

Securing Web Resources using RFID, Dynamic Groups, Honeypots and SIEM Alerting

Mark Deegan

Dept. of Computing, Carlow Campus
South East Technological University
Rep. of Ireland
mark@deeganit.net

Martin Harrigan

Dept. of Computing, Carlow Campus
South East Technological University
Rep. of Ireland
martin.harrigan@setu.ie

Abstract—

Index Terms—component, formatting, style, styling, insert

I. INTRODUCTION

II. RELATED WORK

Amico [1]

III. METHOD

Our system comprises a variety of off-the-shelf components:

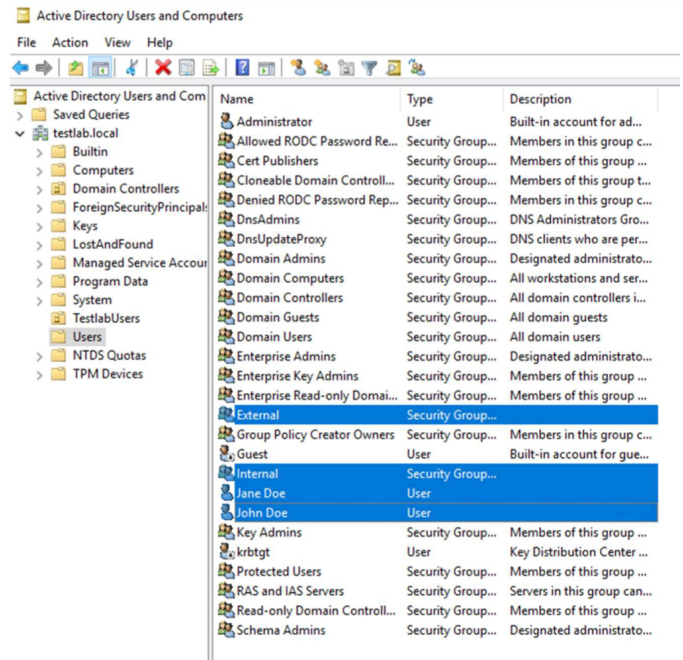
- Microsoft Active Directory with LDAP support
- Raspberry Pi connected to an RFID door entry system (see Fig. 2)
- Progress Kemp LoadMaster
- Progress WhatsUp Gold
- Web servers (Apache HTTP Server)

A. Microsoft Active Directory With LDAP Support

We used Microsoft Windows Server 2019 to run a Domain Controller (DC) (d1.testlab.local) for our domain (testlab.local). This is the primary DC for the scenario and it was setup to host Active Directory (AD) with LDAP support and the Domain Name System (DNS). To ensure that the requests for the Web resources went to the right services on the Progress Kemp LoadMaster, we created appropriate DNS delegations. This is important as we wanted the external requests to be pointed to the external resources and the internal requests to be pointed to the internal resources. It also allows the LoadMaster to do service health checks before responding to a DNS request thus preventing an IP being returned when a resource is unavailable. We added two users, Jane Doe and John Doe, and two groups, Internal and External, to AD (see Fig. 1).

B. Raspberry Pi and RFID Door Entry System

The Raspberry Pi is connected to an RFID door entry system. When a user performs a card swipe, a Python script running on the Raspberry Pi reads the identification details from the card and remotely changes the group membership of the user in Active Directory.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Re...	Security Group...	Members in this group c...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controll...	Security Group...	Members of this group t...
Denied RODC Password Rep...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domai...	Security Group...	Members of this group ...
External	Security Group...	
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Internal	Security Group...	
Jane Doe	User	
John Doe	User	
Key Admins	Security Group...	Members of this group ...
krbtgt	User	Key Distribution Center ...
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controll...	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...

Fig. 1. We created two users, Jane Doe and John Doe, and two groups, Internal and External, in Active Directory.

C. Progress Kemp LoadMaster

Progress Kemp LoadMaster (LM) is a reverse proxy and load balancer. It has many capabilities but for this scenario we are interested in the Edge Security Pack (ESP), the Web Application Firewall (WAF), and the source IP blacklist from the GEO component. We use the ESP for Single Sign-On (SSO) for HTTP(S) services and to communicate with the AD for both for logon and group memberships. This pre-authenticates a user before they gain access to a resource. We also enabled *group steering* on the ESP: this allows LM to send traffic to particular services based their group membership in AD and goes beyond the normal use of groups to simply allow or deny access.

