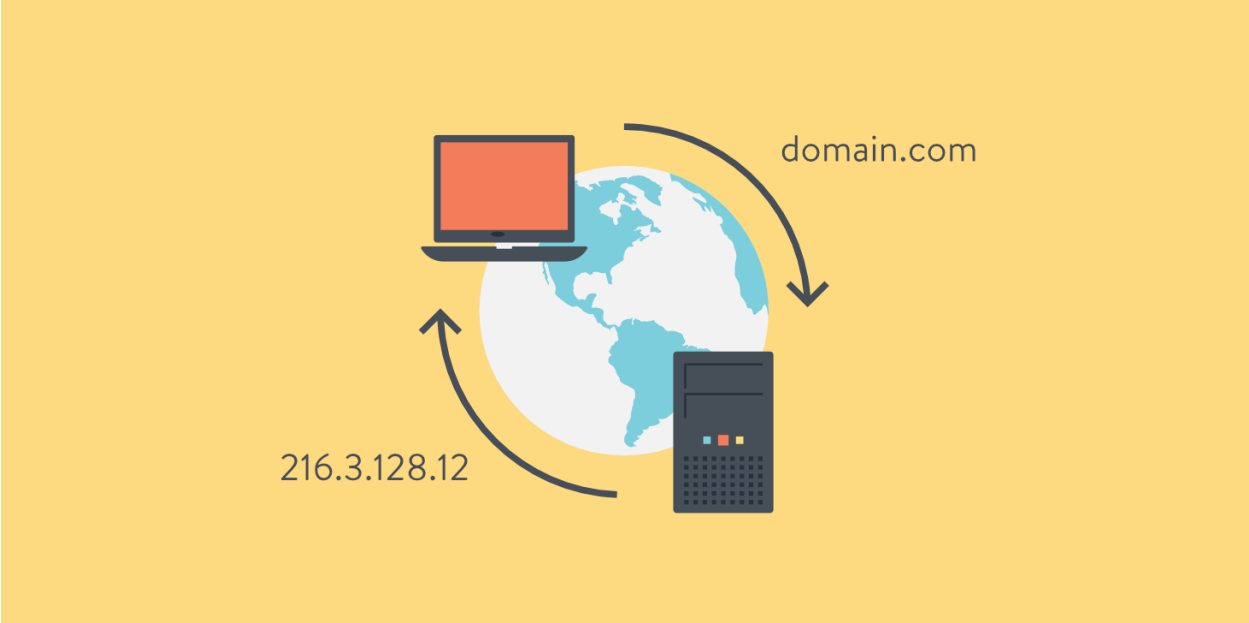
- DNS and its attacks -



- شرح الـ DNS -

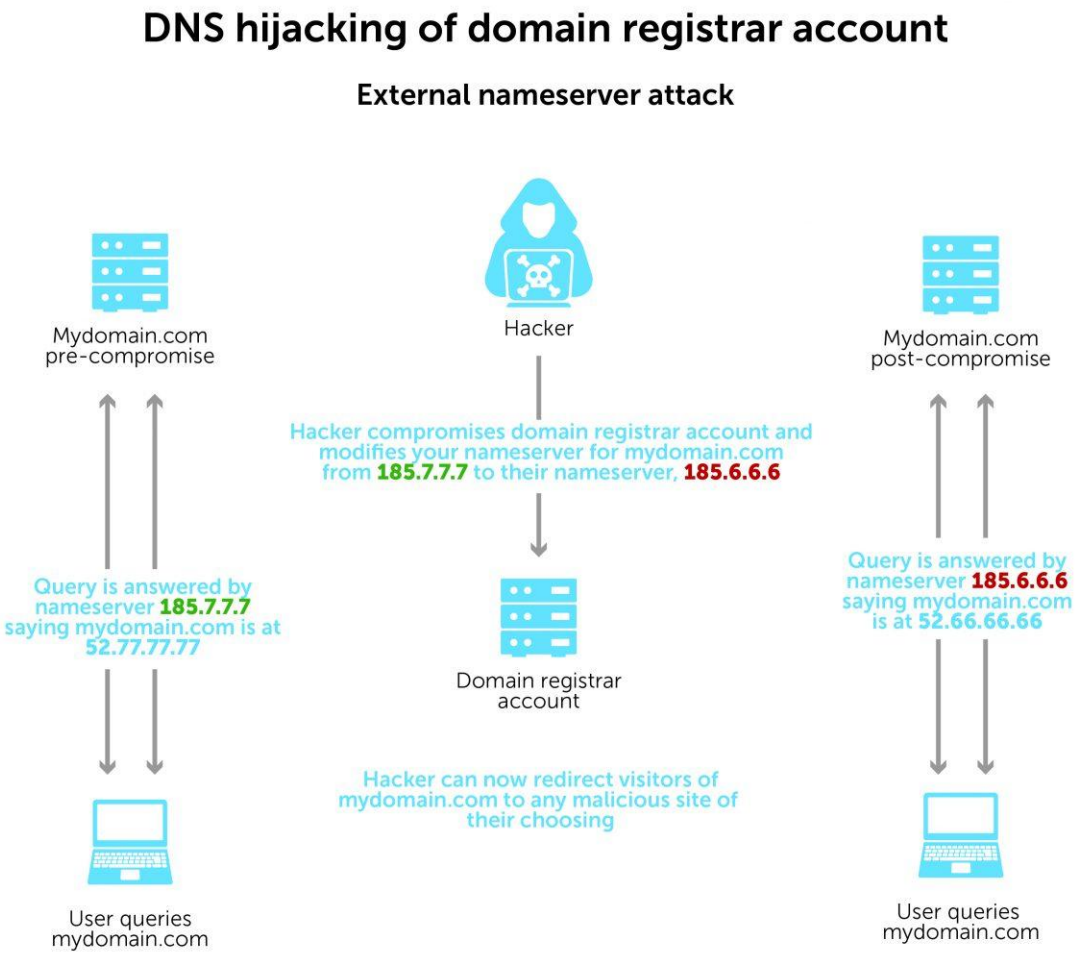
How the DNS works

- شرح هجمات الـ DNS -

- بالرغم من أهمية الـ DNS بس شركات كتير مش بتحب تيجي جنبه او تحاول تعمله update أو تعدل في الـ configuration بتاعته عشان متحصلش مشاكل ويتعطل أو يوقف وبالتالي مواقع هتفضل متوقفة، وبسبب ده بيحصل مجموعة من الهجمات والي هنشرحها واحدة واحدة.

- DNS Hijacking -

- الـ Hackers بيعملوا هاك للـ DNS إما عن طريق إنهم بيغيروا الـ DNS IPs أو عن طريق إنهم يعملوا intercept للريكوست بين الـ Client والـ DNS ويغيروا الـ Destenation بتاع اليوزر لمكان تاني.
- كلمة Hijacking دايما مقصود بيها سرقة شئ ما، وهنا في أنواع من الـ Hijacking:
  - الأول هو Local DNS hijacking: وهنا الـ attacker بيستخدم الـ trojan عشان يقدر يغير إعدادات الـ DNS server بتاع جهاز الـ victim ويحط الـ IP بتاع الـ DNS الخاص بيه وبالتالي يقدر يعمل الي عايزه في ريكوست الـ victim.
