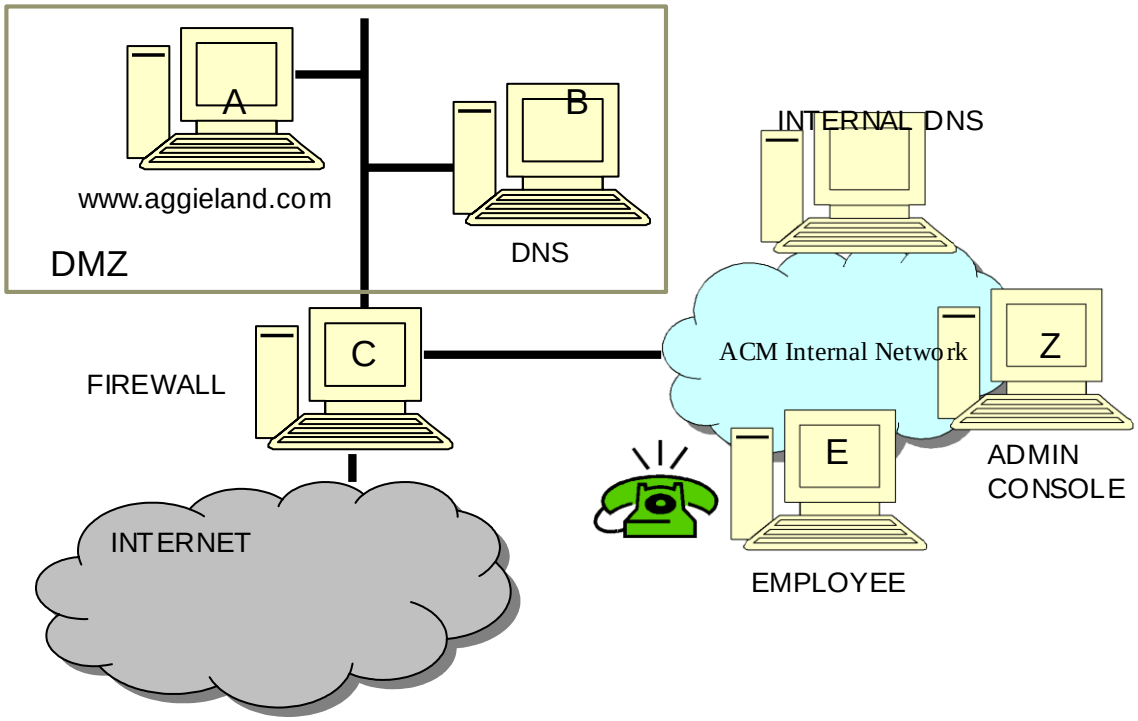
Varun Bindra
MS- Management Information Systems
TEXAS A&M UNIVERSITY

Aggieland Widgets, Inc.

Aggieland Widgets, Inc, the worldwide leader in widget manufacturing. It is not yet selling widgets on the Internet, but it has implemented a Web site that includes various static web pages showing off their widget wares. Aggieland has implemented the network architecture shown in Figure 1. This simple, familiar architecture, or small variation from it, is in widespread use throughout the world for a variety of organizations.



Network Architecture: Aggieland's network can be segmented into two LANS, one in the DMZ (Demilitarized Zone) and another that is internal to the organization and not open to the public.

The DMZ, constructed using a switch, includes a **Web Server** (Figure 1) for sending static pages to potential customers and a **DNS Server**. When the switch receives a packet, it listens to the MAC address of traffic flowing through it and associates particular MAC address to the plug and wire connection on the destination machine (e.g., Network Interface Cards or NICs installed on each system on the DMZ LAN) and then sends this packet to the appropriate destination machine. Because the switch is not hard-coded with the MAC addresses, if it is flooded with incoming traffic, it starts to behave as a hub and sends all the incoming traffic to all the machines on the DMZ LAN. The Internal network consists of a **DNS Server** that runs on a Solaris system with an old version of BIND that is

