International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 2, Apr 2015, 97-102

TOR: PREVENT DNS LEAK THROUGH HONEYPOT

SUMAN GAUTAM[1], NITESH GUPTA[2] & SINI SHIBU[3]

[1]Department of CSE, NIIST (Affiliated to RGPV), Bhopal, Madhya Pradesh, India

[2,3]Asisstant Professor, Department of CSE, NIIST (Affiliated to RGPV,) Bhopal, Madhya Pradesh, India

ABSTRACT

Today, DNS/IP leakage in major problem of cyber crime world. In TOR, DNS are leaked easily in the time duration of whole communication between client and server and many users can't realise these types of hazard. So, attacker takes advantages of this system when it's reached the original IP of client and done much crime through other identity. In this paper we try to do new research in the world of cyber crime for rectified the problem. We are going to introducing the HONEYPOT in a TOR browser. Honey pot is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honey pot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. This is similar to the police baiting a criminal and then conducting undercover surveillance.

KEYWORDS: TOR, HONEYPOT, DNS, PROXIES