ABOUT
SPEAKER

• Saroj Lamichhane – Co-founder/COO Rigo Technology
• The University of Northampton, UK
• Member –
  • OWASP – Nepal chapter
  • ISACA
• VA/PT, IS Audit, MSSP, SoC
PRESENTATION AGENDA

Overview

How Vulnerable is our Cyberspace

Countermeasures

Questions and Answers
OVERVIEW

Online devices in Nepal Cyberspace

- 163,604 – At night (11 PM)
- 163,838 – At Morning (7 AM)

Top Services

- Modem Web Interface - 50,794
- HTTP - 12,144
- Automated Tank Gauge - 6,473 (Ubiquiti?)
- SSH - 6,376 (22) and 763 (2222)
- DNS - 6,100
How vulnerable is our Cyberspace?

- **MS17_010 vulnerabilities**
  - 483 SMB services online
  - 22 is exploitable

- **Double Pulsar Backdoor**
  - 17 was vulnerable
  - 3 hosts are vulnerable
HOW VULNERABLE IS OUR CYBERSPACE (CONTD.)

**Wannacry**
- 2 “A” class bank effected partly
- 10 plus host were infected (Reported Privately)

**Heartbleed**
- 37 exploitable host

**Telnet**
- 4,288 (23)
- 106 (2323)
132 hacked ubiquiti devices due to older vulnerable firmware
DEFAULT PASSWORD

- HTTP (80) - 5
- HTTP (8080) – 86
- HTTP (8081) - 7
- HTTP (8880) - 1
- HTTP Automated Tank Gauge – 71 (Ubiquity)
- Telnet – 20 (Cisco – All Banks)
This page displays the general information and the status of the system.

**General Information**

<table>
<thead>
<tr>
<th>System Time</th>
<th>00:00.b4:cc:77:f5</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>00:00.b4:cc:77:f5</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>1.21</td>
</tr>
</tbody>
</table>

**Print Server Status**

- Print Server
- LPR
- IPP

**File/FTP Server Status**

<table>
<thead>
<tr>
<th>File/FTP Server</th>
<th>MScc77f5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workgroup</td>
<td>WORKGROUP</td>
</tr>
<tr>
<td>Description</td>
<td>NAS SYSTEM</td>
</tr>
</tbody>
</table>
Windows Server 2008 R2 Enterprise 7601 Service
Pack 1

Added on 2017-06-14 21:24:58 GMT
Nepal, Jawalakhel

Details

**SMB Status**
Authentication: disabled

**SMB Version:** 1

Capabilities: unicode, large-files, nt-smb, rpc-remote-api, nt-status, level2-oplocks, lock-and-read, nt-find, infolevel-passthru, large-readx, large-writex, lwio, extended-security

**Shares**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN$</td>
<td>Disk</td>
<td>Remote Admin</td>
</tr>
<tr>
<td>Backup-D-All-7Nov2014</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>Backup-from-E</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>C$</td>
<td>Disk</td>
<td>Default share</td>
</tr>
<tr>
<td>D$</td>
<td>Disk</td>
<td>Default share</td>
</tr>
<tr>
<td>Data</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>DeliveryPhotoVideo</td>
<td>Disk</td>
<td></td>
</tr>
<tr>
<td>E$</td>
<td>Disk</td>
<td>Default share</td>
</tr>
<tr>
<td>F$</td>
<td>Disk</td>
<td>Default...</td>
</tr>
</tbody>
</table>
Samba Version: 3.6.24

SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode, unicode, large-files, nt-smb, rpc-remote-api, nt-status, level2-oplocks, lock-and-read, nt-find, dfs, infolevel-passthru, large-readx, large-writex, extended-security

Shares
Name        | Type | Comments
------------|------|---------
IPC$         | IPC  | IPC Service (NAS Server)
Qsync        | Disk | Qsync
home         | Disk | Home
TUTORIALS    | Disk | For Student
Student      | Disk | System default share
Multimedia   | Disk | System default share
homes        | Disk |
Soft-Pack    | Disk |
DATA-CENTER/VPS VULNERABILITIES

Memcached RCE

- **TALOS-2016-0219** - Memcached Server Append/Prepend Remote Code Execution
- **TALOS-2016-0220** - Memcached Server Update Remote Code Execution
- **TALOS-2016-0221** - Memcached Server SASL Authentication Remote Code
MALWARE INFECTION

The highest risk of local infection
• Nepal - 46.19 %

17th in the world

Mobile malware
• Nepal - 29.90 %

5th in the world
ATM FRAUD

- Hacking Tourism
- Inside Job
SOCIAL NETWORKING RELATED CRIME

- Identity theft
- Personal Abuse
- Fraud and Data Mining
Zombie Host
Used in DDoS

SYSTEM HACKING
WEBSITES DEFACEMENT

- Add hijacking
- Malware Farming
- Used in DDoS
- Personal/Political abuse
“The root of suffering is attachment”

The Buddha
DEFACED WEBSITES (2016)

- .org.np (109)
- .com.np (501)
- .gov.np (451)
- .edu.np (164)
MALICIOUS WEBSITES (2017)

.org.np (29)
.edu.np (11)
.com.np (122)
COUNTERMEASURES

• Awareness
  ✓ General – Non-technical
  ✓ Specific - Technical
COUNTERMEASURES

• Stakeholder
  ✓ ISPs role
  ✓ End user role
  ✓ Organizations Role
  ✓ Law enforcement
    ➢ Digital forensic lab
    ➢ Early threat warning system
COUNTERMEASURES

• Threat sharing platform
  ✓ Inter-banks
  ✓ Inter ISPs
  ✓ Community – Open threat exchange platform
COUNTERMEASURES

• CSIRT Establishment
  ✓ Government
    ✓ Army
    ✓ Police
    ✓ Government Critical infrastructure
      ✓ GIDC
  ✓ Government-Private
    ✓ PPP model
COUNTERMEASURES

• National Cyber Security Policy

• Improvement in ETA-2063

• Others
  • Cyber-storm drill (CTF)
ALL SECURITY is not complete without YOU!