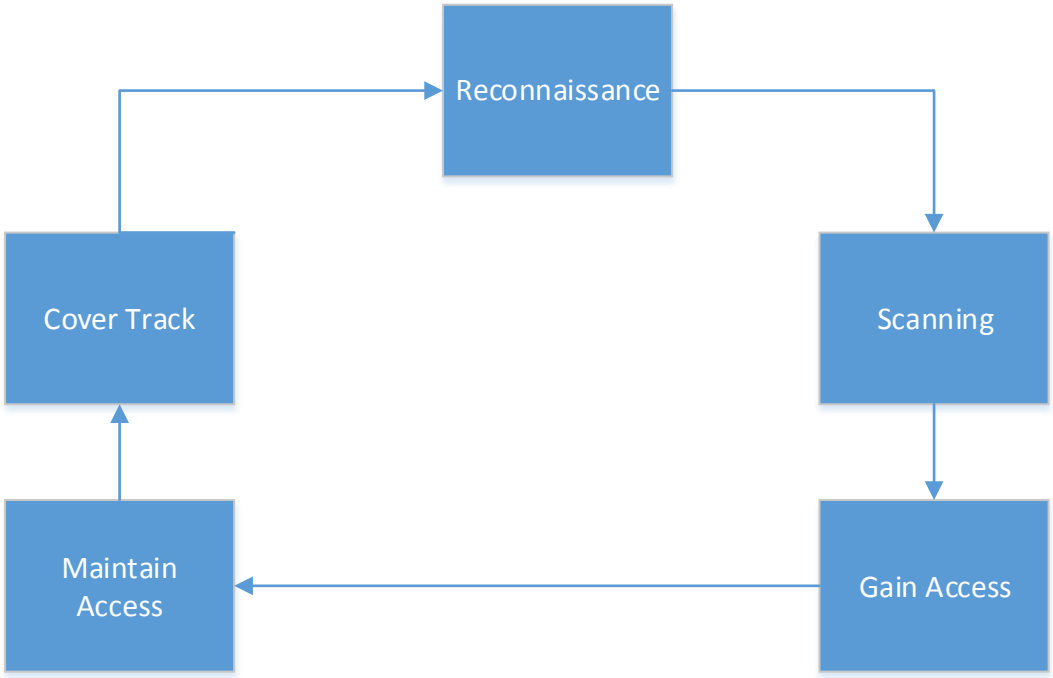
vulnerable to buffer overflow exploits. Furthermore, the address records of the Internal DNS server contain the record for the firewall, *firewall.Aggielandsample-company.com*.

Employee Connectivity: Aggieland has 1,000 employees, all connected via internal IP network. Because the company allows telecommuting, its employees are allowed to install applications on their systems that allow them dial-up access to their Aggieland systems from outside Aggieland's internal network. While Aggieland has password policy in place, this policy is not implemented on a strict basis for this dial-up access. All client machines within Aggieland's network run antivirus software although most users are not even aware of this program on their systems. Clients are encouraged to use antivirus software on their personal systems, especially those that they use for remotely accessing Aggieland network. However, no information is available on how many employees actually have antivirus on their personal systems.

Network Administration: Aggieland has been assigned the IP address space of w.x.y.0-255 and the administrator John Doe's phone number ABC-1024 is listed in the registration information. John Doe and two other administrators are the only ones in Aggieland who have root level privileges on various servers. Aggieland administrators control the firewall and DMZ systems from an administrative console on the internal network. The network administrators are diligent fellows and keep up with all patches that are made available for the operating systems and applications running on the internal network. They use Telnet to communicate with the web server and FTP to load any software on the DNS server located in DMZ. In addition, they connect to the Firewall using their browsers, through a web server listening on TCP Port 47155 of the Firewall. UserID and password is required before the administrators can make any changes to the Firewall configuration. Administrators strictly follow the password policy set by Aggieland (after all they are the ones who defined it!) and their password cannot be easily guessed using password cracking tools available in the public domain.

