International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Cyber-Terrorism and Network Vulnerabilities: A Review

Rahul Kaushik[1], Vicky [2]
[1]Assistant Professor, Department of Computer Science, BG. D.C. Memorial College, Bahal
[2]Research Scholar M.D. University, Rohtak

Abstract: Invention of internet has been proving itself a boon for the society. With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. We all are aware of cybercrimes which are happening as a result of increasing internet usage; popular ones are phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, and child pornography, kidnapping children via chat rooms, scams and many more. There exists a more dangerous form of attack known as Cyber-Terrorism. Cyber-terrorism is the use of Internet attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses. Cyber-terrorism has much more adverse affects not only on an individual but to nations worldwide. Terrorists may be able to do more damage by clicking a keyboard button than by a mouse. In this article we will discuss about cyber-terrorism and its impacts on national security and various network vulnerabilities that are making cyber-attacks so unexceptional in society.

Keywords: Attacks, cyber, internet, terrorism

I. PREFACE TO CYBER-TERRORISM

Cyber-terrorism can be defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives.

Objectives may be political or ideological since this can be seen as a form of terrorism. Cyber-terrorism is the use of Internet attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses. Cyber-terrorism has much more adverse affects not only on an individual but to nations worldwide.

The United States Federal Bureau of Investigation (FBI) defines terrorism as, “The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.” (FBI, 2002).

A. Types of Cyber-terrorism

1) *Simple-Unstructured:* The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
2) *Advanced-Structured:* The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
3) *Complex-Coordinated:* The capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability (wikepedia, 2015)

II. REASONS BEHIND CYBER-TERRORISM

A. Religious

Theological beliefs often justify the use of violence and can include the sacrifice of one’s own life. According to Nelson [11], in contrast to revolutionary terrorism, religious violence may be unfocused and target the wider masses through advanced structured attacks that offer reward

B. ICT

ICT means information and communication technology, which has proved itself a boon for the society is also one the factors responsible for increasing cyber-terrorism attacks. As internet is easily available everywhere at low cost , so in modern era its not difficult to make negative use of technology for heinous crimes

C. Links between terrorists And Hackers

Links between computer hackers and terrorists, or terrorist-sponsoring nations may be difficult to confirm. Some hacker groups may also have political interests that are supra-national, or based on religion or other socio-political ideologies, while other hacker groups may be motivated by profit, or linked to organized crime, and may be willing to sell their computer services, regardless of the political interests involved. (Clay Wilson, 2005).

III. VULNERABILITIES IN NETWORK

There are many technical and non-technical vulnerabilities existing in the system which are responsible for security breaches and acts like cyber-terrorism. Some of these are:

A. Implementation Errors

In their haste to introduce the new features required by enterprises, vendors often neglect design choices that promote security. A constant stream of security advisories emanates from major vendors, thus posing an ongoing challenge to carriers and enterprises to secure their infrastructure. Often within days of these announcements, hackers have already developed exploits.

B. Configuration Errors

All of the components of the network (routers, firewalls, DNS servers, etc.) must be configured to control and customize their behavior and thus maximize potential security. The vendors of these products provide extremely complex, and often primitive, low-level languages for configuring the components, making these systems difficult and expensive to configure -- and the configuration process prone to error.

C. Protocol Vulnerabilities

Unlike voice, private line or frame relay, there is no “admission control” mechanism that’s part of the protocol suite itself. Anyone who has a connection to the network can inject packets into it. There is no mechanism for deciding which packets should be allowed into the network or not. This “open admission” architecture makes it easy for hackers or others wishing to cause harm to inject their destructive traffic. In addition, there are no authentication mechanisms inherent in the IP protocol. Anyone with a connection can send traffic, and their authority to do so is not questioned. (

REFERENCES

[1] B. Nelson, R. Choi, M. Iacobucci, M. Mitchell and F. Gagnon..Cyberterror prospects and implications. Centre for the Study of Terrorism and Irregular Warfare. Monterey, CA, 1999.
[1] Clay Wilson. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress, 2005
[2] FBI, 2002. Code of Federal.Regulations. 28 CFR. Section 0.85 on Judicial Administration. July 2001.
[3] Hossein, 2013, Cyber Security IP Network Vulnerabilities, accessed from https://www.linkedin.com/pulse/20130328181643-5213223-cyber-security-ip-network-vulnerabilities
[4] Wikepedia, 2015, accessed from http://en.wikipedia.org/wiki/Cyberterrorism