**Test znalostí TCP/IP pomocí Wiresharku**

|  |  |  |
| --- | --- | --- |
| **Úkol** | **Použité soubory** | **Znění úkolu** |
| 1. | arp\_resolution.pcap  arp\_gratuitous.pcap | 1. Porovnejte gratuitous (nevyžádaný) ARP se standardním požadavkem ARP. V čem se liší? 2. Kdy se s gratuitous ARP lze nejčastěji setkat? 3. K čemu ho lze zneužít? 4. Proč je ARP komunikace jedna z mála nešifrovaných? |
| 1.  2.  3.  4. | | |
| 2. | ip\_ttl\_source.pcap  ip\_ttl\_dest.pcap | 1. Kolik směrovačů se nachází mezi odesilatelem paketu s adresou 10.10.0.3 (odchytil soubor ip\_ttl\_source.pcap) a příjemcem s adresou 192.168.0.128 (odchytil soubor ip\_ttl\_dest.pcap)? 2. Jak jste to poznal/poznala? |
| 1.  2. | | |
| 3. | ip\_frag\_source.pcap | 1. Na kolik fragmentů jsou pakety fragmentovány? 2. Jak poznáte, že jde o fragment a že budou následovat další fragmenty? 3. Jak by bylo možné fragmentaci použít pro útok na směrovač, který proti tomuto útoku není chráněn? |
| 1.  2.  3. | | |
| 4. | tcp\_ports.pcap | 1. Jakým způsobem jsou přidělovány porty klientům, komunikujícím s webovým serverem? 2. Z jakého roku je odchyt? |
| 1.  2. | | |
| 5. | tcp\_handshake.pcap | 1. Které příznaky jsou nastaveny ve druhé fázi handshakingu? 2. 2. Jaké množství dat je během handshakingu přeneseno? |
| 1.  2. | | |
| 6. | tcp\_teardown.pcap | 1. Které příznaky jsou nastavovány během rozvazování spojení? |
| 1. | | |
| 7. | tcp\_refuseconnection.pcap | 1. Jak směrovač Cisco reaguje na pokus o navázání spojení? 2. O kterou službu je žádán? |
| 1.  2. | | |
| 8. | udp\_dnsrequest.pcap | 1. Co kontroluje pole Checksum? 2. Zajišťuje protokol UDP spolehlivé doručení? |
| 1.  2. | | |
| 9. | icmp\_echo.pcap | 1. Podle čeho lze poznat, která odpověď patří ke kterému dotazu? 2. Jak byste zajistili, aby byly tyto příkazy fragmentovány? 3. Jak lze pomocí ICMP paketů zajistit skrytou komunikaci? |
| 1.  2.  3. | | |
| 10. | icmp\_traceroute.pcap | 1. Proč lze 2. paket označit za dvouhlavý (double-headed)? 2. Co 2. paket oznamuje protistanici? |
| 1.  2. | | |
| 11. | dhcp\_nolease\_renewal.pcap | 1. Proč je zde na transportní úrovni použit UDP a ne TCP? 2. Proč v paket zjišťování (discovery) odesílán z adresy 0.0.0.0? 3. Jak zjistí server v procesu nabídky (offer) adresu klienta? 4. Jaká je hodnota masky podsítě, času obnovy, času opakované vazby, času zápůjčky a identifikátor serveru DHCP? 5. Pro je paket posílaný klientem v procesu požadavku (request) opět odeslán z adresy 0.0.0.0? 6. Podle čeho DHCP server pozná, že jde o odpověď na jeho nabídku? 7. Co vykoná DHCP server po odeslání paketu potvrzení (acknowledgement)? |
| 1.  2.  3.  4.  5.  6.  7. | | |
| 12. | dhcp\_inlease\_renewal.pcap | 1. Kdy probíhá obnovení adresy během zápůjčky protokolu DHCP (in-lease renewal)? Uveďte obě situace! 2. V kolika krocích tato obnova adresy probíhá? |
| 1.  2. | | |
| 13. | dns\_query\_response.pcap | 1. Na co se vlastně klient DNS serveru ptá? 2. Kde je v dotazu údaj, že jde o internetovou adresu? 3. Jak se pozná, že se odpověď vztahuje právě k tomuto serveru? |
