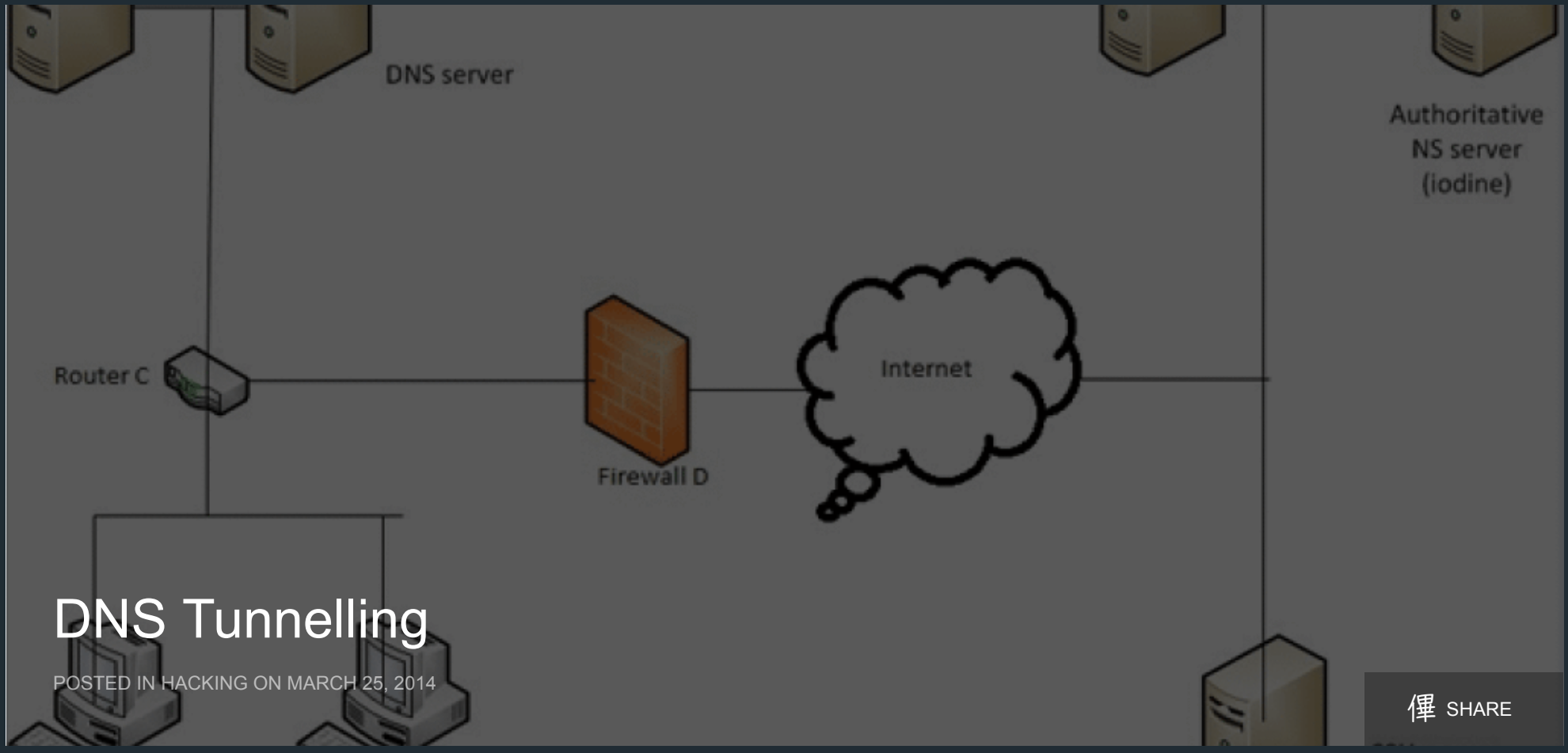


DNS Tunnelling

POSTED IN HACKING ON MARCH 25, 2014

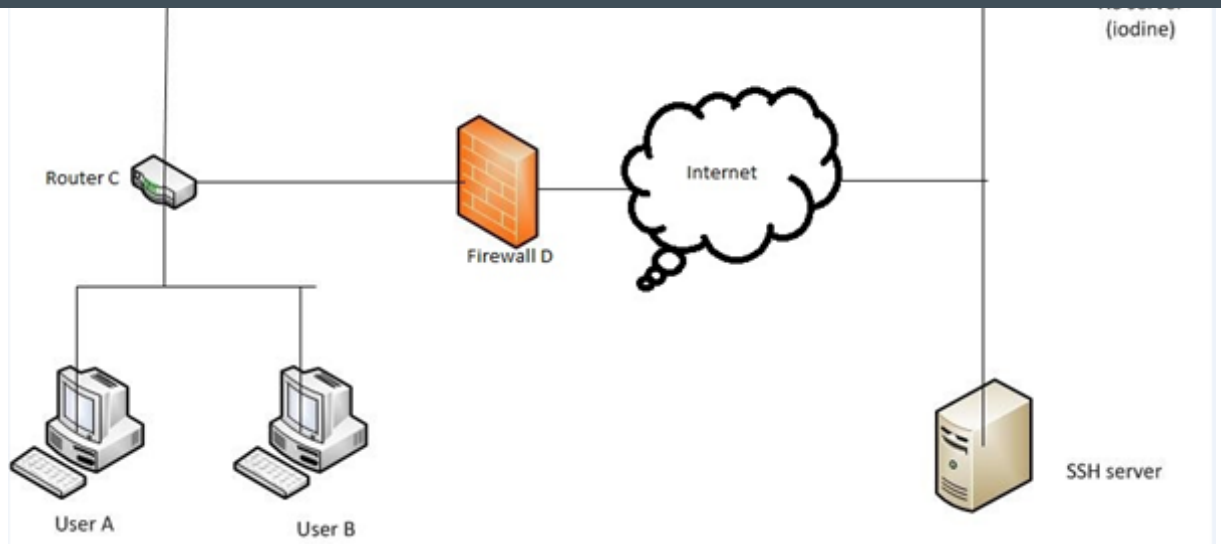
test.

You all know what DNS is, and I don't think any more information is needed on it. Our Internet world exists due to DNS technology, and exploiting DNS can bring down the Internet for a day or month, or in a particular region. One of the common attacks that we heard about in 2012 was Operation Global Blackout, wherein the attacker 'Anonymous' threatened to take down the complete global Internet. Computer security experts were worried and have taken additional layers of protection to secure the network, particularly DNS.

Have you ever come up to a scenario where you were not able to access a website because it was blocked by proxy? Then you need to use DNS tunnelling concepts to bypass the proxy.

By using DNS tunnelling, a user will be able to access a website even though the proxy is blocking the website. Normally when you consider a proxy server, all the HTTP traffic will be received by a proxy server, but no DNS traffic will fall on a proxy server. So exploiting this DNS traffic will allow us to use all blocked websites as well.

So on a DNS tunnel, data are encapsulated within DNS queries and replies, using base32 and base64 encoding, and the DNS domain name lookup system is used to send data bi-directionally. Therefore, as long as you can do domain name lookups on a network, you can tunnel any kind of data you want to a remote system, including the Internet. We use DNS records (NULL/TXT/SRV/MX/CNAME) to encapsulate (downstream) IP traffic.



In the above scenario, Users A and B are behind a corporate firewall D, and no websites are allowed from Users A and B, and only traffic via port 53 is allowed from firewall D. User A and User B can use the Internet by exploiting DNS traffic via DNS tunnelling. The DNS server on the left side has a caching capability, so when user A tries to access any websites that are already in the cache, then the request won't go to the iterative server. If some new request is initiated from User A, then the DNS server will not find its A record in the DNS server, so it will send to an outside DNS server. The maximum length of a DNS query is 255 characters with a limitation of 63 chars per label and is in the form: label3.label2.label1.example.

To tunnel data over DNS, we need control of an external DNS server (in our case, the DNS server to the right), and we add two records on the external DNS server. One is NS record and the other is A record. NS (name server) record allows you to delegate a subdomain of your domain to another name server. So if you have a domain laptop.com you can add a NS record like a.laptop.com NS computer.com which means any DNS query to laptop.com will be delegated to computer.com and its subdomains. The other one is the A record, which contains the IP address mapping to domain name.