  - التاني هو الـ Router DNS hijacking: وهنا هو بيستغل ثغرة موجودة في الرواتر وبعدها بيقدر يغير إعدادت الـ DNS server ويحط الـ IP بتاعه برضو وبكده يقدر يتحكم في ريكوست كل الناس الي موجودة ومتصلة على الراوتر.
  - التالت هو الـ MITM attack hijacking: هنا بيعترض الـ reply الي طالع من الـ DNS ورايح للـ victim بما إن اليوزر طلب مثلا example.com وبعدين الـ attacker بيغير الـ IP بتاع example.com بـ IP تاني تابع ليه ولكن عليه نفس الصفحة وبالتالي الـ victim مش هيشك بما إنه فعلا كتب الدومين صح في المتصفح.
  - الرابع هو Hijacking DNS server: هنا هو بيقدر يتحكم في الـ DNS server - ده بيكون بسبب ثغرة معينة - وبالتالي بيغير كل الـ IPs الي عايزها بـ IPs تابعة ليه وبكده كل الي هيطلب موقع من المواقع الي موجودة على الـ DNS server ده هيتحول لموقع و IP تابع للـ attacker.
- إيه الي ممكن يحققه الـ attacker من هجوم زي ده؟
  - يقدر يعمل phishing page شبيهة بالموقع الأصلي وفيها نفس الـ login page او لو بنك الصفحة هيكون فيها تحويلات بنكية وبالتالي هيقدر يسرق بيانات حساسة.
  - يقدر يعمل redirect للـ victim لصفحة موجودة فيها إعلانات هو بيتربح منها وبالتالي الـ attacker بيكسب فلوس من كل user هيزور الصفحات دي.

