digitálního podpisu, kde je hash hodnota vytvořena ze zprávy a následně je šifrována soukromým klíčem. Tím se zajišťuje autentičnost a nezpochybnitelnost zprávy.

11. Co je to certifikační autorita, co všechno poskytuje?

Certifikační autorita (CA) je důvěryhodná organizace, která vydává digitální certifikáty. CA zajišťuje, že certifikáty jsou platné a důvěryhodné. Certifikační autorita poskytuje následující služby:

Vydávání certifikátů: CA vydává digitální certifikáty, které obsahují informace o identitě subjektu (např. webové stránky, e-mailového serveru) a jeho veřejný klíč.

Ověřování a revokace certifikátů: CA provádí ověření identity subjektu před vydáním certifikátu a má pravomoc jejich zrušení (revokace) v případě, že certifikát byl zneužit nebo je již neplatný.

Hierarchická struktura důvěry: Certifikační autority jsou organizovány do hierarchické struktury, kde existuje kořenová CA a další podřízené CA. Tím se zajišťuje důvěryhodnost certifikátů a jejich vzájemné ověřování.

12. V jaké souvisí certifikát, veřejný klíč a privátní klíč?

Certifikát, veřejný klíč a privátní klíč jsou součástí asymetrické kryptografie (používající pár klíčů - veřejný a privátní). Veřejný klíč je sdílen s ostatními uživateli a slouží k šifrování zpráv nebo ověřování digitálních podpisů. Privátní klíč je držen pouze jedním uživatelem a slouží k dešifrování zpráv nebo vytváření digitálních podpisů.

Certifikát je digitální dokument vydávaný certifikační autoritou, který obsahuje veřejný klíč a identifikační informace o subjektu (osoba, organizace). Certifikát slouží k ověření identity subjektu a důvěryhodnosti veřejného klíče. Je podepsán soukromým klíčem certifikační autority, čímž se zajišťuje jeho autenticita.

13. Při digitálním podpisu emailu, co se posílá a kdo jaké klíče používá?

Při digitálním podpisu e-mailu se zasílá:

E-mailová zpráva: Obsah e-mailu, který má být podepsán.

Hash hodnota zprávy: Hash hodnota e-mailové zprávy je vypočítána a zašifrována soukromým klíčem odesílatele.

Digitální podpis: Výsledná šifrovaná hash hodnota je připojena k e-mailu jako digitální podpis.

K příjmu e-mailu je potřeba veřejný klíč odesílatele, který je použit k ověření digitálního podpisu. Příjemce dešifruje podpis pomocí veřejného klíče a porovnává vypočítanou hash hodnotu s přijatou hash hodnotou. Pokud se shodují, znamená to, že e-mail nebyl po cestě změněn a pochází od odesílatele, který vlastní odpovídající soukromý klíč.

14. Co je to proxy?

Proxy je server, který funguje jako prostředník mezi klientem a cílovým serverem. Klienti se připojují k proxy serveru a požadují po něm určité služby, jako je přístup k webovým stránkám, stahování souborů nebo odesílání e-mailů. Proxy server poté přijímá tyto požadavky a předává je dále na cílové servery.

Proxy server může plnit několik funkcí, včetně zajištění anonymního přístupu k internetu, filtrování obsahu, zvýšení výkonu sítě a zvýšení bezpečnosti. Prostřednictvím proxy serveru lze kontrolovat a regulovat přístup klientů k různým zdrojům a poskytovat vrstvu ochrany mezi klienty a cílovými servery.

15. Jak zabráníte přístupu zaměstnancům na určité webové stránky?

Existuje několik způsobů, jak zabránit přístupu zaměstnancům na určité webové stránky:

Nastavení filtrování obsahu na firemním firewallu nebo proxy serveru. Pomocí konfigurace filtrů lze omezit přístup na základě URL adres, klíčových slov, kategorií webů nebo dalších parametrů.

Využití specializovaného softwaru pro správu a kontrolu internetového přístupu zaměstnanců. Tyto nástroje umožňují vytvářet seznamy povolených a zakázaných webů a poskytují pokročilé funkce pro monitorování a správu přístupu.

Vytvoření interní politiky a směrnice týkající se internetového používání zaměstnanců. Tato směrnice by měla obsahovat pravidla a doporučení pro správné používání internetu v pracovním prostředí.

16. Jak lze logovat provoz na síti?

Pro logování provozu na síti lze využít několik nástrojů a technik:

Použití logovacích funkcí a nástrojů v síťových prvcích, jako jsou směrovače, přepínače, firewall a proxy servery. Tyto zařízení umožňují záznam událostí a provozu v síti, který lze následně analyzovat a monitorovat.

Nasazení specializovaného softwaru pro správu sítě a logování, jako jsou systémy správy událostí a informační bezpečnosti (SIEM). Tyto nástroje shromažďují a analyzují logovací záznamy z různých zdrojů a umožňují detekci anomálií

a hrozeb v síti.