However, botnets can use DNS tunnelling to act as a covert channel, and these covert channels are very hard to detect. These can be identified only by looking for any C&C information on the DNS in the covert channel. In all network systems nowadays DNS is served as it is, but protocols like HTTP, FTP are one of many methods to analyse and inspect the traffic. So the botnets using DNS tunnelling have a better scope for malware writers. The following are some DNS tunnelling tools:

DNS TUNNELLING TOOLS
OzymanDNS
Dns2tcp
Iodine
Heyoka
DNSCat
NSTX
DNScapy
MagicTunnel, Element53, VPN-over-DNS (Android)
VPN over DNS

In DNS tunnelling, requests from the clients will be fragmented and will be sent as separate DNS queries. Likewise, reply traffic will also need to be fragmented. DNS uses UDP rather than TCP, so fragmentation and correct assembly need to be done in a fake server.

DNS tunnels are commonly used to carry out covert file transfers, C&C server traffic and web browsing. File transfer via DNS is likely to use the DNS traffic aggressively considering the DNS protocol and the encapsulation overhead for transferring data over the tunnel. The C&C server traffic will carry minimal traffic as there will be only usual traffic patterns observed. Web browsing using a DNS tunnel is a mixture of both the above.

- DNS tunnelling can be detected by monitoring the size of DNS request and reply queries. It's likely that tunnelled traffic will have more than 64 characters in DNS.
- Use of updated IPS and IDS is another detection mechanism.
- Rules must be configured to monitor a large number of DNS TXT in a DNS server.
- Rules must be configured in SIEM to trigger if volume of DNS traffic from a particular source is very high.
- Another method is to use the split horizon DNS concept so that internal addresses are dealt on a specific server; clients should use a proxy server to connect out to the internet, and the proxy server resolves the external DNS for them. Some proxies also have the capability to check the DNS information too.
- DNSTrap is a tool developed to detect DNS tunnelling by using artificial neural network. In this tool, five attributes are used to train an Artificial Neural Network (ANN) to detect tunnels: the domain name, how many packets are sent to a particular domain, the average length of packets to that domain, the average number of distinct characters in the LLD, and the distance between LLD's.
- Next generation firewalls like Paloalto and Fire Eye have the capability to detect DNS tunnelling.

References

http://psichron.za.net/downloads/dns_tunneling.txt

http://www.splitbrain.org/blog/2008-11/02-dns_tunneling_made_simple

http://arxiv.org/ftp/arxiv/papers/1004/1004.4358.pdf

AUTHOR

Ryan Mazerik

Ryan has over 10yrs of experience in information security specifically in penetration testing and vulnerability assessment. He used to train and mentor consultants of these offerings to expand security delivery capabilities.He has strong passion in researching security vulnerabilities and taking sessions on information security concepts.

- Free BEC eBook: The Great White Shark of Social Engineering
- The CISSP CBK Domains: Information and Updates
- How to Protect Yourself From GDPR-Related Phishing Scams
- Shodan and IoT: The Problem is here!
- How Criminals Can Exploit AI
- New! PhishSim Auto Reports Dashboard & Cryptocurrency Phishing Templates
- How to Prevent BEC With Email Security Features
- How to Prevent BEC with Vendor Payment Integration
- 4 Ways to Integrate BEC Prevention Strategies into Your Organization
- Cooperation between Humans and Artificial Intelligence in the Name of Security
- Exploiting NFS Share
- CGEIT Domain 3: Benefits Realization
- CGEIT Domain 2: Strategic Management

Security Awareness

DoD 8140

Ethical Hacking

Hacker Training Online

CCNA

PMP

Microsoft

Incident Response

Information Assurance

MORE POSTS BY AUTHOR

DDoS on UPNP Devices

ScanBox Framework

Save Our Souls (SOS)

(mailinator.com).
Where dnscapy clients can retrieve the ip list and access a miniweb.exe website.(trickle charge web hosting)
While running a dnscapy server at the same time
Creating a mini world wide web.
The screensaver internet(water drop bucket).
Failed to convert ozymandns to php(it would be nice to add that as a wapsite plugin)
Thank you (hindsight)
end of essay.
Reply
Leave a Reply
Your email address will not be published. Required fields are marked *

Comment
Name *
Email *
Website
6 × 3 =
Post Comment