Varun Bindra
MS- Management Information Systems
TEXAS A&M UNIVERSITY

Below is the proposed plausible strategy to gain access and maintain access on one or more Aggieland Widgets,Inc systems. In the below explained process, it is advisable to use the same approach which a hacker uses to examine a network. Penetration testing customarily commences with three pre-test phases: foot printing, scanning and enumerating. These pre-test phases are very paramount and can make the distinction between a prosperous penetration tests that provides a consummate picture of the customer's exposure or one that doesn't.
There are five main steps which the hacker follows –



In this report the brief detail along with tabular presentation is explained which includes the name of activity, objective behind that particular activity, various tool and methods used, detail about each activity, results, assumptions and the possible controls. Aggieland Widgets,Inc is using DMZ architecture and the purpose of a DMZ is to add an additional layer of security to an Aggieland organizations local area network. With this architecture an external network node only has direct access to equipment in the DMZ, rather than any other part of the Aggiland network. But the internal consist of DNS server which runs on solaris system with old version of BIND vulnerable to buffer overflow exploits.

1) Reconnaissance - The process of accumulating information about an intended target of a malignant hack by probing the target system. The process typically involves port scanning in order to find weaknesses in the target system like finding week ports or if there are ways around the firewall and routers. The process of exploiting the system can then be carried out once the hacker has found a way to access the system.

   Reconnaissance is further classified into 2 types-

a) Passive reconnaissance – It involves accumulating information regarding a potential target without the targeted individual's or company's erudition. Passive reconnaissance can be as simple as visually examining a building to identify what time employees enter the building and when they depart. However, it's customarily done utilizing Internet searches or by Googling an individual or company to gain information. This process is generally called information accumulating. Convivial engineering and dumpster diving are withal considered passive information-amassing methods.

b) Active reconnaissance - It involves probing the network to discover individual hosts, IP addresses, and accommodations on the network.

Activity Name	Reconnaissance
Objective	• Attack in which the objective to collect information on Aggieland servers, employee of the organization and other information about servers.
Tools Used	• Search engine hacking - Search engines can be used like Google for reconnaissance • Social engineering • Domain name management / Search services • Non-intrusive network scanning • DNS reconnaissance
Activity Details	• Hacker can use various tools like Google search engine, FOCA, Sparta, DNS reconnaissance to extract the useful information. • Try using different keywords like allinurl, allintext, related, allintext etc in order to find different information. • Sniffing the network - It is the means of passive reconnaissance and can yield subsidiary information such as IP address ranges, denominating conventions, hidden networks, and other available services on the system or network. • Some hackers might dumpster dive to find out more about the Aggieland Widgets,Inc organization. Dumpster diving is the act of going through the organization's trash. • Used Google to find various credentials about Aggieland Widgets,Inc names of employees working in that organization and there contact information. • Details about the network used within the organization and what other safety measures organization has taken in order to protect their valuable information. • A hacker can use social engineering to manipulating people so they can give up confidential information. • Details about servers used like DNS server which is been used by the organization.
Results	• IP address can be revealed using any search engine and URL of Aggiland website.

	• Reconnaissance can reveal DNS server which is responsible for mapping the utilize cordial domain names to their corresponding IP addresses of Aggiland servers. If an intruder transmutes the DNS settings, so that Aggiland computer now uses one of the rogue DNS servers that is owned and maintained by the hacker. When this transpires, the rogue DNS server may translate domain names of desirable websites to IP addresses of maleficent websites.
Result from previous activities used in this step	• There is no as such information revealed in the previous step which can be used here.
Assumptions	• The assumption regarding this activity is that it is easy for hackers to gain access over the network and also they can use social engineering to gain access to the Aggieland system. • Hacker can make a contact with an employee of that organization or he may try to break physical security of that organization.
Suggested Controls	• Manage DNS server securely • Configure it to be as secure as possible against cache poisoning • Separate the authoritative function from the resolving function using different servers. • Avoid third party access - Many websites uses plug-in, widgets and other integrated components which can lead to compromises of website security and hacker can exploit vulnerability in website. For this reason company needs to update their software on a regular basis to prevent hackers from using discovered exploits. • Organizations should inform all employees to shred sensitive information or dispose of it in an approved way. • Avoid outdated scripts - Scripts are often used to develop a website to control everything from graphics to databases. They are mundane element for hackers to gain control of the website itself. • Utilize a good firewall and intrusion aversion system (IPS). The firewall controls which ports are exposed and to whom they are visible, while the IPS will detect port scans in progress and shut them down afore they are able to gain a full map of your network.

