Monday, July 3, 2017

Benign (Normal human activities)

Tuesday, July 4, 2017

**Brute Force**

**FTP-Patator (9:20 – 10:20 a.m.)**

**SSH-Patator (14:00 – 15:00 p.m.)**

Attacker: Kali, 205.174.165.73

Victim: WebServer Ubuntu, 205.174.165.68 (Local IP: 192.168.10.50)

NAT Process on Firewall:

Attack: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50

Reply: 192.168.10.50 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73

Wednesday, July 5, 2017

**DoS / DDoS**

**DoS slowloris (9:47 – 10:10 a.m.)**

**DoS Slowhttptest (10:14 – 10:35 a.m.)**

**DoS Hulk (10:43 – 11 a.m.)**

**DoS GoldenEye (11:10 – 11:23 a.m.)**

Attacker: Kali, 205.174.165.73

Victim: WebServer Ubuntu, 205.174.165.68 (Local IP192.168.10.50)

NAT Process on Firewall:

Attack: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50

Reply: 192.168.10.50 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73

**Heartbleed Port 444 (15:12 - 15:32)**

Attacker: Kali, 205.174.165.73

Victim: Ubuntu12, 205.174.165.66 (Local IP192.168.10.51)

NAT Process on Firewall:

Attack: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.11 -> 192.168.10.51

Reply: 192.168.10.51 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73

Thursday, July 6, 2017

Morning

**Web Attack – Brute Force (9:20 – 10 a.m.)**

**Web Attack – XSS (10:15 – 10:35 a.m.)**

**Web Attack – Sql Injection (10:40 – 10:42 a.m.)**

Attacker: Kali, 205.174.165.73

Victim: WebServer Ubuntu, 205.174.165.68 (Local IP192.168.10.50)

NAT Process on Firewall:

Attack: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50

Reply: 192.168.10.50 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73

Afternoon

**Infiltration – Dropbox download**

**Meta exploit Win Vista (14:19 and 14:20-14:21 p.m.) and (14:33 -14:35)**

Attacker: Kali, 205.174.165.73

Victim: Windows Vista, 192.168.10.8

**Infiltration – Cool disk – MAC (14:53 p.m. – 15:00 p.m.)**

Attacker: Kali, 205.174.165.73

Victim: MAC, 192.168.10.25

**Infiltration – Dropbox download**

**Win Vista (15:04 – 15:45 p.m.)**

First Step:

Attacker: Kali, 205.174.165.73

Victim: Windows Vista, 192.168.10.8

Second Step (Portscan + Nmap):

Attacker:Vista, 192.168.10.8

Victim: All other clients

Friday, July 7, 2017

Morning

**Botnet ARES (10:02 a.m. – 11:02 a.m.)**

Attacker: Kali, 205.174.165.73

Victims: Win 10, 192.168.10.15 + Win 7, 192.168.10.9 + Win 10, 192.168.10.14 + Win 8, 192.168.10.5 + Vista, 192.168.10.8

Afternoon

Port Scan

**Firewall Rule on** (13:55 – 13:57, 13:58 – 14:00, 14:01 – 14:04, 14:05 – 14:07, 14:08 - 14:10, 14:11 – 14:13, 14:14 – 14:16, 14:17 – 14:19, 14:20 – 14:21, 14:22 – 14:24, 14:33 – 14:33, 14:35 - 14:35)

**Firewall rules off** (sS 14:51-14:53, sT 14:54-14:56, sF 14:57-14:59, sX 15:00-15:02, sN 15:03-15:05, sP 15:06-15:07, sV 15:08-15:10, sU 15:11-15:12, sO 15:13-15:15, sA 15:16-15:18, sW 15:19-15:21, sR 15:22-15:24, sL 15:25-15:25, sI 15:26-15:27, b 15:28-15:29)

Attacker: Kali, 205.174.165.73

Victim: Ubuntu16, 205.174.165.68 (Local IP192.168.10.50)

NAT Process on Firewall:

Attack: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50

**Afternoon: DDoS LOIT (15:56 – 16:16)**

Attackers: Three Win 8.1, 205.174.165.69 - 71

Victim: Ubuntu16, 205.174.165.68 (Local IP192.168.10.50)