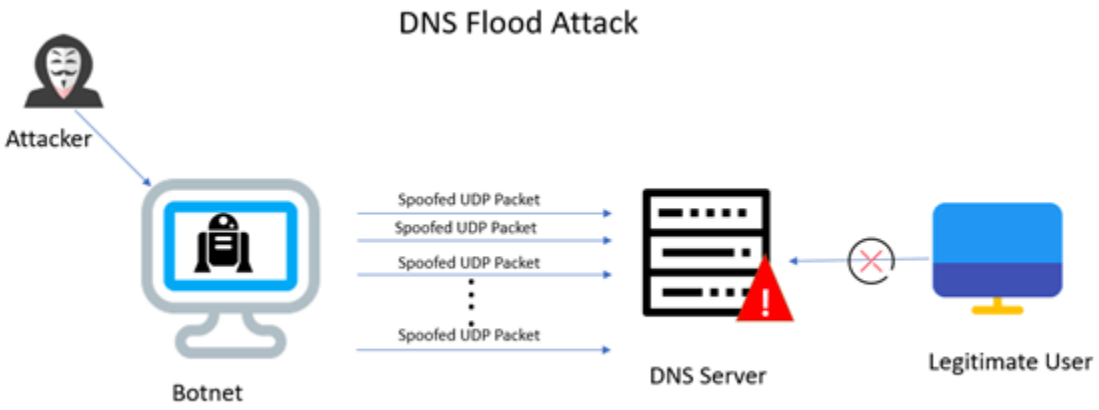


- مصادر لو عايز تتعمق أكتر
- What is DNS Hijacking - How to Protect Yourself?
- Protect your network from DNS hijacking
-

- DNS Flood Attack -

- واحد من الهجمات البسيطة للـ DNS، هنا الـ attacker بيحاول يوقف عمل الـ DNS server خالص.

- الهجوم ده بيتم عن طريق إن الـ attacker بيبعت requests كتير جداً للـ DNS server لحد ما الـ DNS server ميقدرش يتعامل مع كل الـ requests دي ف بالتالي يوقف بسبب الحمل الزيادة الي حصل فجأة.
- الهجوم ده صعب توقفه بما إن كل الـ requests بتكون جاية من Single IP ولكن بيكون صعب لما الـ requests تكون جاية من hosts مختلفة ف التعامل مع إنك توقفها بيكون صعب شوية.