| 1.  2.  3. | | |
| 14. | dns\_recursivequery\_client.pcap | 1. Na co se klient ptá DNS serveru v prvním paketu? 2. Jak poznáme, že je požadována rekurze (sebeopakování)? 3. V čem se liší rekurze od iterace? Co je zvláštní formou čeho a co je efektivnější? |
| 1.  2.  3. | | |
| 15. | dns\_recursivequery\_server.pcap | 1. Kolik úrovní rekurze zachycuje konverzace? |
| 1. | | |
| 16. | dns\_axfr.pcap | 1. Jaký je obvyklý důvod pro přenos dat (přenos zóny) mezi dvěma zařízeními DNS? 2. Proč se mezi dvěma zařízeními přenáší data ne pomocí UDP, ale pomocí TCP? 3. Jaké riziko představuje přenos tak velkého objemu dat? |
| 1.  2.  3. | | |
| 17. | http\_google.pcap | 1. Ve 4. paketu prohlížeč posílá požadavek na stažení (GET) kořenového adresáře (/) webového serveru pomocí verze 1.1 protokolu http. Jaké další informace o sobě prohlížeč posílá? 2. V kterém paketu potvrzuje webový server úspěšnost odpovědi (kód 200)? |
| 1.  2. | | |
| 18. | http\_post.pcap | 1. Uživatel posílá pomocí metody POST webovému serveru data ke zpracování. V jakém programovacím jazyku je příslušný skript napsán? 2. Jaký je kód odpovědi, v jejímž rámci bude požadavek přesměrován na příslušnou webovou stránku s komentářem? |
| 1.  2. | | |
| 19. | facebook\_login.pcap | 1. Jaké je číslo portu, na který se klient přihlašuje v rámci procesu autentizace služby Facebook? 2. Kolik kryptosad je klientem nabízeno? 3. Který symetrický šifrovací algoritmus je obsažen v serverem vybrané kryptosadě? 4. Po doručení obsahu souboru home.php je připojení použité při autentizaci zrušeno příkazem teardown. Uveďte čísla paketů, kterými je uzavřeno připojení protokolu http na portu 80 a čísla příkazů, kterými je poté uzavřeno připojení HTTPS na portu 443. |
| 1.  2.  3.  4. | | |
| 20. | facebook\_message.pcap | 1. Jaká metoda se používá při přenosu dané soukromé zprávy na Facebook? 2. Metoda AJAX (Asynchronous JavaScript and XML) umožňuje vytvářet interaktivní webové aplikace, které načítají informace ze serveru na pozadí. Zpráva byla odeslána z interaktivního vyskakovacího okna, tedy není přesměrována na konkrétní stránku. Který parametr tedy v ní chybí (viz úloha 18)? 3. Soukromá zpráva je zasílána v zašifrované nebo nezašifrované podobě? |
| 1.  2.  3. | | |
| 21. | twitter\_login.pcap | 1. Uživatelská data pro autentizaci (uživatelské jméno a heslo) jsou přenášena v zašifrované či nezašifrované podobě (viz pole Encrypted Application Data)? 2. V kterém paketu (uveďte číslo) bude autentizace ukončena procesem teardown? 3. Proč se v paketech 19, 21, 22 navazuje nové připojení k serveru na portu 80 a ne 443, jak při autentizaci? 4. Jaká metoda http byla použita (viz paket 23)? |
| 1.  2.  3.  4. | | |
| 22. | twitter\_tweet.pcap | 1. Po přihlášení jsou odesílána data na tweet. Jakým slovem začínají? Je to zcela bezpečné? 2. Jaká metoda http byla použita? |
| 1.  2. | | |