2) Scanning - After the reconnaissance stages have been consummated, scanning is performed. During scanning, the hacker perpetuates to accumulate information regarding the Aggieland Widgets,Inc network and its individual host systems. Information such as IP addresses, operating system, accommodations, and installed applications can avail the hacker determine which type of exploit to utilize in hacking a system. Hackers use scanning to identify target system's IP addresses. Scanning is withal used to determine whether a system is

on the network and available. Scanning implements are habituated to amass information about a system such as IP addresses, the operating system, and accommodations running on the target computer.

Activity Name	Scanning
Objective	• To identifying active hosts on a network for network security assessment.
Tools Used	• Nmap sctpscan Unicornscan Port Knocking warvox Nmap is best network vulnerability scanning software
Activity Details	• As this network can be accessed remotely by employees of organization so the first approach for hackers will be to find an open port and assail the open ports and services. • With the Nmap tool an attacker can find out details open ports and services. Network mapper is a free and open source utility for network revelation • Hacker can use WarVox which provides the unique ability to classify all telephone lines in a given range, not just those connected to modems. • Port knocking can be used by hackers which is a method of establishing a connection to a host that does not initially indicate that it has any open ports. • Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what accommodations like application name and version, those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in utilization, and dozens of other characteristics.
Results	• Nmap displays open and closed ports are displayed Example port 22, Protocol tcp, State - open , Service - ssh • Attacker will understand which port are open and which services are running on those port. • After understanding the complete structure attacker can plan his attack on the particular network.
Results from previous activities used in this step	• IP address • Server used • Platform used • Details of what level of security is used in organization from previous results.

	• DNS access
Assumptions if any	• Multilayer protection is used within the company • Hacker may find open port during scanning and he can take an advantage of that to hack entire system. • Employee within company may install some malicious software.
Suggested controls	• Turn-off all the unnecessary open ports • Do not change your default banner this will not reveal OS and Version of the system. • System hardening should be done. • Implement IP spoofing at the network edge, and also make use of strong firewall rules. • Physical security should also be considered • Any software installation should be restricted without the permission of administrator. • Allow critical devices, or devices housing or processing sensitive information, to respond only to approved devices • Maintain proper patch levels on endpoint and LAN/WAN systems

3) Gaining access - This is the phase where the actual hacking takes place. Vulnerabilities which were discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network, local access to a PC, the Internet, or offline.

Activity Name	Gaining Access
Objective	• To objective of hacker is to gain the access of the Aggieland Widgets,Inc network.
Tools Used	Some of the common tools which hackers uses to gain access over the network are • Network sniffers • Keyloggers • Password cracking tools • Rainbow Tables
Activity Details	• Network sniffer may be used by an attacker to gain access to information not intended for them. • Keyloggers - This can be installed to any computer to record

	every key typed. If the keylogger is hardware plugged in between the keyboard and computer, it can record all passwords entered.
Results	• The access over the network allow the intruders to move freely within the environment. Some implements like Rainbow Tables and homogeneous implements avail intruders purloin credentials, escalate privileges to admin, and then get into any system on the network that's accessible via the administrator account. Once the assailants gain elevated privileges, the network is efficaciously surmounted and is now owned by the intruders. • Once a hacker has access to your router administration page, he can do many things like inject malicious content to your web browser, and attack other computers connected to the network, and much, much more • Send maleficent emails to all the contacts in aggiland mail folders in order to spread viruses, malware and spyware to other computers. • Use Aggiland organization computers to direct attacks against targets such as banks and governments.
Results from previous activities used in this step	• Port details - open ports • IP address • Server used
Assumptions if any	• If an attacker install a keylogger and capture every username and password typed on the keyboard which will give him access to every single detail and he can misuse them. • A hacker can then use your computer to log into your bank accounts, carry out transactions and basically steal your money.
Suggested controls	• In order to protect attack from router up gradation of router is recommended in Aggieland Widgets,Inc organization • By using the most secure network protocol your router supports. • By using very long and strong passwords. • Turning off remote / web browser based administration • Enabling your router's firewall. • Encrypt highly sensitive information and protect keys