We created two steering groups associated with the Internal and External groups in AD. We created Perl Compatible Regular Expression (PCRE) rules to match the authorisation

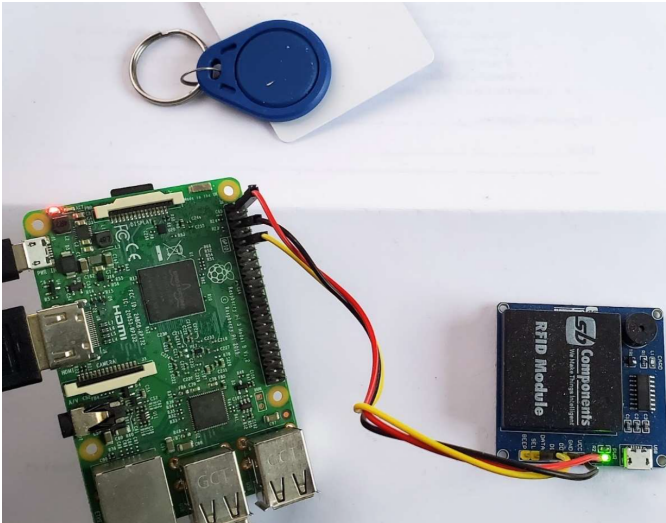


Fig. 2. The Raspberry Pi was connected to an RFID door entry system. We created a Python script that read the identification details from swiped cards and interacted with Active Directory.

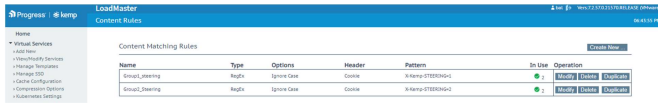


Fig. 3. ...

cookies and steer the requests to the correct services (see Fig. 3).

The login page that is displayed by the ESP is the same for both *valid* and *invalid* access attempts. A valid access attempt occurs when a user's group and request are both internal or both external; otherwise the access attempt is invalid. This helps with threat hunting as a threat actor will get the same login page for the honey pot as with the valid site. The honey pot can gather the details of the access attempt without being discovered.

The GEO component performs DNS resolution and service health checks before returning a result. We created GEO DNS entries for `internal.testlab.local` and `external.testlab.local` (see Fig. 4). We also used an IP blacklist that is updated each day to withhold DNS results from anyone on the list.

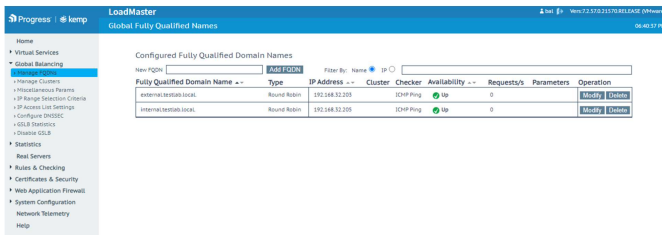


Fig. 4. We configured two FQDNs for `internal.testlab.local` and `external.testlab.local` using LoadMaster's GEO component.

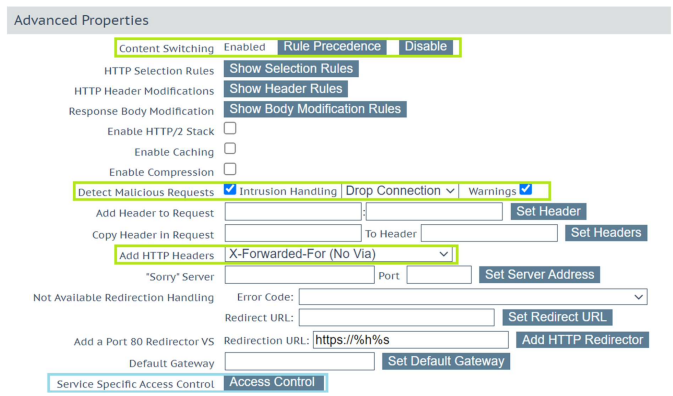


Fig. 5. We enabled IDS/IPS in LoadMaster as an additional layer of defence for little configuration.

Additionally, we enabled IDS/IPS. This includes rules defined by the SNORT community [?] and enables the SNORT rule filtering on the Layer 7 HTTP engine to check for any known bad requests. Figure 5 shows to configuration highlighted in green. There is also an option to prevent access via whitelists and blacklists highlighted in blue.

D. Progress WhatsUp Gold

E. Web Servers

IV. RESULTS

V. CONCLUSION

REFERENCES

- [1] J. Amico, "Open sourcing our token delegate program," <https://a16z.com/2021/08/26/open-sourcing-our-token-delegate-program> and <https://archive.today/X47Kb>, 2021.