Injections and Ability to Respond to Them.

Inject Number: 6

Competition: MWCCDC Invitational

From: CIO

To: IT Staff

Subject: INCIDENT REPORTING

If you suspect an incursion by the Red Team, please submit an Incident Report with as much detail as possible. Many of the points lost due to Red Team activity can be recouped through diligent, thorough, and complete reporting of known and suspected attacks. Please submit one report for each incident; be as detailed as possible.

Include the following information:

* date/time the attack started (if known)

* date/time the attack was discovered

* attacker source address

* target system name / address

* target port / service

* type of attack (virus, hacking, DoS, etc)

* result of attack

* vulnerability that allowed the attack

* how discovered

* how contained

* remediation actions / controls

* result of remediation

Thank you.

CIO

Inject Number: 7 – did not respond in time. → Not completed.

Competition: MWCCDC Invitational

From: IT Director

To: Bue Teams

Subject: 01-SMTP and POP3 services

The CIO has noticed that our email systems are not up and running. These services are configured on the x.39 public address which should be properly NATed.

Please Remedy the issue and provide a brief summary on why the service is not running.

Thank you.

IT Director

Inject Number: 8 → **was able to respond with One Logon Banner**

Competition: MWCCDC Invitational

From: General Counsel

To: Infrastructure Team

Subject: 02-Implement Logon Banners

Implement logon banners that meet the best practices standards:

Login banners provide a definitive warning to any possible intruders that may want to access your system that certain types of activity are illegal, but at the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s).

A requirement for successfully prosecuting unauthorized users who improperly use a university computer is that the computer must have a warning banner displayed at all access points. The banner must warn authorized and unauthorized users:

what is considered proper use of the system;

that the system is being monitored to detect improper use and other illicit activity;

that there is no expectation of privacy while using this system.

Provide screen shots of these in functioning for:

1.) Firewall

2.) A Windows Server

3.) A Linux Server

Thank you.

General Counsel

Inject Number: 9 → **responded. See User Policies below**

Competition: MWCCDC Invitational

From: HR Director

To: Infrastructure Team

Subject: 03-Create Acceptable Use Policies

The HR VP is requiring that we implement an Acceptable Use Policy for our user community to acknowledge. Please develop a policy statement in a format that is a policy and ready for employees to sign.

If you use outside resources to aid in drafting our policy, be sure to give proper acknowledgment and respect to all copyrights.

Management Instructions:

At a minimum we'll need one policy document to cover acceptable use of the following:

* Email

* Internet Usage

* Social Media & Blogging

* Mobile Device and IoT

* Personal Use of Company Equipment

* The use of personal digital assistants (i.e. Alexa) in the work place

Make sure these do not conflict with any existing Company policies or Laws, or modify those other policies to match these, as appropriate

"User Policy
Updated 11/23/19

1. Unauthorized access is strictly prohibited. All unauthorized access will be prosecuted to the fullest extent of the law.
2. All users must be authorized by the IT department.
3. Users will use email accounts provided by IT department.
4. Email and Internet usage will be work related only, accessing sites not related to work will result in disciplinary action. Users must not use company equipment for personal use
5. Users must have all personal mobile devices connected to the company network approved by IT department—this includes personal assistants such as Alexa.
6. Any suspicious activity will be reported to the IT department immediately.
7. Company and IT department have right to change User Policy when necessary."

Inject Number: 10 → **Attempt on Debian, not completed.**

Competition: MWCCDC Invitational

From: Director - Systems Engineering

To: Infrastructure Support

Subject: 04-Configure NTP

Team, we really need to have a consistent time on our network so that log entries are properly documented and can be used in court.

Inject Instructions:

1) You are to set up one main clock on the network that every machine will be reconfigured to get the time from. clearly identify which device this is in your response.

2) Please configure all devices, servers and workstations to get their time from this clock.

Provide screen shots demonstrating that the time is synced across all machines and devices, including the commands and/or utilities used to accomplish the tasks.

Thank you.

Director - Systems Engineering

Inject Number: 11 → **responded, see response below**

Competition: MWCCDC Invitational

From: CIO

To: IT Director

Subject: 05-Incident Response - Logging Issue

You have detected hackers have entered your network and maybe in the process of exfiltrating data. You have quickly acquired some special auditing tools to capture data while the attack is occurring. Will there be any issue with using these logs in a subsequent court case. What will be necessary to make the logs acceptable? Cite any sources you used in your research.

Thank you.

CIO

"There will be no issue moving forward with proper documentation relating to the hacking of our network. All users will be logged with accurate time and place of the attacks. Users will be notified of potential ability to be called to court, user policy will be updated."

Inject Number: 12 → **completed and responded without screenshot**

Competition: MWCCDC Invitational

From: Sec Ops

To: Network Team

Subject: 06-Implement Denial of Service Protection Policies

The CEO read a report in Network World about how hackers often use DoS Attacks against major businesses.