4) Maintain Access - Once a hacker has gained access, they keep that access for future exploitation and attacks. Once the hacker owns the system, they can utilize it as a base to launch other attacks. In this case, the owned system is sometimes referred to as a zombie system.

Activity Name	Maintaining Access
Objective	• To maintain the access to the Aggiland network and can hack whenever he wants to hack. • Hacker want to maintain Super Admin privileges which John Deo and his team has.
Tool(s) Used	• Backdoor • rootkit • Sniffers • Trojan horse
Activity Details	• After gaining the access to the network an intruder escalates all the privileges of the super admin and upload the piece of code which is termed as backdoor on the targeted network so that he can hack that particular system whenever he wants to. An attacker may maintain his super admin privileges in aggiland network. • Rootkit is a set of tools used to avail the attacker maintain his access to the system and utilize it for maleficent purposes. Rootkits have the capability to mask the hacker, hide his presence, and keep his activity secret. An attacker may use rootkit to hide his identity while attacking in aggiland networks. • Trojan horse appear to be one type of software but disguise a malevolent intent. So hackers can use trojan horse in Aggieland networks in order to maintain access.
Result(s)	• In this phase hacker maintain the access to the network and he can do anything he want to. • He can steal passwords even he can destroy entire system of aggiland. • A hacker is able to gain access to the system, and potentially use the system as a zombie in order to hack additional systems.
Results from previous activities used in this Step	• All the network details, Passwords and other details mentioned in previous steps can be used in this step. • As hacker needs to maintain access so any updated information in the network is required by him.

Assumptions (if Any)	• Attacker can attack again and again as he is super admin. • He can also send malicious virus to other contacts • Attacker may found other contact from Aggieland Widgets,Inc organization and he might attack other organizations associated with Aggieland Widgets,Inc.
Suggested Controls	• Using IDS and IPS devices to detect intrusions, we can also use them to detect extrusions. • Detect sessions of unusual duration, frequency, or amount of content • Look for connections to odd ports or nonstandard protocols • Prevent direct session initiation between servers in data center and networks not under your control • Detect and filter file transfer content to external sites or internal devices

5) Covering Tracks and Hiding - To avoid getting caught hackers clears all the evidence and all kind of log files. They delete all uploads backdoor and anything which is related to them, which may later reflect his presence. Following techniques can be used to hide details like such as hidden directories, hidden attributes, and Alternate Data Streams (ADS), can be used.

Activity Name	Covering Tracks and Hiding
Objective	• To hide the identity to be secure
Tool(s) and methods Used	• Steganography • Trojans • Port binding • Connect-back • Connect availability use

Varun Bindra
MS- Management Information Systems

Activity Details	• To avoid getting traced and caught, hackers normally clears all the traces by clearing all kind of logs and also by deleting the backdoor. Contacts. • Trojans destroy the details from log • Clearing Event Logs with the Meterpreter – The command clearev to clear all event logs • Shredding the History File
Result(s)	• Unable to catch attacker. • Attacker cannot be caught and he can make multiple attempts to hack the network again.
Results from previous activities used in this Step	• Attacker can keep the track of all the above information which he gathered from scanning.
Assumptions (if Any)	• Attacker may keep the track of the path which he followed and can use the same path in futue to attack the same network.
Suggested Controls	• Aggieland Widgets,Inc corporation should have firewalls in place that can block entry points from all but authorized users with which the execution of a port binding backdoor attack is nearly impossible. • Network monitoring - Monitoring can help guarantee that any suspicious activity such as information being gathered by a command and control server is flagged with network administrators.