Eric Guzman 2/16/25
Hacking and Penetration Testing Professor Foti

Hacking Research Report

Executive Summary:

I looked at four large corporations Apple, Microsoft, Facebook, and Walmart based on publicly available information in this report. Through technical reconnaissance and open source intelligence (OSINT) techniques, I found domain registration information, network topology details, and information about each organization that might be able to be used by an attacker. The findings of the analysis presented some potential vectors of phishing, social engineering driven, and network intrusion attacks based on information available by public sources. I also found IP resolution and DNS configurations that showed security mechanisms that are in place, like Walmarts use of UltraDNS for DNS management and Akamai for content delivery. These results really show the need for organizational minimization of their online footprint and stronger information security controls.

Methodology:

The research was conducted by using a combination of technical and open source domain reconnaissance techniques like WHOIS requests, nslookup, and traceroute commands to retrieve domain ownership, IP address, and network path information for Apple.com, Microsoft.com, and Facebook.com. Public Domain Research included using Google to search company websites to obtain primary organizational data on Walmart, including executive leadership, physical headquarters, social media presence, and business partners. I also used dig and SOA record analysis tools to find DNS details that included Walmarts nameservers, DNS record structure and use of UltraDNS and Akamai. Traceroute allowed me to see that they also use CDN traffic routing giving more information on how sophisticated their security is.

Technical Research Results:

Apple.com -
The domain is owned by Apple Inc.
Registered IP addresses point to Apple's cloud infrastructure.
Network traces indicate global data center spread.

Microsoft.com -
Operates a huge infrastructure under Microsoft Corporation.
Heavy usage of Azure services for hosting.
WHOIS records indicate several administrative contacts.

Facebook.com -
Owned by Meta Platforms.

Makes use of cloud based load balancing and distributed servers.
Traceroute suggests heavy use of content delivery networks.

Public Domain Research Results:

Walmart (Target Organization):
Domain: Walmart.com
Headquarters: 702 SW 8th St, Bentonville, AR 72716, USA
Executives: CEO Doug McMillon, Chairman Greg Penner
Social Media: Active presence on Facebook, Twitter, LinkedIn, and Instagram.
Primary Nameserver: pdns1.ultradns.net
Additional Nameservers: A mix of UltraDNS and Akamai (e.g., pdnswm1.ultradns.net, a3-64.akam.net, a22-67.akam.net)
SOA Record: The responsible contact is hostmaster@walmart.com, which could be a point of interest for social engineering attacks.

Potential Vulnerabilities: The availability of executive contacts and corporate structure data can be used in spear-phishing attacks.

Findings and Conclusions:

The research identifies the excess of information freely available on open platforms, which can be abused by attackers. Apple, Microsoft, and Facebook are extremely secure with enterprise grade cybersecurity but remain vulnerable to DNS poisoning, phishing, and credential compromise. Walmart has high online visibility, and therefore, it is vulnerable to supply chain attacks and executive email impersonation scams. Common Vulnerabilities: Public WHOIS information, DNS data, and social media connections contribute to the attack surface.

Avenues for Future Research:

To go deeper in my security assessment even further, other research I could conduct could be:
Dark web intelligence gathering for leaked credentials or any insider threats.
Social engineering simulations to test company resilience.
Vulnerability scanning of Walmart's (or any of the four companies) subdomains and public facing infrastructure.
Investigating misconfigurations in UltraDNS and Akamai services that could expose weaknesses in Walmart’s infrastructure.

If an attacker were to mount an intrusion, they would try to identify poorly secured internal systems, harvest executive contact data for spear-phishing attacks and maybe exploit third party vendor relationships to infiltrate supply chains. This report highlights the need for organizations to actively deal with their digital presence and install strong security measures to avoid reconnaissance based attacks that can all be done using publicly available data.

Part 3: Challenge Exercise
Using what you learned in this lab, conduct data gathering and footprinting on the www.jblearning.com/cybersecurity website and add that research to your Hacking Research Report.

jblearning.com:

Domain: JBLEarning.com

WHOIS Lookup: The domain is registered with NameCheap, Inc. and uses Cloudflare for DNS management.

IP Resolution: nslookup and dig found two IPs: 104.18.216.42 and 104.18.217.42.

Traceroute Analysis: The network path revealed other hops before reaching Cloudflare's edge network, confirming traffic is routed through Cloudflare's CDN.

DNS Analysis: The domain uses Cloudflare nameservers (CASS.NS.CLOUDFLARE.COM and HENRY.NS.CLOUDFLARE.COM), which proves that the real web server location is masked.

Found Physical Location:
104.18.216.42 - 10 San Francisco, California, USA.

Potential Vulnerabilities: The presence of Cloudflare suggests strong protection against direct attacks, so looking for misconfigurations in servers might be the best opportunity to find vulnerabilities.