Be sure your Palo Alto Firewall is configured with a defining DoS Protection Policy together with defining zone protection on the EXTERNAL zone.

Your deliverable is a report to the IT Director on how you accomplished this, with screen shots showing the policy and the zone protection dialogue box.

Thank you.

Sec Ops

Inject Number: 13 → not completed, see response below.

Competition: MWCCDC Invitational

From: IT Director

To: Infrastructure Support Group

Subject: 07-Firewall Policy

Develop a FW policy, leveraging the application-layer logic of the Palo Alto firewall as much as possible that:

1.) Permits your services to be scored.

2.) Restrict outbound traffic to expected response traffic plus your own internal needs

3.) Appropriately restricting traffic transiting between segments (Public, Internal, and User)

3.) Deny all other traffic.

4.) Enable threat protection on all permitted traffic flows.

In your response, show a screen shot of the policy and a memo that documents each policy statement and whether it is restricting inbound traffic, outbound traffic, or denying other flows.

Thank you.

IT Director

"Hello,
The Firewall is already providing the functions requested by the CISCO router. Adding a router would change the NAT processing. More clarification is requested in order to follow up with these requests.

Thank you."

Inject Number: 14 → did not complete

Competition: MWCCDC Invitational

From: IT Director

To: Blue Team

Subject: 08-Preparation for Screening Router

The IT Director is planning on placing a router in front of the Palo Alto Firewall as a screening router. NOTE: there is no router currently. This is purely a planning document in anticipation of acquiring one. This will require some addressing changes and a decision on where to handle NAT. The document you are preparing plans for that and specifies the approach to these issues.

Prepare a document that addresses the issues:

1.) What will be the addresses on the inside and outside interfaces of the router ?

2.) What will be the addressing on the firewall's outside interface ?

3.) Will NAT processing change, if so how, or can it be left alone ?

5.) Develop prototype inbound access lists, for a CISCO router, that:

1.) Filter out bogons (https://www.team-cymru.com/bogon-reference.html). Do this as relevant for the competition environment.

2.) Filter out packets sourcing from your own address space.

3.) Packets with low TTL values.

4.) Other elements to consider ?

Thank you.

IT Director

Inject Number: 15

Competition: MWCCDC Invitational

From: CIO

To: Security Operations Group

Subject: 08a-Capture Red Team Traffic

Using WireShark and the external Windows 10 PC, do a packet capture of a series of packets that represent Red Team activity. Filter the capture so that only those packets are displayed.

Submit a screen shot along with an explanation as to why you think these packets represent Red Team activity.

Thank you.

CIO

Inject Number: 16

Competition: MWCCDC Invitational

From: IT Director

To: Security Operations Group

Subject: 08b-Log Management

Create a centralized logging service, or configure Splunk to be the repository for all syslog activity.

Respond with a screen shot documenting your choice and its functionality.

Thank you.

IT Director

Inject Number: 17 → completed past due time

Competition: MWCCDC Invitational

From: IT Director

To: IT Staff

Subject: 09-Daily Firewall backup

Configure the Palo Alto firewall to do a daily backup at 2pm (local time) to an internal FTP server. Please provide a screen shot of the GUI configuration and evidence of a test backup.

Thank You

IT Director

Thank you.

IT Director

Inject Number: 18

Competition: MWCCDC Invitational

From: IT Director

To: Security Operations Group

Subject: 09a-Abnormal Activity Log Report

Using the logs from your central repository, create a report of log entries that represent an attack/Red Team activity.

Provide a screen shot of those log records, together with an explanation as to why these records are thought to be Red Team activity.

Thank you.

IT Director

Inject Number: 19

Competition: MWCCDC Invitational

From: IT Director

To: Server Support Group

Subject: 09b-Web Page Security

Develop a script or use an open-source tool to implement a check on the files that compose the web pages of our services. The script should provide an alert to the support group staff if they are changed from their baseline.

Respond with a business quality memo that describes the solution of the implementation and screen shots to document it and its functioning state.

Thank you.

IT Director

Inject Number: 20 → completed

Competition: MWCCDC Invitational

From: Internal Audit Mgr

To: Infrastructure Support Group

Subject: 10-Verify Perimeter

Using the Windows-10 machine outside the FW and a port scanning tool: scan the external interface of your address space to inventory:

1.) The responding servers

2.) The services offered on each server

Respond with a business-quality memo with this information listed in tabular form. Include, as an appendix, the screen shots of the tool discovering this information.

Thank you.