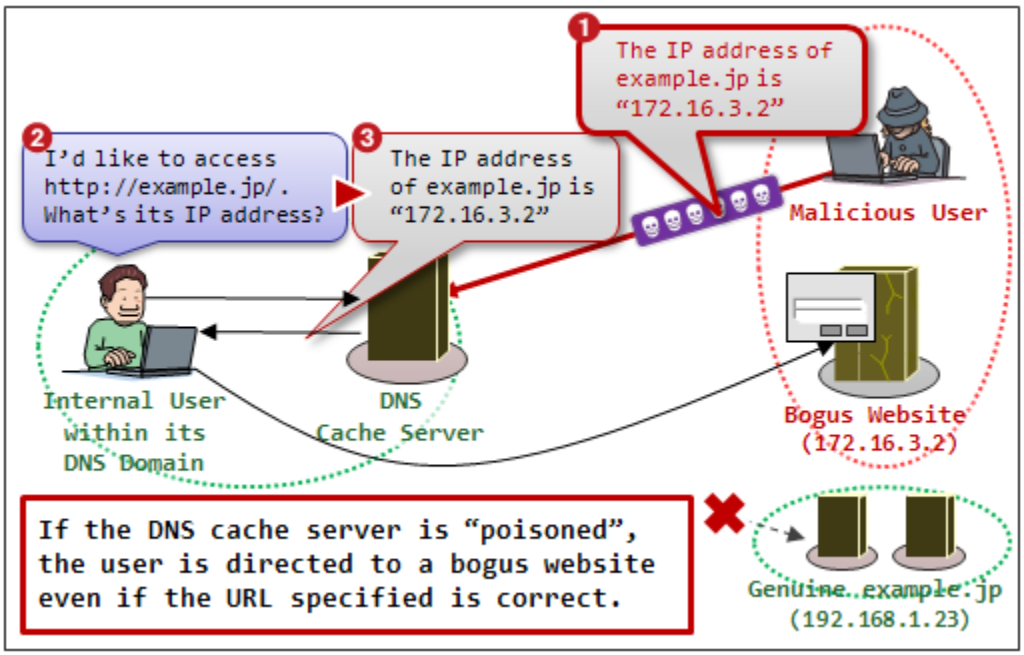


- DNS Cache Poisoning -

- في الأول خلينا نعرف يعني إيه DNS Cache أصلاً؟
  - أول مرة بتيجي تطلب فيها google.com بيروح الـ DNS server يرد عليك بالـ IP بتاع google.com وف نفس الوقت بيحفظ عندك على الجهاز DNS resolver's cache الي هو بالبلدي بدل ما كل شوية تيجي وتسألني وتاخد وقت عشان أرد عليك، لا ده هيكون عندك زي Local DNS فيه إن google.com الـ IP بتاعه كذا، وبالتالي هيكون أسرع وده معنى DNS Cache إن يكون عندك زي نسخة من الـ requests الي عملتها قبل كده وهتكرر كتير.
  - فالـ DNS Cache Poisoning هو إنه بيوصل للـ DNS resolver's Cache الي موجود عندك على الكمبيوتر ويغير فيه ويخلي مثلا إن google.com الـ IP بتاعها حاجة تابعة للـ Attacker وبالتالي لما تطلب google.com الريكوست هيروح للـ DNS resolver's Cache وهنا هتحصل المشكلة إنه هيرجعلك الصفحة الخاصة بالـ IP الي حطه الـ attacker.
  - وبرضو ممكن تحصل عن طريق الآتي:
    - بيتم عن طريق إنك الأول بتعمل ARP Spoofing لجهاز الـ victim وبالتالي أنت دلوقتي بقيت الراوتر, في العادي جهاز الـ victim لما هيكتب مثلا google.com الريكوست هيعدي على الراوتر ومنه للـ DNS Server وبعدين يرجع للراوتر ومنه لجهاز الـ victim, الي بيحصل بقى إن جهاز الـ victim بيكتب google.com وبيعدي الريكوست على الراوتر وللـ DNS server ويجيب

الـ IP، والـ response راجعة لجهاز الـ victim انا هنا بكون عامل الـ ARP Spoofing ومفهم الراوتر إني جهاز الـ victim ف هاخد الـ response واعدل فيها الـ IP بتاع جوجل لـ IP تاني وبعدين الريسبونس تكمل لجهاز الـ victim كأني الراوتر.

- WiFi Wireless Security Tutorial - 14 - Whats is DNS Spoofing and MITM Atta...



