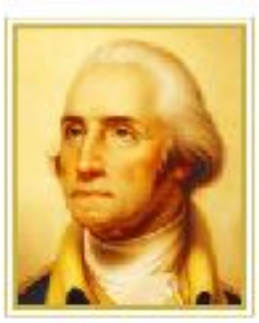

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

Computer Science 6907
Computer Network Defense II

In Class Exercise #1

Kevin Yasuda
Matthew Norris

Command and Control

As discussed in class, Domain Generation Algorithms (DGAs) are often implemented by malware authors as either a primary or secondary means of maintaining connectivity to their widely deployed bots. In the lecture, we provided samples of several mechanisms/algorithms that may be deployed to accomplish this. For your in-class exercise, you will first configure your own DNS server, analyze some simple DGA traffic to identify the algorithm being employed, and create new Address records on your DNS server to respond to all instances of the DGA traffic. Instructions for the basic server setup are included below for your reference.

Host Setup:

- First, to minimize confusion and simplify administration, you should change your hostname to be a unique hostname for your system. For the purposes of this exercise, you should change your hostname to be "CND2-DGA-student<n>" where <n> is your student number. e.g. CND2-DGA-student07 for the 7th VM.
  - vi /etc/hostname
- Next, you will need to set a valid, unique IP address. For this exercise, your IP should be 192.168.88.10<n> where <n> is your student number. e.g. 192.168.88.104 for the 4th VM.
  - vi /etc/network/interfaces
- To correctly configure SSH to run on boot, you will need to enable it for the default run level of the system. To identify the current runlevel, you can run the following program and issue the update-rc.d command below to enable the service on boot.
  - who -r
  - update-rc.d -f ssh enable <runlevel>
- SSH is configured by default to disallow remote connections from the root user. This is good practice in production (should always use sudo!), but in our lab we will override this default. To enable SSH to permit root logins, you will need to make the following configuration change.
  - vi /etc/ssh/sshd_config

```
#PermitRootLogin without-password
PermitRootLogin yes
```

- Now that you have made the above configuration changes, you can reboot the system to enable them to take effect. Once you reboot, if your changes were successful, you should be able to connect in remotely from the bastion host.
  - reboot

——

Exercise/Practical:

- Now that the system is configured to function properly on the network, you can begin to configure the DNS server. When the Bind9/named DNS server is installed on Debian systems, the configuration files reside in the /etc/bind directory.
- First, you will need to configure the named.conf file - in the version installed, you can leave the default configuration file unmodified and instead modify the named.conf.local file. The following entry will define the name of the current server (from the standpoint of the DNS system) and the file where specific A/host records can be defined.
  - vi /etc/bind/named.conf.local

```
zone “student00.dga.tiwaz.net” {
        type master;
        file “/etc/bind/student00.dga.tiwaz.net.hosts”;
};
```

- Now that you have specified the host file to define the DNS records you want to enter, you can create the zone configuration file for your domain. Specifically, the instructor DNS server is configured to delegate subdomains for each student server. The master DNS server is configured to look for all student00.dga.tiwaz.net child records from 10.75.75.100, all student11.dga.tiwaz.net child records from 10.75.75.111, etc… Thus, you will need to create a full zone file for your delegated subdomain. A boilerplate zone file is included below for your reference. To look up proper syntax for adding additional records, please reference Google. Suggestion: Use shorter TTLs to allow you to iterate faster.
  - vi /etc/bind/student00.dga. tiwaz.net.hosts

```
$ttl 38400
student00.dga.tiwaz.net.      IN    SOA    localhost.localdomain.  CND2-DGA-student00.dga.tiwaz.net. (
                        2016011401      ; serial
                        10800           ; refresh
                        3600            ; retry
                        604800          ; expire
                        38400           ; minimum
                        )
student00.dga.tiwaz.net.      IN    NS     server.student00.dga.tiwaz.net.
```

- Once you have configured the named server to serve the domains of your choosing, you will need to modify the named daemon to listen on TCP port 53 for IPv4 (as opposed to the default behavior. To do this, you will need to make the following change.
  - vi /etc/bind/named.conf.options

```
// listen-on-v6 { any; };
listen-on port 53 { any; };
```

- Now that you have configured the server, you can restart it and test your configuration. Note you can also explore using the bind command program - “rndc”
  - /etc/init.d/bind9 restart

- Error logs from your server and named service get written to the /var/log/syslog file, you can review the errors in this file to perform basic troubleshooting.
  - tail /var/log/syslog

- Once you have successfully configured your DNS server, the instructor DNS server will begin querying your server with domains that are being generated by a DGA. Your in-class exercise is to identify the algorithm being utilized to generate the traffic. Once you have identified the DGA, create the appropriate entries on your DNS server to respond to those queries with the IP address of your DNS server.