Internal Audit Mgr

Inject Number: 21 → **responded to and denied requested access for vulnerability assessment**

Competition: MWCCDC Invitational

From: Internal Audit Dept

To: Infrastructure Group

Subject: 11-Internal Assessment

Using an open-source vulnerability assessment tool, such as OpenVAS, scan your internal network segments to:

1.) Discover what services are enabled on each server/device

2.) What potential vulnerabilities are present on each

Respond with a business-quality memo that summarizes your finding in tabular form. Supply, as an appendix, screen shots of tool working.

Thank you.

Internal Audit Dept

Inject Number: 22 → **did not complete, did not receive from anyone running Linux.**

Competition: MWCCDC Invitational

From: IT Director

To: Server Support Group

Subject: 12-Linux Firewall Configuration

Configure the software firewall features on each Linux server to only allow expected inbound and outbound traffic. Show screen shots of each server's configuration.

Thank you.

IT Director

Inject Number: 23 → **completed windows server 2008, completed windows 8.1**

Competition: MWCCDC Invitational

From: IT Director

To: Server Support Group

Subject: 13-Windows Firewall Configuration

Configure the software firewall on each Windows server to only allow expected inbound and outbound traffic. Show screen shots of the configuration of each server.

Thank you.

IT Director

Inject Number: 24 → denied patch update notes/vulnerabilities

Competition: MWCCDC Invitational

From: IT Director

To: Server Admin Group

Subject: 14-Patch Levels

Submit a business quality memo that summarizes the inventory of IT devices (service, firewalls) in tabular form and their current OS/patch level. Have a columns that for;

Device Name

OS Version

Current Version

Does the existing version have known vulnerabilities, catalog two that are a concern to you.

Thank you.

IT Director

Inject Number: 25 → completed.

Competition: MWCCDC Invitational

From: IT Director

To: To Infrastructure Team

Subject: 15-QoS Marking of Traffic

Traffic inbound to our DMZ servers is very important. Develop a configuration on the PA Firewall that marks the TOS field of the IP packet in accordance with the IP Precedence scheme. DMZ destined packets should be marked as 3. All other traffic should be 0.

Respond with a memo that documents how you accomplished this with a copy of the PA QoS policy that shows how this was implemented.

Thank you.

IT Director

* vulnerability that allowed the attack

* how discovered

* how contained

* remediation actions / controls

* result of remediation

* date/time the attack started (if known)

* date/time the attack was discovered

* attacker source address

* target system name / address

* target port / service

* type of attack (virus, hacking, DoS, etc)

* result of attack

- 20-30 ports block not scored ports
- 1 hour in started scoring default creds
- check database - used default creds
- splunk/phantom double-edged sword, they will implant on them
- dont browse on boxes you don't need to
- block ports asap
- incedent: state sorce of activity, evendence
- think about why scords happen, could be attack
- lots of false positives
- trafic gen, then interserved w/ other trafic
- dont say no on injects
- find policys on internet (make sure to give ~~credit~~ credit)
- finish injects
- injects = hints
- no fake injects in midwest
- no socal engineering
- gui for firewall

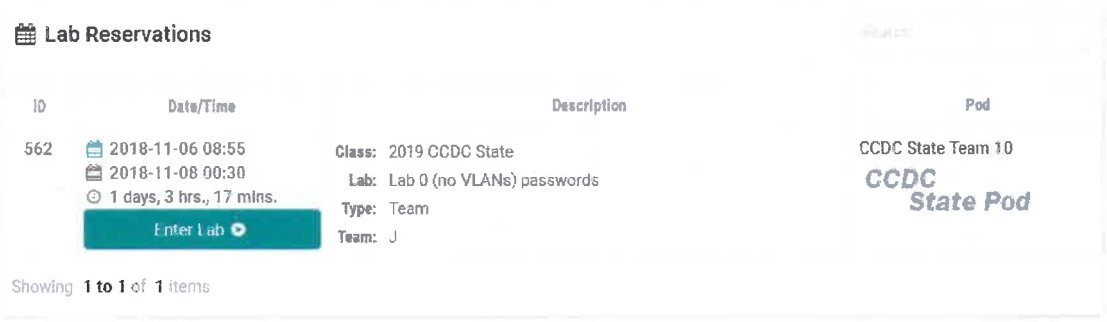
v1u1, v1u2, v1u3, …., v1u8

Accounts for other teams follow the same pattern. For team2 the accounts are,

v2u1, ….

Note that teams initially only have access to the ISE/Team Portal. Team assignments are issued prior to the event so the proper accounts are known. The password needed to access the Competition Stadium is issued by the ISE via an inject to inform teams of their initial password applicable for all team accounts.

Once authenticated you will be asked to change your password and confirm a few details regarding your profile. Remember your new password! Subsequently you should see a lab reservation for your competition network, similar to the following:



Each team member can click on 'ENTER LAB' for their respective lab/pod reservation to gain access to their competition network. The competition network topology, shown later in this document, should be clearly visible. To access individual VMs simply click on the respective VM name at the top of the screen.