मितिः २०७८/०४/२९ (13 August, 2021)

साइबर सुरक्षाका लागि जनहितमा जारी सन्देश

डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमणसंग सम्बन्धितः

(१) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमण के हो?

Distributed Denial of Service(DDoS) Attack एउटा यस्तो आक्रमण हो जसमा साईबर अपराधीले नेटवर्कमा आबद्द रहेका विभिन्न उपकरणहरुलाई संक्रमित बनाई सोही उपकरणहरुको प्रयोग गरी सेवा प्रदान गर्ने सर्भरलाई लक्षित गरी आक्रमण गर्दछ। यसले गर्दा उक्त सर्भरबाट उद्देश्य अनुरुपको सेवा उपलब्ध गराउन नसक्ने हुन्छ। DDoS आक्रमण सामान्यतया Volume Based Attacks, Protocol Attacks, Application Attacks गरी तीन प्रकारका हुन्छन्। साईबर अपराधीबाट भएका केही महत्वपुर्ण DDoS आक्रमणहरु The AWS DDoS Attack(2020), Google Attack (2017), The GitHub Attack in (2018), The Mirai Dyn DDoS Attack(2016), The CloudFlare DDoS Attack(2014), The Spamhaus DDoS Attack(2013), Six Banks DDoS Attack (2012) रहेका छन्।

(२) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमणले कसरी काम गर्छ?

साईबर अपराधीले botnet अर्थात zombie computers (network of thousands to millions of remotely controlled, hacked computers or bots) प्रयोग गरी लक्षित वेबसाइट, नेटवर्क तथा सर्भरमा Packet Flood पठाई DDoS आक्रमण गर्ने गर्दछ। Packet Flood आक्रमणहरु मुख्यतः यस प्रकारका हुन्छन्।

क. Network Layer : Smurf Attacks, ICMP Floods, and IP/ICMP Fragmentation

ख. Transport Layer: TCP Attacks include SYN Floods, UDP Floods, and TCP Connection Exhaustion

ग. Application Layer: HTTP-encrypted attacks.

यसरी Packet Flood पठाउँदा सर्भरको सबै स्रोत साधन(Resources) प्रतिउत्तर पठाउन व्यस्त हुने र सर्भर crash समेत हुन गई उद्देश्य अनुसारको सेवा प्रदान गर्न सक्दैन।

(३) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमण भएको कसरी थाहा पाउने ?

प्रयोगकर्ताको कम्प्यूटर तथा नेटवर्कमा निम्न लक्षणहरु निरन्तर देखिएमा DDoS आक्रमण भएको हुन सक्छ।

- Locally or remotely फाइल access गर्दा ढिलो हुने।
- कुनै विशेष वेबसाइट खोल्दा लामो समयसम्म पनि नखुल्ने।

- इन्टरनेट सेवा बारम्बर अबरुद्द हुने।
- कुनै पनि वेबसाइट नखुल्ने।
- धेरै Spam इमेल प्राप्त हुने।

(४) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमणबाट कसरी बच्ने ?

१. प्रत्येक संस्थाले आफ्नो नेटवर्क तथा सर्भरको सुरक्षा कमजोरीहरु(Security Vulnerabilities) पहिचान गर्न Information Security Audit गरौं।

२. सुरक्षा कमजोरीहरु(Security Vulnerabilities) लाई यथासिघ्र हटाऔं।

३. DDoS आक्रमणबाट बच्न DNS सर्भरको Bandwidth लाई नियन्त्रण गरौं।

४. Router र नेटवर्क Firewall लाई Latest Security Patch सहित नियमित रुपमा अद्यावधिक(update) गरौं।

५. नेटवर्क ट्राफिकलाई नियमित अनुगमन गरौं।

६. Malicious traffic लाई रोक्न UTM/ Next Generation Advanced Firewall / Intrusion detection systems (IDS)/ Intrusion Prevention systems(IPS) को प्रयोग गरौं।

७. नेटवर्कमा जडित उपकरणहरुमा Default पासवर्ड हटाई बलियो पासवर्ड राखौं।

८. Router Configuration गर्दा Best Practices Security Policy तथा Cyber Hygiene अवलम्बन गरौं।

९. Zero Trust Security Model अपनाऔं।

१०. DDoS Response Battle Plan सहितको Business continuity Plan, Disaster recovery तथा Emergency response plan तयार गरौं।

११. आफ्नो नेटवर्क वा सर्भरमा DDoS आक्रमण भएको देखिएमा तत्काल इन्टरनेट सेवा प्रदायकलाई जानकारी गराई समस्या समाधान गर्न पहल गरौं।

१२. नेटवर्कको Critical Server को उपलब्धताको लागि Backup मा अर्को इन्टरनेट लिंक पनि राखौं।

Nepal Telecommunications Authority (NTA)
Cyber Security Task Force (NTACERT)
Jamal, Kathmandu, Nepal
Email: cert@nta.gov.np, Website: www.nta.gov.np