

Other_Topics

Tuesday, November 21, 2023

6:40 AM



Network Recon



Webservers

SQL Databases

NoSQL Databases

Distributed Databases

Distributed Queues

Proxy Servers

SMTP Servers

POP3 Servers

IMAP Servers

SIEM Platforms

SMB Servers

SSH Servers

Telnet Servers

NTP Servers

TFTP Servers

IRC Servers

Finger Servers

RADIUS

VNC

SNMP



Real World WebApps





- Remote Code Execution
- Stored XSS
- File Upload
- SQL Injection
- XML External Entity
- SSRF
- SSTI
- Command Injection
- Local File Inclusion
- Reflected XSS
- CSRF
- Arbitrary File Download
- Directory Traversal
- Broken Authentication



Metasploit



- Windows Apps Exploits
- Linux Exploitation
- Meterpreter
- Post Modules
- Metasploit CTFs
- Metasploit Pivot CTFs
- Latest Targets
- WordPress Exploitation
- Pivoting
- Auxiliary Modules
- WebApp Exploits

 Infrastructure Attacks 



[Memcached](#)

[Squid Proxy](#)

[MongoDB](#)

[Apache](#)

[Nginx](#)

 Privilege Escalation 

[Linux](#)

[Web to Root](#)

[App to root](#)



[Linux Capabilities](#)

 Code Repositories 

[Git](#)

[Python PyPi](#)

[APT Repository](#)

 Endpoint Security 



[osquery](#)

[OSQuery MITRE](#)

[Sysdig](#)

[Malware Scanner](#)

[HIDS](#)

 Persistence 

[Maintaining Access](#)

[Data Exfiltration](#)



Log Analysis



Webserver Logs

SSH Logs

Proxy Logs

DNS Logs

Windows Event Logs

Other Tools



REST



JWT Basics

JWT Advanced

JWT Expert

API Security

GraphQL



MITRE ATTACK Linux



Discovery

Credential Access

Persistence

Privilege Escalation



Service Exploitation



Linux Services

WebApp Frameworks



Web Technologies



WebSockets

Bot Attack