Konfigurace a nasazení softwarových nástrojů pro sledování síťového provozu a analýzu paketů, například Wireshark. Tyto nástroje umožňují detailní analýzu síťového provozu na úrovni jednotlivých paketů a umožňují odhalování problémů a chyb v síťové komunikaci.

17. Jak lze odhalit DOS útok?

Odhalování DOS (Denial of Service) útoků může být složité, ale existují některé přístupy a techniky:

Monitorování síťového provozu a analýza anomálií. DOS útoky obvykle způsobují vysokou zátěž na sítě, což lze detekovat sledováním a analýzou síťového provozu. Pokud je identifikována neobvykle vysoká aktivita z jednoho nebo více zdrojů, může to naznačovat DOS útok.

Použití systémů detekce a prevence útoků (IDS/IPS). Tyto systémy jsou navrženy k odhalování a blokování různých typů útoků, včetně DOS útoků. IDS/IPS systémy monitorují síťový provoz a aplikují různé algoritmy a pravidla pro detekci a prevenci útoků.

Spolupráce s poskytovateli služeb a využití jejich infrastruktury pro detekci a ochranu před DOS útoky. Poskytovatelé služeb (ISP) obvykle mají monitorovací a obranné mechanismy na svých síťových zařízeních, které mohou pomoci detekovat a eliminovat DOS útoky směřující na vaši síť.

18. Jak lze odhalit přístup do systému neznámou osobou?

Odhalení neoprávněného přístupu do systému neznámou osobou může zahrnovat několik kroků a postupů:

Monitorování logovacích záznamů a sledování neobvyklých aktivit. Záznamy o přihlášení, používání systému a souborových operacích mohou obsahovat informace o neoprávněném přístupu. Monitorování a analýza těchto záznamů může odhalit podezřelou činnost.

Nastavení silných uživatelských jmen a hesel. Používání složitých a jedinečných kombinací uživatelských jmen a hesel může snížit riziko neoprávněného přístupu. Dále je důležité vyžadovat pravidelnou změnu hesel a zabránit použití příliš jednoduchých hesel.

Použití dvoufaktorové autentizace. Dvoufaktorová autentizace zvyšuje bezpečnost tím, že vyžaduje dvě nezávislé formy ověření totožnosti, například heslo a jednorázový kód, který je odeslán na mobilní zařízení uživatele.

Nasazení firewallu a bezpečnostních systémů. Správná konfigurace firewallu a dalších bezpečnostních systémů může pomoci odhalit a blokovat neoprávněný přístup. Firewall může být nastaven tak, aby povoloval přístup pouze z autorizovaných sítí a blokoval nepovolené přístupy.

19. Co vše obsahuje certifikát vydávaný certifikační autoritou?

Certifikát vydávaný certifikační autoritou (CA) obsahuje několik důležitých informací:

Informace o vlastníkovi certifikátu, jako je jméno nebo název organizace.

Veřejný klíč, který je spojen s daným certifikátem a slouží k ověření a šifrování komunikace.

Digitální podpis vydavatele certifikátu, který slouží k ověření pravosti certifikátu.

Platnost certifikátu, tj. časové období, po které je certifikát platný.

Identifikace certifikační autority, která certifikát vydala.

Certifikát je vydáván certifikační autoritou a slouží k ověření totožnosti a autentičnosti vlastníka certifikátu. Při použití certifikátu se používá veřejný klíč obsažený v certifikátu pro ověření digitálního podpisu a zajištění bezpečné komunikace.

20. Jak zabezpečit server proti zneužití?

Zabezpečení serveru proti zneužití vyžaduje několik opatření:

Aktualizace a správa softwaru. Pravidelné aktualizace a správa softwaru, včetně operačního systému a aplikací, jsou klíčové pro odstranění známých zranitelností a zabezpečení proti novým hrozbám.

Použití silných hesel a autentizace. Používání silných a jedinečných hesel pro přístup ke serveru je důležité. Dále je vhodné implementovat dvoufaktorovou autentizaci pro zvýšení bezpečnosti.

Nastavení firewallu a správa přístupových práv. Správná konfigurace firewallu a správa přístupových práv mohou omezit neoprávněný přístup ke serveru.

Monitorování a logování provozu. Monitorování provozu na serveru a

logování událostí může pomoci odhalit podezřelou aktivitu a rychle reagovat na hrozby.

Zálohování dat. Pravidelné zálohování dat je důležité pro obnovení serveru v případě havárie nebo útoku.

Použití šifrování. Použití šifrování dat při přenosu a uložení může pomoci chránit citlivé informace před neoprávněným přístupem.

21. Jak zabezpečit domácí počítač proti zneužití?

Pro zabezpečení domácího počítače proti zneužití lze přijmout následující opatření: Instalace antivirového softwaru a pravidelné aktualizace. Antivirový software pomáhá detekovat a odstraňovat škodlivý software a malware. Je důležité pravidelně aktualizovat antivirový software, aby byl schopen rozpoznat nejnovější hrozby. Aktualizace operačního systému a aplikací. Pravidelné aktualizace operačního systému a aplikací jsou důležité pro odstranění zranitelností a zajištění bezpečnosti počítače.