- مصادر للنقطة دي:
- DNS Cache Poisoning Attack | Internet Security

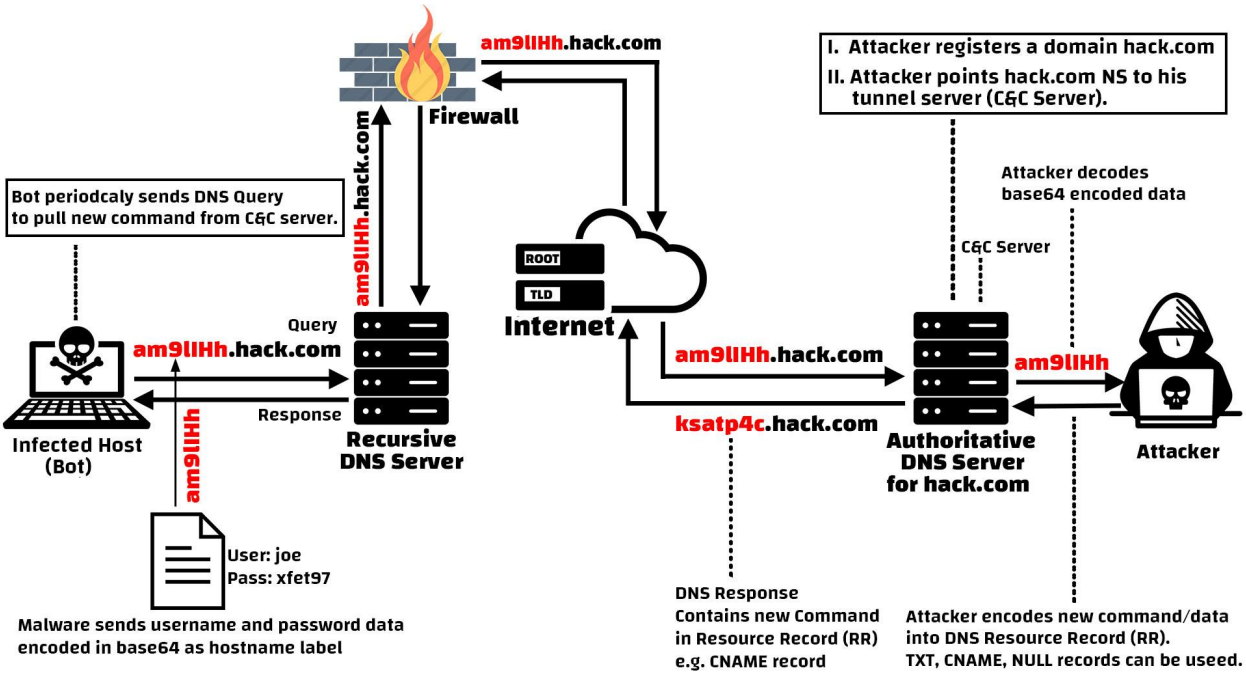
- DNS Spoofing Vs DNS Hijacking -

- الفرق بين الأتنين هو إن:
  - DNS Spoofing: مجرد بيتم تعديل الـ DNS resolver's cache بدون ما يتم التعديل على الـ DNS server نفسه، وهنا تعمل redirect للـ victim لـ malicious websites.
  - إنما الـ DNS Hijacking: بيمكنك إنك تقدر تعدل في الـ DNS server عن طريق malware وبيخليك تحط fake DNS server وفيه fake IPs بتوديك لـ malicious websites.

- يعني غالبا الهدف بيكون واحد وهو إنك توصله لـ malicious website أو phising website ولكن الطريقة بتختلف.

- DNS Tunneling -

- بإختصار هو إننا بنستخدم الـ DNS كـقناة نقدر ننقل فيها الداتا من جهاز الـ victim لجهاز الـ attacker.
- الـ DNS Tunneling مش هجوم في حد ذاته ولكن تكنيك عشان يقدر يعمل Bypass للـ Firewalls.
- الـ DNS مش مُستخدم لغرض نقل الداتا وبالتالي صعب إن حد يشك إن في داتا بيتم نقلها عن طريق البروتوكول ده (DNS).
- الهجوم بيحصل عن طريق إن الـ attacker بيكون عنده Local DNS أو Authority DNS والـ victim بيعمل query للـ DNS الخاص بالـ attacker بيسأل عن موقع معين ولنفترض example.com، ف الـ attacker بيخليه يبعت الداتا في الـ query request زي Administration.example.com وهنا نلاحظ إن أول كلمة هي Administration وهي عبارة عن الـ current user في الـ victim system وطبعا يقدر ينقل حاجات تاني كتير.



- تقدر تعرف أكتر عن الموضوع من هنا:
  - DNS tunneling down the rabbit hole
  - QTNA #21: DNS Tunneling

- DNS Tunneling Attack

- Random Subdomain Attack -

- حاجة شبيهة بالـ DDOS Attack وليهم نفس الهدف، لكن هنا الـ queries مش بتكون للـ Domain name server نفسه ولكن بتكون للـ subdomains مش موجودة والـ attack غالبا بيحصل من botnet من users هما مش عارفين إنهم بيبعتوا الـ requests دي، ف بيبقى صعب تعمله detect.

- NXDOMAIN attack -

- حاجة شبيهة بالي فوق بس الـ queries بتروح لـ Non-exesting domains وبالتالي بسبب عدد الـ requests الكتيرة بيحصل توقف للـ DNS server بتاعك.

- دي كانت مجموعة من الهجمات الي بتحصل على الـ DNS وبإختصار شديد، ف تقدر تدور على كل واحدة فيهم وتبحث أكتر وتعرف أكتر عنهم.
- ولو انت Pentester فاللينك الي تحت بيفهمك ازاي تعمل DNS enumeration ودي خطوة مهمة في الـ Recon
-

- https://securitytrails.com/blog/dns-enumeration